Surrey Heath Borough Council

Surrey Heath House
Knoll Road
Camberley
Surrey GU15 3HD
Telephone: (01276) 707100
Facsimile: (01276) 707177
DX: 32722 Camberley
Web Site: www.surreyheath.gov.uk

Department: Democratic Services

Division: Legal & Democratic Services

Please ask for: Rachel Whillis

Direct Tel: 01276 707319

E-Mail: democratic.services@surreyheath.gov.uk

Monday, 28 March 2022

To: The Members of the **Employment Committee**
(Councillors: Colin Dougan (Chairman), Cliff Betton (Vice Chairman), Sharon Galliford, Mark Gordon, Josephine Hawkins, Rebecca Jennings-Evans, Alan McClafferty, Graham Tapper and Victoria Wheeler)

In accordance with the Substitute Protocol at Part 4 of the Constitution, Members who are unable to attend this meeting should give their apologies and arrange for one of the appointed substitutes, as listed below, to attend. Members should also inform their group leader of the arrangements made.

Substitutes: Councillors Peter Barnett, Rodney Bates, Paul Deach, Sashi Mylvaganam, Adrian Page and Kristian Wrenn

Dear Councillor,

A meeting of the **Employment Committee** will be held at Council Chamber, Surrey Heath House, Knoll Road, Camberley, GU15 3HD on **Wednesday, 6 April 2022 at 7.00 pm**. The agenda will be set out as below.

Please note that this meeting will be recorded.

Yours sincerely

Damian Roberts

Chief Executive

AGENDA

Pages

Part 1
(Public)

Members are invited to declare any interests they may have with respect to matters which are to be considered at this meeting. Members who consider they may have an interest are invited to consult the Monitoring Officer or the Democratic Services Officer prior to the meeting.

Minutes of a Meeting of the Employment Committee held at Surrey Heath House on 8 February 2022

+ Cllr Colin Dougan (Chairman)
+ Cllr Cliff Betton (Vice Chairman)

+	Cllr Sharon Galliford	+	Cllr Alan McClafferty
+	Cllr Mark Gordon	+	Cllr Graham Tapper
+	Cllr Josephine Hawkins	+	Cllr Victoria Wheeler
*	Cllr Rebecca Jennings-Evans		

+ Present
* In attendance virtually but did not vote

Members in Attendance: Cllr Rodney Bates

Officers Present: Louise Livingston, Julie Simmonds, Rachel Whillis.

22/EC Minutes

The minutes of the meeting held on 7 October 2021 were agreed as a correct record.

23/EC Pay Settlement 2022/23

The Committee considered a report setting out the current position on negotiations for the 2022/23 Pay Award. It was reported that negotiations had taken place at a Joint Staff Consultative Group meeting, but the Group had not reached an agreement on a proposed pay award. Staff Representatives had requested a consolidated payment of £650 on all pay scale points, whilst Member representatives had offered a consolidated payment of £500 on all pay scale points. Consequently, in accordance with the Annual Pay Settlement Procedure, both options were presented to the Committee for consideration.

Members considered the factors that had been presented as the basis for the Staff Representatives' request. Having taken into account these representations, whilst also recognising the Council's financial position, the Committee agreed to recommend to Full Council that a £500 increase on a pay scale points be agreed as the Pay Award for 2022/23.

It was advised that during the negotiations Staff Representatives had requested clarity on Christmas closure, specifically asking for the continuation of the arrangements in recent years whereby the Council had closed between Christmas and New Year. This had been facilitated by a combination of a contractual day's leave and the awarding of a further additional day's leave, which had been matched by staff taking a day's leave from their annual leave entitlement. Having indicated a desire to enhance the offer being made to staff, plus also recognising a need for further clarification on the status of the additional day's leave, Members agreed to grant an additional day's leave over the Christmas period in 2022/23. Arrangements for beyond 2022/23 would be further discussed at a future meeting.

The Committee echoed comments made at the Joint Staff Consultative Group meeting about improving the procedure for negotiations and agreed to add an item to its next meeting's agenda. It was also agreed to add an item to the future work programme on assessing whether to link future pay awards to the Medium Term Financial Strategy.

RECOMMENDED to Full Council that a consolidated increase of £500 on all pay scale points be agreed as the Pay Award for 2022/23.

RESOLVED that an additional day's leave be granted for the Christmas period 2022/23.

24/EC Safeguarding Policy and Procedure

The Committee considered a revised Safeguarding Policy and Procedure, which had been updated in line with changes in processes and guidance. Where possible, it had been amended to simplify and ensure clearer guidance when used as a reference document.

RESOLVED to adopt the revised Safeguarding Policy and Procedure, as set out at Annex A to the agenda report.

25/EC Casual, Fixed Term and Temporary Workers Policy and Procedure

The Committee was informed that the Casual, Fixed Term and Agency Workers Policy and Procedure had been reviewed to take into account the new Senior Management Structure and associated titles.

RESOLVED that the Employment Committee be advised to agree that the revised Casual, Fixed Term and Agency Workers Policy and Procedure, as set out at Annex A to the agenda report, be agreed.

26/EC Pension Discretions Policy

The Committee was informed that each pension fund was required to have a discretionary policy, which needed to be kept under review. Surrey County Council had not issued an updated Pensions Discretions Policy. Although there was no legal requirement that it be reviewed annually, it was this Council's practice to review it annually.

The Joint Staff Consultative Group had considered the Policy at its meeting on 13 January 2022 and had recommended updating paragraph 5.2 of the Policy to state that the table in the appendix referred to for the relevant decision maker. It had also agreed that references to job titles would be updated to reflect the revised senior management structure.

RESOLVED that the Pensions Discretions Policy be updated, as set out Annex A to the agenda report.

27/EC Review of Recruitment Policy and Procedure

The Committee considered proposed changes to the Recruitment Policy and Procedure, which aimed to reflect operational changes within the recruitment process. These changes included a new job profile template, a new timescale for making job adverts live, a new online staffing resources form, ongoing temporary changes to right to work checks due to COVID-19, and the new Disclosure Barring Service umbrella body company.

RESOLVED that the revised Recruitment Policy and Procedure, as set out at Annex A to the agenda report, be adopted.

28/EC Review of Health and Safety Policy - Statement of Intent

The Committee considered a review of the Health and Safety Policy- Statement of Intent, which had been updated to reflect the change in the Council's Chief Executive.

RESOLVED that the revised Statement of Intent, as set out at Annex A to the agenda report, be adopted.

29/EC Review of Health and Safety Policy - Organisation

The Committee considered proposed changes to the Health and Safety Policy – Organisation. Subject to further minor grammatical changes, it was agreed that the revised Policy be adopted.

RESOLVED that the revised Health and Safety Policy – Organisation, as set out at Annex A, as amended, be adopted.

30/EC Joint Staff Consultative Group Constitution

The Joint Staff Consultative Group Constitution had been reviewed and updated to reflect the establishment of the Employment Committee and its role in relation to the agreement of Staff Terms & Conditions. Amendments to the Constitution had also been made to reflect the revised senior management structure and the HR Manager's job title.

RECOMMENDED to Full Council that the revised Joint Staff Consultative Group Constitution, as attached at Annex A to this report, as amended, be adopted.

31/EC Work Programme

The Committee discussed its work programme for rest of the municipal year and agreed to add a review of the Annual Pay Settlement Procedure to the agenda for the next meeting.

It was also agreed to add an item on Christmas leave from 2023 onwards to the work programme, with a projected date for consideration in June 2022. An item

assessing whether to align future pay awards to the Medium Term Financial Strategy would also be added to the forward programme.

RESOLVED that the work programme for the remainder of the 2021/22 municipal year, as set out at Annex A to the agenda report, as amended, be agreed.

Chairman

Surrey Heath Borough Council
Employment Committee
6 April 2022

Information Security Policy

Strategic Director/Head of Service	Louise Livingston
Report Author:	Stuart Field, ICT Manager
Key Decision:	no
Wards Affected:	n/a

Summary and purpose

This report provides the Employment Committee with information regarding the Council's Information Security Policy which is an annual item on the agenda.

The policy has been amended to reflect:

2.5 inclusion of web browser
5.3 further information regarding personal and third party equipment
6.10 further information regarding remote access
9.2 Further information regarding storing documents and files

Recommendation

The Committee is advised to RESOLVE that that the revised Information Security Policy, as set out at Annex A to the report, be adopted.

1. Background and Supporting Information

1.1 The Information Security Policy is to be reviewed annually. If there is a need to change it before the annual review it will come back for recommendation sooner.

1.2 The proposed revisions to the Policy were considered by the Joint Staff Consultative Group at its meeting on 29 March 2022.

2. Reasons for Recommendation

2.1 The Information Security Policy needs to be kept under review and will be presented to the Committee annually unless there is a requirement to change it sooner.

3. Proposal and Alternative Options

3.1 The adoption of the Information Security Policy for the next 12 months when it is reviewed again unless it requires reviewing before this anniversary.

Annexes
Annex A - Information Security Policy

Background Papers
n/a

SURREY HEATH BOROUGH COUNCIL

INFORMATION SECURITY POLICY ~~v2021~~v2022

1. Message from the Chief Executive

Information is the lifeblood of the Council and is one of its most important assets. It exists in many forms, but a great deal of it now depends on Information and Communications Technology (ICT). There are many threats and risks to our information and we must do all we can to control them. All of us have a responsibility to play our part in ensuring the security of our information and systems.

All information which is produced on behalf of the council is its corporate memory and owned by the council.

The Information Security Policy sets the framework for protecting and securing our information assets in Surrey Heath Borough Council. This Policy will help to:

- Ensure that the personal privacy of our citizens is respected
- Ensure that organisational confidentiality is protected.
- Safeguard the information contained within our computer systems
- Reduce legal risk
- Reduce the risk of error, theft, fraud and misuse of facilities
- Provide guidance for our staff to make the best use of our systems
- Comply with Chapter II, Section 40 of the Data Protection Act 2018 'that data be processed in a secure manner'

We have many technical ICT elements in our approach to security – firewalls, anti-virus software, passwords and access control, back-ups and so on. They play an important role, but can be rendered useless if we do not all play our part. Writing a password on a piece of paper and storing in a drawer, downloading software which might damage the network, clicking on links in suspicious emails, logging staff onto the network using your own password or letting an intruder into the building without checking their credentials are just a few examples of how individual actions can create great damage.

I expect all Surrey Heath staff to be familiar with the essential elements of the Council's Information Security Policy and to ensure that they work within the guidelines that it contains.

Chief Executive

2. Introduction

The Policy is made up of a number of separate documents or sub-policies. They cover the rules and guidance which need to be applied by staff, managers, system administrators, ICT specialists and others. Some policies directly affect certain groups only, such as network administrators when they are doing network configuration and support.

This policy is not relevant to members as they do not connect to the Surrey Heath network. All ICT security and information governance for members will be referenced in the Constitution – part 5 Codes and Protocols – Section C – IT Code of Practice for Members

Any breach of this policy will be considered as a potential disciplinary offence.
In the absence of the ICT Manager, all incidents should be reported to the Executive Head of Transformation or the Corporate Enforcement Manager

There are regulations which affect all users with access to information. In order to comply we must ensure we manage our information effectively, taking into account any legal requirements. Below is a list of legislation which affects some or all services and are drivers for ICT security and Information Governance:

UK General Data Protection Regulation
Data Protection Act 2018
Lawful Business Practice Regulation 2000
Human Rights Act 1998
Freedom of Information Act 2000
Protection of Freedoms Act 2012
Environmental Information Regulations 2004
Regulation of Investigatory Powers Act 2000
Misuse of Computers Act 1990
Re-use of Public Sector Information Regulations 2015

All queries and comments relating to this policy document should be addressed to the ICT Manager.

3. Training and Awareness

It is important that staff attend scheduled training courses to ensure that they understand how to use the systems and software. Data protection training is mandatory. We need to satisfy ourselves, and our partners, that we have a comprehensive approach to Information Security

4. Responsibilities

All staff – to be aware of and apply the Information Security Policy and any related policies in their handling of information, whether or not using technology to do so.

Managers – to ensure their staff are aware of their responsibilities, and to prevent breaches within their service areas.

Network & Security Team – development and application of the policy and practices, and responsibility for the investigation and resolution for any identified or suspected ICT security incident.

Information Governance Manager, Data Protection Officer and Senior Information Risk Owner – for data protection and security breaches

ICT Manager and Information Governance Manager – custodian of the policy, and responsible for its updating, subject to appropriate consultation with and approval (as required)

2.0 Password Policy

2.1 Purpose and scope

The purpose of having a password policy for the organisation is to provide guidance on best practice when using passwords for all of our ICT Systems.

This policy applies equally to all users of ICT Systems at Surrey Heath Borough Council, including head of paid service, statutory officers, all permanent members of staff, temporary staff, contractors and third-party support companies. Good password practice should be applied to any system where a password is required.

2.2 Network user accounts

Each network user is given a unique user account and associated password to grant them access to the Council's computer systems. This password is unique to the user and must be kept confidential to that user.

2.3 Okta Single Sign on

Okta is an environment that links to your network account and enables a single sign on dashboard environment which makes it easy for you to log into your various applications. Once logged into Okta using your network password, users will be able to seamlessly log into each application displayed on their dashboard. The technology is designed to avoid the need for users to remember or write down lots of different passwords, and in so doing reduce the risk of unauthorised access to the network.

2.4 Application passwords

Each application is usually controlled with user identification and permissions to ensure users can only access appropriate areas of that application. Application access can be linked to your network login and automatically log a user in.

Older legacy applications will require a user to log in separately with a different password to their network password. This application password is unique to the user and must be kept confidential to that user.

2.5 User responsibility

It is the user's responsibility to protect their passwords from being disclosed to any other person. Under no circumstances should you reveal your password to a colleague, a member of ICT support staff or any other person that may ask for it.

Passwords **must** be kept confidential at all times. If a member of ICT support staff require access to a user's account to resolve a Service Desk call, they must, in normal circumstances, obtain written permission from the user (or line manager in the user's absence), and reset the password. Only in exceptional circumstances can

ICT reset a user password without permission. The password will then need to be reset once the support call has been closed.

Under no circumstances should you log someone else onto a system using your password.

Passwords should not be written down on pieces of paper, stored on sticky notes or stored in computer files, or saved within a web browser. ~~without password protection~~. This will be considered as a disciplinary offence. It is recommended that a user creates either a word document or excel spreadsheet and applies a memorable password. This should then be used to store all Surrey Heath passwords relevant to that user.

Passwords must not be inserted into or transmitted via email messages as these are not secure. Passwords will only be issued verbally on the phone to an actual individual if the issuer is certain of the user's identity. Passwords will normally be issued in person and the issuer will need to see proof of identify if the user is not known.

2.6 Temporary passwords

Temporary passwords must be changed immediately at first logon. Any password resets performed by the ICT Service Desk staff will be set to 'Force password change at next logon' as default.

2.7 Network password standards

Various security standards now suggest network passwords should be a minimum of 15 characters and users are encouraged to use a phrase rather than a single word with numbers and non-alpha numeric characters.

This new standard makes the password more difficult for hackers to penetrate.

Choose a phrase type password. Suggestions of phrases (but please do not use the suggestions below) could be:

- Barney_is_a_purple_d1nosaur
- Pouring rain is all we need!
- London_bound_City_break
- Wear_a_Sunhat_in_sunny_weather!

The combination needs to be at least 3 of the following 4 categories, and you can use spaces.

- Uppercase
- Lower case
- Numbers (0 through to 9)
- Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces e.g. ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/

The password must NOT contain your login name.

2.8 Past passwords

The last 20 Network passwords are remembered by the system. This prevents passwords being repeatedly reused. It is bad practice to alternate between two passwords each time a password change is required.

You have up to 3 login attempts before your account is locked. You will need to wait 5 minutes before you try again, or contact the ICT Service Desk to have the account unlocked.

2.9 ICT Passwords and 1Password

Members of ICT who have administrative access to applications or servers should only use the 1Password application for their storage. This will ensure passwords are secure and accessible for other members of the team if required.

It also ensures passwords are available and accessible in a disaster recovery scenario where building access has been lost.

2.10 Misuse of passwords

Any member of staff found to be attempting to gain access to systems without permission including but not limited to, guessing, cracking or attempting to coerce other staff members to give up their password will be subject to disciplinary proceedings.

2.11 Passwords for documents

If a document contains confidential or sensitive personal data it must be password protected or stored in a secure location within Box.

2.12 Browser use on shared devices (such as standalone loan laptops and shared logins to training room PCs and meet & greet etc)

If you use a web browser to access services such as email accounts, social media or any other service which require login credentials (username and password) you must use an incognito (private) mode browser window.

Failure to do this could result in your accounts being left signed in and other users gaining access to your accounts.

3.0 Starters, Change of access and Leavers Policy

3.1 Purpose and scope

This policy clarifies the requirements for making changes to User Access Rights or Privileges for any of the Council's ICT systems. It covers new starters and leavers procedures, and change of job roles resulting in change of permissions

This policy applies equally to all users of ICT Systems at Surrey Heath Borough Council, including head of paid service, statutory officers, all permanent members of staff, temporary staff, contractors and third-party support companies.

3.2 New accounts and system access

New account registration requests should be submitted to Human Resources who require time to carry out the appropriate security checks according to the role. Once Human Resources have completed their checks, ICT Service Desk requires four working days to create the account and system access prior to that user being issued with connection details.

New account requests must be authorised by the Human Resources Team and the line manager of the new member of staff.

Requests should be logged on the ICT Service Desk system. This raises a call with the Service Desk that is used to maintain and record all new user requests.

3.3 Name changes

Name change requests should be logged with the ICT Service Desk

3.4 Job or role change

If a network user changes role or job within the council, the permissions and system access should be reviewed and where possible cleared and re-created for the new role. This prevents inappropriate permissions being inherited from one role to another. It is the responsibility of a network user's line manager to log a call on the ICT Service Desk System to advise ICT of the change of user role, failure to do so will be regarded as a serious breach of security.

All system administrators and ICT staff that are responsible for making changes to user permissions on any of the Council's ICT systems must complete the following processes each time a permission change is made:

- The call will generate a sign off request for the Executive Head who has the necessary authority to authorise the required change on that system. Once the authority for the change has been granted the actual work on changing permissions can proceed. No changes will take place without sign off being received.

- Authorisation details should be recorded in the journal for the Service Desk call. If the change request was logged by a system administrator, they will be notified when the sign off has been received from the system owner and the call updated on their behalf. It is then the system administrator's responsibility to update the service desk with details about the permission changes once complete. The ICT Service desk can then close the call with all the relevant information relating to this Permissions Change Request

- Northgate Iworld, Northgate Information@Work and Civica Financials user access is controlled by System Administrators who are non ICT staff. The above procedures also apply to these System Administrators.

3.5 GSi Convergence Framework (GCF) Network access

The GCF Network is a Cabinet Office controlled program providing an accredited and secure network between public sector organisations.

Users who require access to receive GCF services via the Public Sector Network should submit a request through the ICT Service Desk.

All new starters, including temporary and contract staff, will be subject to appropriate security checks according to the role through the Human Resources team.

The User's Human Resource file will be checked for a copy of a 10 year passport or 2 of the following documents:

British driving license
Form P45
Birth Certificate
Proof of Residence i.e. council tax or utility bill

If these documents are not currently on file, they will need to be provided in order for the account to be created.

Once Human Resources are satisfied that the appropriate checks have been made, they will instruct the ICT Service Desk to create the GCF access.

3.6 Account closure

It is the responsibility of the network user's line manager and departing member of staff to make suitable arrangements for important work, related documents and email to be made available for others to use in the future **prior** to the termination of a member of staff's employment. It is important that the corporate memory of the Council is preserved.

It is the responsibility of the departing member of staff to delete or transfer work related electronic files that are stored in their email folders or their H:\ drive or Box drive prior to the termination of their employment. They must make arrangements to delete or transfer personal data to a suitable medium before they leave. Further advice can be provided by ICT Services.

Once a line manager is aware that a member of their staff is leaving the employment of the authority, steps should be taken to deal with any required work related email,

information or electronic computer files that have been stored by that employee in their personal areas such as their email folders or their personal document storage. Arrangements must be made between the manager and member of staff to move these documents to either a suitable shared area or to a colleague or line manager's folder. Any requests must be made within 4 weeks following the leaver's last working day, at which point the emails and files will be removed from the network. CMT email accounts will be kept for 6 years after they have left. Emails and documents created by a user are the property of the council and should be available for others to use after someone leaves.

The leaver's personal folder in Box will be moved to a 'Leavers' folder. All content in the Leavers folder is subject to an automatic retention policy and will be **deleted** after 3 years from being moved into this folder.

It is the responsibility of the line manager to log a staff leaver request using the ICT Service Desk system **in advance** of the network users leave date where possible.

The ICT Manager will review all active users on the network every 6 months.

The ICT Manager will also circulate a leavers report initiated from the HR system every month end identifying any leavers in the previous month. This will be circulated to the ICT Service Desk, Application Support Team, Financial Services and Revenues and Benefits to ensure all leavers have been removed/inactivated from the network and applications – this is a fall back process only. Any leavers identified as still active on the network will be notified to the Executive Head of Transformation and the relevant Head of Service responsible for the line manager who failed to notify ICT. Any breach of this rule will be treated as extremely serious due to the impact a leaver remaining on the network could have on the security of council services.

It is the responsibility of the leaver's line manager to return the leaver's security pass and any provided equipment to the ICT Service Desk on the leaver's last working day. This includes, but is not exclusive to, encrypted memory sticks, laptops, iPads and mobile phones.

When a member of staff leaves the employment of Surrey Heath Borough Council ICT, a risk assessment must be carried out by the ICT Manager as to whether it is necessary to reset administrator network and application passwords.

3.7 Network access for visitors and temporary staff including agency staff and work experience students

Under no circumstances should anyone be given access to the Surrey Heath network without having read and signed an agreement to adhere to the Surrey Heath Information Security Policy.

3.8 Work Experience students

Students must under no circumstances be left with unsupervised access to the council's network.

Please refer to the Work Experience policy for further guidance

3.9 Suspension of accounts

It is the responsibility of the Human Resources Department to immediately notify either the ICT Manager, a member of the Network & Security Team, or ICT Service Desk Team should it be deemed necessary to suspend access for any user of the Surrey Heath network. Once notified, ICT will inform appropriate team members to ensure the account is not re-enabled in error. This is particularly relevant in a redundancy or disciplinary situation.

3.10 Building Access

Each member of staff will be issued with their own unique identification security pass on their first day of service containing a photograph and employee name. This will allow building access to restricted areas within restricted time zones. Passes should be visible at all times, particularly when entering through secure doors.

Employees must keep passes secure at all times and be able to account for it, particularly when outside of the office.

Non authorised personnel should never be allowed to pass through a secure door. It is the responsibility of all employees and tenants of Surrey Heath House to challenge anyone attempting to tail-gate.

If a pass is lost, the ICT Service Desk must be notified immediately so that the pass can be inactivated.

If a pass is forgotten, a temporary pass can be issued from the ICT Service Desk, but must be returned the next time that employee is in the office. Temporary passes not returned will be disabled.

Temporary passes can be issued to visitors under certain circumstances. A permanent employee will be required to sign for the pass to agree to take responsibility for the return.

4.0 Patch Management Policy

4.1 Purpose

This policy exists to define the patch management to create a consistent configured environment that is secure against known vulnerabilities in operating systems and software.

The Patch Management Policy covers Workstations and Servers, applications and operating systems.

It is the responsibility of the ICT Manager, Network & Security Team, Application Support and ICT Service Desk to ensure that our technology environment is up to date with current patches.

4.2 Windows Server Update Service (WSUS) Patch Management

WSUS server connects to the Microsoft service periodically and downloads all available updates for onsite servers.

Although Microsoft carry out extensive testing for all patches, it is vitally important only to deploy updates which are relevant to the Council's particular environment, as any changes through patches can have a detrimental effect on other applications or systems.

The Network & Security Officers will review and schedule the patches to be applied to each server if required, preferably outside of normal office hours to avoid disruption to users. Any updates which are later found to cause problems with selected users or applications can be automatically recalled and uninstalled centrally.

Cloud based servers will be patched by the member of ICT who administers the server if this is not managed by a Supplier.

A record of all updates downloaded and tested and deployed will be kept by the Network & Security Officers.

A log of all withdrawn updates will be kept by the Network & Security Officers.

A log of all available patches not deployed will be kept by the Network & Security Officers.

All logs are to be made available on request by the ICT Manager for audit purposes.

4.3 Workstations

All desktops and laptops are patched at least monthly. As Microsoft patches are released, a test machine is initially patched and tested.

A desktop image management tool is used to automatically roll out the latest desktop patch releases. Laptop updates are managed and updated through an endpoint management solution.

Once the test patch is signed off, the image management tool is used to roll out a layer to a test group of machines for a few days of testing.

If no issues arise the remaining suite of desktops and laptops are patched automatically.

Patch releases are monitored regularly by the Network & Security Officers. If an urgent patch is available, this will be prioritised and installed immediately.

4.4 Application Software

Patches to application software by third parties will be managed by system administrators, the Application Support team or the ICT Service Desk.

Any application patches and upgrades will be loaded onto the test system where available in the first instance, and when fully tested by users, will be copied onto the 'live' system. Any updated application software found not to be compatible with the 'live' system will be removed and the software rolled back to the previous release.

Cloud based applications will normally be patched by the third party supplier as detailed in the relevant contracts.

4.5 Cloud Services

It is essential, where cloud services are employed (particularly with respect to IaaS and PaaS), that the Network and Security Officers are absolutely clear (whether through contractual agreement or other arrangements) whether the responsibility to carry out certain actions (ie patching) lies with the team or the cloud supplier. Note that in the case of an audit or site visit you can expect Public Sector Network team assessors to check this.

If you are using cloud services: Cloud Security Principle 5.3 *Protective Monitoring* should be factored into your overall monitoring strategy. Note that a cloud service will only provide monitoring with respect to the service provisioned. If you consume Infrastructure as a Service (IaaS) or Platform as a Service (PaaS), you are responsible for monitoring of capability deployed onto the infrastructure. If you are consuming Software as a Service (SaaS), you should consider how you will be able to monitor for any potential abuse of business process or privilege.

5.0 Virus and Malicious Software Management Policy

5.1 Purpose and scope

The purpose of this policy is to help protect council computer systems and networks from the threat of Viruses and Malicious Software.

This policy applies equally to all users of ICT Systems at Surrey Heath Borough Council, including head of paid service, statutory officers, all permanent members of staff, temporary staff, contractors and third-party support companies.

5.2 What is a virus or malicious software?

A computer virus or malware is malicious computer software designed to disrupt, corrupt, delete or obtain information for improper purposes. Viruses have the potential to spread in a very short time as they take advantage of computer networks and electronic mail systems to replicate quickly, sometimes before anti-virus vendors have produced updates for their software.

Viruses have traditionally been transmitted by email often using spoofed email addresses to make the email look like it is from a legitimate source.

Viruses and malware can be activated by visiting infected web pages, opening attachments in emails, running macros in office documents, installing unauthorised software and transmission of data using CD/DVD's, USB memory sticks, memory cards and any other form of portable media. You should be aware of the risks when using any of the above. This policy provides advice and best practice in these areas.

5.3 Personal and third party equipment

Only authorised computers provided by ICT Services with the relevant security software loaded on them are permitted to be connected directly to the Council's computer networks. Under no circumstances should non Surrey Heath equipment be connected to council networks without prior written permission from the ICT Manager. Any breach of this rule will be treated as extremely serious due to the impact a virus on the network could have on council services and noncompliance with code of connection agreements to the Public Sector Network.

Remote access to the Surrey Heath network is only acceptable with non-Surrey Heath equipment for ICT support contractors and ICT staff for remote support, or other staff using authorised access through the Watchguard portal or Azure Virtual Desktop. All data must remain with the Surrey Heath network and/or Cloud Services and must not be downloaded directly to a non-Surrey Heath device.

5.4 Anti-virus software

ICT Services install anti-virus software on every PC, server and laptop computer that is used on the Council's computer networks. This software is installed before a machine is issued by ICT Services and is configured to automatically update with virus definitions from a central server on a regular basis. This software is installed to

protect the PC and the Council's computer networks, systems and users. It takes only one weakness in the security infrastructure to cause serious problems for a large number of staff.

The anti-virus software that the Council uses performs real-time scanning that will look for viruses whenever a computer file is accessed. Users should still be vigilant when opening files especially if they are from a third party organisation. If users suspect they have opened a suspicious email they must contact the ICT Services Desk immediately.

Users must not under any circumstances alter the settings or configuration of the anti-virus program.

5.5 Email scanning

The Council uses an email scanning service that scans incoming and outgoing email traffic for all Surrey Heath Borough Council email users. This system filters out viruses that are attached to electronic mail messages. It is important to note that this system captures a large number of viruses but there is still the potential for viruses to slip past this system, so vigilance when opening emails is still very important. The key message is to never click on links or attachments to emails where you do not know the originator, or the content may look suspicious. Always contact the ICT Service Desk if you are not sure.

As well as the anti-virus scanning service, the Council also use a system that scans incoming and outgoing email for SPAM and improper content. SPAM, amongst other things, is used to launch phishing attacks. Some emails attempt to trick people into revealing confidential information that could then be used for fraudulent purposes or for an attack on an organisation. If a user suspects a phishing attack they should contact the ICT Service Desk immediately for advice.

6.0 Physical and Environmental Security Policy

6.1 Purpose and scope

The Council requires that physical access to ICT equipment shall be controlled in an adequate manner to provide reasonable protection against theft, damage, loss, or misuse.

The policy covers the use of any ICT equipment that is owned by or provided by Surrey Heath Borough Council. It is applicable wherever that equipment is being used, whether in a Council workplace, off-site or in transit between work locations.

This policy applies equally to all users of ICT Systems at Surrey Heath Borough Council, including head of paid service, statutory officers, all permanent members of staff, temporary staff, contractors and third-party support companies.

6.2 Physical Access Controls

General access to buildings should require appropriate levels of control.

Physical access to all areas except the contact centre and public areas in Block B of Surrey Heath House will be controlled by a door entry swipe card system. Swipe cards are issued to staff, tenants and some visitors via the ICT Service Desk. Staff and tenants should display their identity pass at all times whilst in the secure areas. Staff and tenants should be mindful of tailgating and challenge or be prepared to be challenged if not displaying an appropriate pass.

All visitors will be escorted to and from the area/person they are visiting, and must report and register at main reception each day and clearly display a visitors pass whilst in the restricted areas

Network computer equipment will be housed in a controlled and secure environment with restricted access to essential ICT and Security staff only, using entry controls. No unauthorised access should be given and suppliers or contractors requiring access to this equipment should be supervised wherever possible.

6.3 Manual workstation lock

To ensure network accounts are not misused, it is a mandatory requirement when leaving your workstation to lock the screen to prevent unauthorised access to your computer and work. Under no circumstances should you leave your workstation unlocked with unsupervised access to the network to another person. The only exception to this would be for a member of ICT or a supplier who is trying to resolve a support call.

This is a simple process of pressing and holding down the Ctrl+Alt keys and then pressing the Del key, this will bring up the Windows Security box on screen where you can then press Enter or click on ‘Lock Computer’ to lock your workstation.

A quicker option is to hold down the Windows Key and press the ‘L’ key. This prevents anyone tampering with your computer whilst you are away from your desk.

6.4 Automatic workstation lock

The network also has an automatic policy that locks user’s systems, as discussed above, after a period of 7 minutes of inactivity. All staff must manually lock their own system when they leave their desk as there is still a window of 7 minutes where misuse could occur. The automatic workstation lock should not be removed or changed.

6.5 Laptop & Mobile equipment

Users of laptop & mobile equipment are responsible for the security of the hardware and the information it holds at all times. The equipment should only be used by council officers to whom the equipment is issued, equipment must not be transferred to other users in the council without express permission of the ICT Manager. Family members and friends are not permitted to use council issued ICT equipment.

All mobile devices issued to officers by ICT are enrolled and managed by an endpoint solution. This provides the ICT team with oversight of these devices so they can monitor endpoint security and provide support. If a device falls out of compliance a notification email will be sent to the officer the device is issued to. It is the duty of the officer to contact ICT should a notification email be received. If a device remains out of compliance for an extended period, the device will be wiped and will need to be returned to ICT to be reconfigured.

ICT require the return of any managed devices should a member of staff be away from work for an extended period.

Passwords should never be stored with the device.

When travelling in a car with portable equipment the following must be adhered to

- must be kept in the locked boot of the car and out of sight if it is essential to leave it unattended at any time.
- must not be left in a car overnight
- if it is stored at home it must not be left on display

When travelling, be careful what is displayed on the screen. Do not look at any confidential or personal information which others could see.

Laptop & mobile equipment must not be left unattended in public places.

Do not discuss confidential or personal information on SHBC devices in public

As outlined in the mobile device agreement form, the ICT team need to be notified immediately should a device be lost or stolen. ICT reserve the right to turn on tracking of council devices when reported lost or stolen to aid with device retrieval.

6.6 Equipment installation

ICT Equipment must always be purchased, tagged and installed by, or with the permission of the ICT team.

Under no circumstances should ICT equipment be moved by non ICT staff unless it is portable equipment.

If a user requires equipment to be relocated it should be pre-arranged by logging a call with the ICT Service Desk.

All software must be purchased through and installed by the ICT Service who maintains a central record for licensing purposes. All software media will be retained by the ICT Service to ensure it is correctly licensed, installed, used and available for business recovery purposes. No unauthorised software must be installed on any Council equipment.

Instant messaging is limited to corporate supplied applications. Non-corporate supplied services must not be installed or used on Council provided computers, unless there is a specific work requirement to do so.

Approval of any such installation shall be subject to the prior written approval of the ICT Manager.

6.7 Equipment and media disposal

All PCs, laptops, tablets, digital cameras, mobile phones and the like, and any other form of ICT equipment that has the capacity to store data in any form must be returned to the ICT Service for proper disposal. There is a risk of a data breach if these devices are disposed of before data has been properly removed or wiped.

Electrical device disposal should be compliant with WEEE legislation.

6.8 Return of equipment

All equipment and software provided by the Council remains the property of the Council at all times and must be returned before leaving the Council or when it is no longer required.

6.9 Network Availability

Access to the computer network is available during normal office hours 08:00 to 18:00 Monday to Thursday and 08:00 to 17:30 Friday. Access outside of these times cannot be guaranteed due to essential maintenance that might be taking place.

The ICT Manager, Network and Security Manager and Executive Head of Transformation reserve the right to take down any part of the ICT network without prior agreement to carry out urgent essential maintenance as deemed necessary.

6.10 Remote access

By default access to your Surrey Heath provided account outside of the UK is restricted. Should there be a business requirement for access whilst abroad, a request will need to be raised via Freshservice. Requests are reviewed on case by case basis and are subject to approval by ICT Management.

Okta

Staff are encouraged to use the Okta portal for remote access
https://surreyheath.okta.com

The Okta portal allows access to email, Box, Freshservice and other systems without requiring additional passwords. Please use your existing Surrey Heath email address and password to login, for remote access you will also be promoted for Multi Factor Authentication (The ICT Service Desk will be able to provide further advice on this). Certain Okta integration will require the install of an Okta browser plugin, please follow the prompts to install this if required. The ICT Service Desk is unable to provide support on non-Surrey Heath equipment but can provide user notes for assistance.

Watchguard Access Portal

Staff are able to access internal systems via the Watchguard Access Portal. Please login to Okta
(https://surreyheath.okta.com)
using your email address and network password. Multi Factor Authentication will be required for remote access. (The ICT Service Desk will be able to provide further advice on this). From the Okta dashboard click Watchguard Access Portal and click the resources you need to access entering your network credentials when prompted. Whilst there isn't a need for additional software to be installed we would encourage the use of a modern browser for access. If you don't see a Watchguard Access Portal icon in Okta please raise a request via Freshservice where they will be happy to assist within normal service level agreement timeframes. The ICT Service Desk are unable to provide support on non-Surrey Heath equipment but can provide user notes for assistance.

Azure Virtual Desktop

Staff are able to access internal systems via Azure Virtual Desktop where available. The Virtual Desktop software is automatically deployed to Intune managed laptops where access is required.
For further information on Azure Virtual Desktop please contact the ICT Service Desk.

6.11 Third party access

It is the responsibility of all users requesting or obtaining Third Party Access to comply with this policy.

Third party access to the Surrey Heath network may be made for Surrey Heath Borough Council administrative or support purposes only. The preferred access provision will be by the creation of a network account for that third party with remote access coming through the staff portal. In certain circumstances it may be necessary for the supplier to be given direct access using on-demand collaboration tools such as TeamViewer or Webex. These tools must never be used on the Surrey Heath network without prior authorisation from the ICT Manager or Network and Security Manager due to the security risk this type of connection can create to the network.

Access Requests

Requests to allow access to the Surrey Heath network or attached devices must meet the following criteria:

(a) Requests for third party access must be formally requested by logging a call on the ICT Service Desk and obtaining approval from the ICT Manager.
(b) The requestor must then complete and sign the SHBC Third party access request document.
(c) The originator of this Service Desk call will act as the sponsor for the Third Party. Where there is an approved need for third party access, security controls will be agreed and defined in a contract with the third party as detailed in Third Party Remote Use Agreement.

Access to the Surrey Heath network facilities by third parties will not be provided until the above has been actioned and approved.

Third party access must be permitted only to the facilities, services and data, which are required to perform the specified tasks, as outlined by the System Administrator in the original request for access.

The purpose of the third party access must be outlined by the System Administrator.

Once the work has been completed, the supplier must contact Surrey Heath ICT to confirm the work has been completed. Surrey Heath domain account administrators will then disable access and logging a Service Desk call.

Third Party Remote Use Agreement

Please refer to the Third Party agreement that must be signed by all third parties prior to access being given.

Confidentiality

Where third parties have direct or indirect access to data or information owned by Surrey Heath Borough Council, this information must not be divulged or distributed to anyone. Documents which contain personal information including but not limited to names, addresses or telephone numbers, medical records, financial records of Surrey Heath Borough Council must be carefully controlled and must not be released or disclosed to any unauthorised individuals or sources. It may be necessary to have a data sharing agreement in place, prior to this third party access. Please contact the Information Governance Manager for advice.

Unique Supplier Authentication

In order to ensure individual accountability on Surrey Heath network devices and applications, all third parties at a supplier level granted access must be given a unique user-id and password. The Third Party will at all times be held responsible for any activities which occur on Surrey Heath Borough Council networks and applications using this unique user-id. The Third Party is solely responsible for ensuring that any username and password that they are granted remains confidential and is not used by unauthorised individuals.

Host Security

When a Third Party is logged into the Surrey Heath Borough Council network, they should not leave the host they are logged onto unattended. Workstations/laptops that are used to display Surrey Heath data must be located in such a way that confidential information is not displayed to unauthorised persons or the general public. Up-to-date Virus checking software must be installed on any relevant devices that are being used to access the Surrey Heath Borough Council network or attached devices.

6.12 Virtual Private Networks

Certain applications may require a virtual private network configured to enable the software to function correctly.

If a virtual private network connection is required, an agreement contract should be made with the third party to ensure the security of the Surrey Heath network and to meet Public Sector Network connection requirements.

7.0 Internet Usage Policy

7.1 Purpose and scope

This policy is to provide guidance on acceptable internet use whilst connected to the Surrey Heath network.

7.2 Use

Internet services are provided by the Council for use in the performance of the Council's services. As a general rule, staff should use Internet technologies and services only in the execution of their official duties and tasks.

Occasional, limited and responsible private use is permitted subject to compliance with the particular rules given below.

Users are not permitted to subscribe to chargeable services on the Internet without the specific authority of the Executive Head responsible.

This policy applies equally to all users of ICT Systems at Surrey Heath Borough Council, including head of paid service, statutory officers, all permanent members of staff, temporary staff, contractors and third-party support companies.

7.3 Misuse

The following actions will normally amount to misuse of the Internet and breach of this policy:

- creating, circulating, distributing, storing, downloading or intentionally viewing material which is offensive, obscene, sexually explicit, pornographic, racist, defamatory, hateful, which incites or depicts violence, or describes techniques for criminal or terrorist acts, or which otherwise might bring the Council into disrepute or expose it to legal action.
- using the Internet for purposes that may be illegal or contravene Council policies (such as disclosing personal information in contravention of data protection legislation).
- political lobbying or private business, taking part in discussions on matters which are politically controversial, whether nationally or locally, or giving advice or information known to be contrary to the Council's policies or interests.
- breaking through security controls, whether on the Council's equipment or on any other computer system.
- accessing Internet traffic (such as email) not intended for the user, even if not protected by security controls, or doing anything which would adversely affect the ability of others to access Internet resources they are entitled to access.
- intentionally or recklessly accessing or transmitting computer viruses and similar software, or intentionally accessing or transmitting information about, or software designed for, breaching security controls or creating computer viruses.
- any activities which could cause congestion and disruption of networks and systems.

- any illegal activity

7.4 Copyright

Copyright laws apply to any copyrighted material accessed or sent through the Internet. Copyright infringement can occur through downloading files from the Internet or where text is copied into or attached to an email message.

Users must not transmit copyright software from their computer to the Internet, or permit anyone else to access it on their computer via the Internet.

Copyright and other rights in all messages posted to the Internet from a Council account, like other material produced at work, belong to the Council, and not to users personally.

7.5 Provision of Access

Internet access may be withdrawn for breaches of this policy or at the discretion of the employee's Executive Head.

7.6 Personal Use

Occasional, limited and responsible private use is permitted subject to managerial approval and compliance with this policy.

Personal use of the internet should normally be undertaken outside working hours.

Downloading of music or video files is not permitted except for Council-related purposes.

Printing from the internet for personal use is not permitted.

8.0 Secure Data Transfer Policy

8.1 Purpose and scope

This policy protects data which is being electronically transferred to or from Surrey Heath Borough Council ICT systems internally or externally. This policy must be applied to any sensitive or personal data being transferred by electronic means. Transfer of non- electronic sensitive or personal information is not covered by this policy and advice should be sought in advance from the Information Governance Manager.

No data containing personal or sensitive information should be made available or transferred outside of the Surrey Heath Borough Council ICT Systems without a data sharing agreement or approval and advice from the Information Governance Manager. This includes forwarding of data to a non Surrey Heath email account.

This policy applies equally to all users of ICT Systems at Surrey Heath Borough Council, including head of paid service, statutory officers, all permanent members of staff, temporary staff, contractors and third-party support companies.

8.2 Physical security

ICT systems, infrastructure and media should be protected from inappropriate access in accordance with the Information Security Policy. Particular care must be made to ensure that portable systems and media containing sensitive or personal data are secure. Any loss of ICT hardware should be reported to the ICT Service immediately and any suspected loss or inappropriate access of sensitive or personal data should be reported to the Information Governance Manager and your line manager immediately. Media used for data transfer must be adequately protected during transit with encryption and passwords. Further advice can be provided by contacting the ICT Service Desk.

8.3 Electronic security

Sensitive or personal data being stored on media for transfer or sent electronically across a network must be protected. The appropriate type of protection should be determined in consultation with the ICT Service. Contracts with third parties must contain clauses to protect data. Advice should be sought in advance from Legal Services and the Information Governance Manager when third parties are acting as ‘data processors’ as defined in the General Data Protection Regulation. Typically, data should be password protected and encrypted. The possible forms of protection are dependent on the type of data, location, size, recipient, sensitivity and other constraints so it is not possible to have a single solution for all needs, but if it contains personal or sensitive personal data it must not be accessible to others if it inadvertently falls into the wrong hands.

Increasingly, the majority of information which is not stored in business database system such as Uniform or Civica Financials now resides in Box. There are tools in the Box platform which enable you to securely share content with other staff members, other departments or people external to the organisation. Usually, if you

have content you need to share externally you will be advised by ICT to make use of these features in Box. Box sharelinks can be password protected and you can also disable them manually and set an expiry date on the sharelink after which it will be deactivated.

Cloud computing – No Surrey Heath data should be stored outside of the European Economic Area unless that country ensures an adequate level of protection approved by the Information Governance Manager. You must not sign up to any cloud computing systems which would store potentially sensitive information without the ICT Manager's authority File hosting services such as Dropbox, Microsoft Onedrive and Google Docs should not be used for transferring sensitive or personal Surrey Heath data.

8.4 Media

Only hardware provided by or approved by the ICT Service may be used for data transfer. Hardware sent to third parties should be verified clean and empty before it is used (preferably new stock). The recipient must either return the hardware after use or have in place an appropriate disposal regime. This must be checked in advance of data being sent. An audit should take place if it is expected the recipient is to destroy the information.

Electronic storage devices that have been used on non-council computers represent a significant security risk to the Council and its ICT systems. Only removable media supplied by the ICT Service should be used with Surrey Heath Borough Council systems. It is **not** acceptable to introduce non Surrey Heath memory cards, USB storage devices or any other electronic storage device onto any Council computers unless permission to do so has been sought from the ICT Manager. A valid business case will be required to obtain this approval. In the majority of cases you will now be advised by ICT to utilise sharing features in Box as per 8.3 above if you need to share content or data.

Media should be password protected with passwords being issued to the recipient once confirmation of receipt has been received. Under no circumstances should passwords be sent with the media.

Media received from third parties or returned by third parties must be virus checked before use. Media received from third parties should be disposed of in accordance with this security policy.

8.5 Email

Email is not a secure form of transfer. Any sensitive or personal data transferred by email must be protected. The appropriate type of protection should be determined in consultation with the ICT Service. The email management policy within this Information Security Policy and the Email Management Procedures available on the Information Governance pages of the intranet provides policy and guidance on using emails as a form of communication. Typically, data should be password protected, encrypted and zipped. The possible forms of protection are dependent on the type of data, location, size, recipient, sensitivity and other constraints so it is not possible to have a single solution for all needs. Passwords to access emailed data should be sent under separate cover or by other means (e.g. by post).

Transportation

Transportation must be appropriate to the purpose. The Post Room can provide assistance with postage and couriers.

Government Secure Email

Central and Local Government organisations must follow the guidance for their secure email service to be considered secure by the rest of government. Further information about this facility can be obtained from the ICT Team

Protective marking

Where appropriate, the National Protective Marking Scheme classifications should be used. This provides for unclassified information and 3 levels of classification Official, Secret and Top Secret. In most cases local government information will fall into the lower category of UNCLASSIFIED. It is not necessary to mark each document/email if it is official. If it contains sensitive/personal information you may wish to classify it Official – Sensitive in the subject field of the email.

Processing of Credit/Debit card payments and PCI compliance

Credit/Debit card numbers must never be written down or transmitted by email or other insecure, online method (chat, instant messaging etc.), including internally. When processing a 'customer not present' card transaction, an employee may only enter the card information directly into the Surrey Heath payment form as the payee provides the information.

Point of sale devices must only be accessed by authorised employees who require access as part of their job.

All receipts containing credit/debit card transaction information must be stored in a secure location.

In the event of a compromise to customer credit/debit card numbers or to the card processing device, you must immediately follow the Surrey Heath Data Breach Policy and contact the Information Governance Manager.

Formal training must take place for all relevant employees to teach them about security as it relates to credit/debit cards, paper with credit/debit card numbers on them and the devices that process credit card transactions. It is the responsibility of the Information Governance Manager and Senior Information Risk Officer to ensure this training takes place. The Information Governance Manager must be informed if a new person is allowed to take PCI payments.

Call recording must be paused whilst taking credit/debit card details over the telephone.

9.0 Data Storage Policy

9.1 Purpose and scope

The purpose of this policy is to help to protect Council data by providing guidance on best practice for storing data on council computer networks and systems, it should be read in-line with the Records Management Policy.

This policy applies equally to all users of ICT Systems at Surrey Heath Borough Council, including head of paid service, statutory officers, all permanent members of staff, temporary staff, contractors and third-party support companies.

9.2 Storing documents and files

The majority of documents and files stored by the Council should be within the Surrey Heath Borough Council Box environment. Each user will be provided with a team environment and a personal environment within the Box platform.

Data is a corporate resource and therefore should be available to colleagues if required. Please do not store any corporate data or files locally on the C:\ drive of your PC or within your Azure Virtual Desktop profile.

Documents should be stored either in your personal folder in Box or within your team's Box folder or other Box folders that have been collaborated with you. Please remember that Box administrators within the ICT team retain access to all content across the Box platform. Staff hold responsibility for their data stored in Box. If you accidentally delete data you have 90 days to recover it. After the 90 day period data is not recoverable as the ICT team do not back up this data. Please be aware that we do have systems in place in the Box environment to monitor anomalous user behavior such as large volumes of data being deleted etc.

Network drives are backed up on a daily basis , so recovery of essential data is possible. Local drives on computers and laptops are not backed up, therefore if the computer disk fails; the work stored on it will be lost.
Where possible work files and documents should be stored on structured workgroup shared box folders where colleagues can access work in your absence.

Personal documents should be stored on the users personal Box folder which is provided for you when your Box account is created. Please do not rename this personal folder. Any personal data stored on the corporate network must be Surrey Heath related.

Non Surrey Heath related data(images and files) must not be stored on the Surrey Heath corporate network,Surrey Heath hardware or Surrey Heath cloud services.

USB drives / memory sticks and other removable media
Electronic storage devices that have been used on non-council computers represent a significant security risk to the Council and its ICT systems. Only removable media

supplied by ICT Services should be used with Surrey Heath Borough Council systems. It is not acceptable to introduce non Surrey Heath memory cards, USB storage devices or any other electronic storage device onto any Council computers unless permission to do so has been sought from the ICT Manager. The majority of Surrey Heath networked computers have the USB drives restricted in use to help maintain the security of the network and data.

All removable media supplied for use with ICT systems must be returned to ICT Service Desk for clearing or disposal when no longer required.

ICT Service Desk will provide encrypted memory sticks when data is to be transferred from the council network. (Please reference 8.3. On most occasions where you need to share data externally you will be advised by ICT to use sharing tools in Box) Authorisation and guidance for this must be obtained from the ICT Manager or Information Governance Manager.

All USB sticks must be issued with a password and recorded against the asset in the asset register maintained by the ICT Service Desk.

Printed material
Confidential information, including information containing personal data, must not be put in bins or left unattended, including at the time of printing. It must be shredded or placed in the confidential waste bins as soon as possible or certainly by the end of the day. Shredders are located on all floors. If there is a lot of shredding, the facilities team can provide confidential waste sacks. Facilities Team must be notified when the bags are full and collected by the end of day. Facilities team must shred them immediately or as soon as possible, but the bags must not be left unattended for others to access. To ensure that no confidential waste is put into waste bins, spot checks will be carried out.

10.0 ICT Procurement Policy

10.1 Purpose and scope

The purpose of this policy is to provide guidance on the procurement of any ICT related software or hardware to ensure any specification meets the Surrey Heath digital strategy and that relevant procurement rules are followed. This relates to new software or hardware, upgrades or replacement products.

This policy applies equally to all users of ICT Systems at Surrey Heath Borough Council, including head of paid service, statutory officers, all permanent members of staff, temporary staff, contractors and third-party support companies.

10.2 Procurement

Any software or hardware should be procured through the ICT team by contacting the ICT Service Desk in the first instance.

A representative from the ICT team should always be present at any software or hardware demonstrations.

Before proceeding with any software procurement in excess of £5000, including new implementation or upgrade, the relevant service area needs to complete a business case, identifying resource implications, costs and benefits. This must be presented to the Transformation Action Group for approval.

If any software or hardware to be procured will involve the processing of personal information a Data Protection Impact Assessment (DPIA) must be completed before proceeding to assess any risk to privacy of the data subjects and ensure compliance with Data Protection Legislation. The Information Governance Manager should be consulted in the first instance to ascertain if a DPIA is required.

10.3 Cloud software

Any cloud software procured must have a cloud security principal assessment which is documented to demonstrate due diligence prior to any contract being signed. https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles

The assessment should be completed jointly by the service and member of the ICT Service.

11.0 Email Management Policy

11.1 Purpose and scope

The purpose of having an email management policy is to manage the lifecycle of an email from creation to destruction. There are a number of rules and procedures that we need to follow in order to manage email accounts professionally and in line with our customer care standards whilst considering regulations such as The General Data Protection Regulation and the Data Protection Act 2018.

This policy applies equally to all users of ICT Systems at Surrey Heath Borough Council, including head of paid service, statutory officers, all permanent members of staff, temporary staff, contractors and third-party support companies. Any email stored on the Surrey Heath Email Exchange service is the property of Surrey Heath Borough Council and forms part of Surrey Heath's corporate memory.

11.2 Using emails

Email messages can often be misunderstood or misinterpreted and you must take every care to ensure you don't give offence. Think carefully about whether email is the best way of communicating.

Email messages can be used for different types of communication and can constitute a formal record of proceedings. For example, an email may have to be released if it falls within scope of a Freedom of Information Request, Environmental Information Regulation or Subject Access Request under the General Data Protection Regulation, or used as proof of a decision in legal proceedings.

Emails containing confidential information must never be forwarded to other recipients unless it is business relevant.

11.3 Speed of response

You must comply with the corporate timescale to respond to external emails within 7 working days of receiving them, except for complaints which must comply with the complaints procedure.

11.4 Email content expectations

It is expected that all users of Surrey Heath email should follow the email management guidance available on the Surrey Heath intranet under Information Governance.

Surrey Heath Human Resources policies should be considered at all times when composing emails. It is not acceptable to include derogatory or inflammatory comments.

It is the responsibility of all members of staff to exercise their judgement about the appropriateness of content when using email. If you need clarification on this, please contact the Information Governance Manager.

The forwarding of chain mail or jokes is not permitted.

11.5 Misuse of email

Executive Heads can authorise an officer to access an email account, including whilst a member of staff is on annual leave or other absence. This can be arranged through the ICT Service Desk. There must always be a valid business case for this authorisation.

The content of email messages is not routinely monitored. However, members of staff are advised that the content of email messages will be monitored if they are suspected of misusing the email system.

Only authorised personnel can access email accounts. Do not log other people onto your email account.

Your personal webmail must never be used for Surrey Heath business. Your official Surrey Heath email account is the only approved email system.

11.6 Personal email

Personal email should not be sent or received through Surrey Heath addresses. It is forbidden to subscribe to non-work related mailing lists using your Surrey Heath email address.

11.7 Access to staff emails

If necessary, assign access to your email account using a change request via the ICT Service Desk. If a line manager needs access to your account, including to read unread emails, they need to raise a change request through the ICT Service Desk and obtain Executive Head of Service authorisation.

If necessary, to enable the Council to undertake its responsibilities under Freedom of Information (FOI) or Environmental Information Regulations (EIR) the Information Governance team, including the FOI Officer, may be required to access staff emails via the Barracuda achieve system, only emails where no exemption under FOI or EIR applies, will be released.

11.8 Sensitive Personal Data

If your email contains sensitive personal data, the email should be encrypted with a password. If you require assistance with this please contact the ICT Service Desk.

11.9 Email retention

The email retention policy is 6 years on the main inbox and sent items folders. If any email content is required for longer than 6 years under the retention and disposal

schedules, it must be transferred into a different subfolder, which can be within the main folder.

If a member of staff leaves Surrey Heath, there is an exception to this retention and disposal policy. Unless advised otherwise by the leaver's line manager through the leavers call logged on the ICT Service Desk system, the email account will be deleted as part of the leavers' process.

11.10 Email forwarding

Auto forward of emails is not allowed. If you have a business requirement please seek advice from the Information Governance Manager

11.11 Management of Public Folders/Shared Mailboxes

A public folder/shared mailbox is an email account that can be shared by a group of people. These are usually generic accounts where the email is not for a specific person. Each folder must have an owner, usually at WMT level. The owner is responsible for ensuring the folder is properly managed.

New shared mailbox requests can be made by raising a call on the ICT Service Desk. New requests must be authorised by an Executive Head.

12.0 Secure Government Email Policy

12.1 Purpose

The security of electronic information is critical in today's environment, with potential interception of unsecured email sent over the internet being a realistic possibility.

Surrey Heath no longer supply GCSX mailboxes. Instead the @surreyheath.gov.uk Mailbox has been configured to meet the standards set out by the Government Digital Service for securing government email.

Electronic information considered restricted or sensitive will now be secure to send from your @surreyheath.gov.uk mailbox. It is the responsibility of the sender to ensure that the recipient mailbox is also secure and meets Government guidelines.

Further information on the guidance for secure email can be found here

https://www.gov.uk/guidance/securing-government-email#use-appropriate-encryption-methods

13.0 Clear Desk Policy

13.1 Purpose and scope

This policy is to instruct employees on how they should leave their workspace at the end of their working day. Physical documents are as important as electronic data when considering storage and security.

Confidential information left out on desks can put the Council at risk of a security breach or information theft.

Removing printouts, post-its and even USB sticks at the end of the day will significantly reduce this risk.

This policy applies equally to all users of ICT Systems at Surrey Heath Borough Council, including head of paid service, statutory officers, all permanent members of staff, temporary staff, contractors and third-party support companies.

13.2 Requirement

At the end of the working day all employees are expected to tidy their desk and to tidy away all office papers into locked desk drawers and filing cabinets.

The General Data Protection Regulation and Data Protection Act 2018 requires data controllers to ensure that personal information is kept secure. A clean desk policy will help the authority to comply with these regulations.

With contractors including cleaning staff, tenants and visitors having access to various areas of the building, it is essential that desks are kept clear of printed data.

In addition to the notes above, please read the Agile Working Policy and refer specifically to section 13, Corporate Standards. Desks designated as ‘flexi desks’ are required to be kept free from any personal effects and must be kept clear and clean for the next user.

13.3 Tips for keeping a tidy desk

a) Put a regular date and time in your diary to clear your paperwork

b) Use the confidential waste bins or a confidential shredding sack which you can obtain from the Facilities Team, or one of the shredding machines located on each floor for personal/confidential

paper no longer needed

c) Use recycling bins for non-personal/confidential papers no longer needed

d) Do not print off emails to read them. This just generates increased amounts of

clutter

e) Go through the things on your desk to make sure you need them and what you

don’t need, dispose of appropriately

f) Always clear your desktop before you go home

g) Consider scanning paper items and filing them in electronic form with adequate back up facilities.

13.4 Audit

Regular audits will take place to ensure staff are complying with this policy.
Staff who do not comply with this policy could face disciplinary action.

14.0 Box Security Policy

14.1 Purpose

This policy is to instruct employees and members of the ICT Team on security of the Box document storage platform.

The risk of sharing a document incorrectly is extremely high if the staff member is not fully trained on the safe usage of this facility. The functionality of Box brings great flexibility and enables users to work in a more agile approach. It is the responsibility of ICT to ensure staff are adequately trained to use Box before they are given access, to reduce the risk of a data breach or data loss.

14.2 Administration

3 members of ICT will have full administration access over the Surrey Heath Box environment.

Network & Security Manager
Digital Development Manager
Digital Developer

All other users have access to their personal area and a shared service area.

These administrators are all covered by confidentiality agreements and are not allowed to access documents and folders outside of their shared service departmental and personal areas without written permission from the folder or document owner, the ICT Manager, or Executive Head of Service

Users will also have access to shares granted from any other Box users.

Users will not be setup on the Box platform until an approved service request has been received through the ICT Service Desk system.

14.3 Box lock out

The 3 administrators will have the ability to lock users out of the Surrey Heath Box environment which will affect access from any location and from any device.

The 3 members of the Network & Security Team and the Service Desk also have the ability to lock users out from any systems connect through the Okta single sign on facility. This will also affect Box access

14.4 Box training

Due to the risk of sharing folders and documents incorrectly, no user will be given access to Box until they have received ICT delivered Box training. The Digital Development Manager will ensure a training record is held for each user.

Annual data protection training to all staff should include reminders on data security awareness in relation to file sharing in Box

Surrey Heath Borough Council
Employment Committee
6 April 2022

Data Protection Policy

Strategic Director/Head of Service	Gavin Ramtohal
Report Author:	Sally Turnbull, Information Governance Manager
Key Decision:	no
Wards Affected:	n/a

Summary and purpose

This report provides the Employment Committee with information regarding the Council's Data Protection Policy which is an annual item on the agenda.

The policy has not changed with the exception of one job role change.

Recommendation

The Committee is advised to RESOLVE that the revised Data Protection Policy, as set out at Annex A to the report, be adopted.

1. Background and Supporting Information

1.1 The Data Protection Policy is to be reviewed annually. If there is a need to change it before the annual review it will come back for recommendation sooner.

1.2 The proposed revisions to the Policy were considered by the Joint Staff Consultative Group at its meeting on 29 March 2022.

2. Reasons for Recommendation

2.1 The Data Protection Policy needs to be kept under review and will be presented to the Committee annually unless there is a requirement to change it sooner.

3. Proposal and Alternative Options

3.1 The adoption of the Data Protection Policy for the next 12 months when it is reviewed again unless it requires reviewing before this anniversary.

Annexes
Annex 1 - Data Protection Policy

Background Papers
n/a

DATA PROTECTION POLICY

Document history

Date	Version	Author	Changes made
15th October 2018	Draft 5.1	Geraldine Sharman	Initial revision of 2017 policy
26 October 2018	Draft 5.2	Geraldine Sharman	Reviewed and written policy
17 January 2019	Version 5	Geraldine Sharman	Approved version
Feb 2021	Version 5	Sally Turnbull	Review
Feb 2022	Version 5	Sally Turnbull	Review

Approvals

Name	Role/Title	Date
Janet Jones	ICT Manager	31st October 2018
Karen Limmer	Data Protection Officer	13th November 2018
Louise Livingston	Executive Head of Transformation	
Kelvin Menon	Executive Head of Finance as Senior Information Risk Owner	7th November 2018
Belinda Tam	HR Manager	
Paul Deach	ICT Portfolio Holder	28th November 2018
CMT members	Data Protection Officer	11th December 2018
Joint Staff Consultative Group		17th January 2019
Employment Committee		25th March 2021

Document Filename and Location:

Filename:181026 Data Protection Policy (v5)

Format	Version	Filepath	Owner
Draft	Draft 5.1	Box:\ICT Policies and Documentation\Data Protection Policy\Data Protection Policy 2018	Geraldine Sharman
Published	Version 5	Box:\ICT Policies and Documentation\Data Protection Policy\Data Protection Policy	Sally Turnbull

1. Scope of this policy statement

1.1. Surrey Heath Borough Council (SHBC) is committed to fulfilling its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA2018) and has produced this policy to provide assurance to customers and staff and to assist officers. UK GDPR and DPA 2018 need to be considered side by side.

1.2. UK GDPR and DPA 2018, otherwise known as Data Protection legislation, establishes a framework of rights and duties which are designed to safeguard personal data to which SHBC is committed. This framework balances the legitimate needs of the Council to collect and use personal data about the people the Council deals with for business and other purposes against the right of individuals to respect the privacy of their personal details. This includes members of the public, clients and customers, members, current, past and prospective employees, suppliers (such as sole traders) and other individuals with whom the Council communicates.

1.3. Surrey Heath Borough Council will use personal information lawfully and securely regardless of the method, by which it is collected, recorded and used and whether it is held on paper, electronically or recorded on other material such as audio, visual media (CCTV) or Body Worn Cameras. This includes use of printers where information is immediately printed to ensure this is conducted in a secure location and never left on printers. The Council will respect the privacy of individuals.

1.4. To this end, Surrey Heath Borough Council fully endorses and adheres to the principles of Data Protection, as set out in Article 5 of the UK GDPR (see Section 3).

1.5. If any Surrey Heath Borough Council work is outsourced that we ensure the company used complies with the same standards as would be expected if completed by SHBC.

2. Definitions

2.1. Personal Data

'Personal data' under the Data Protection legislation is information about a living individual who can be identified from the information. The information can be factual information (e.g. names and addresses) or expressions of opinion or

intentions about an individual. Other examples of personal data include location of data, on line identifiers (IP addresses and mobile devices ID's and photographs).

2.2. Consent

Consent is the fact that permission has been given. A person who consents to something is in effect giving permission for that thing to happen. Explicit consent requires an affirmative action to be taken, this can be articulated either orally or in writing but a clear and voluntary preference is given and it must be given freely where the available option and the consequences have been made clear.

2.3. Data Subject

Data subject means 'an individual who is the subject of personal data'. This must be a living individual

2.4. Data Controller

Defined as a person (or organisation) who (either jointly or in common with other persons/organisations) determines the purposes for which, or the manner in which, any personal data are, or are to be, processed. The Data Controller is ultimately responsible for all records processed

2.5. Data Processor

The data processor means any person (other than an employee of the data controller) who processes the data on behalf of the data controller

2.6. Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment is a process to help the Council identify and minimise the data protection risk of a project. A DPIA must be completed for any new, or change, to processing of personal information whereby there may be a risk to the individual.

2.7. Information Asset Register

An information asset is a collection of information, defined and recorded as a single unit so it can be understood, shared, protected and used efficiently to help the Council provide a service. Information assets have recognisable and manageable value, risk, content and lifecycles. Maintaining an Information Asset Register (IAR) is a requirement of the UK GDPR. The IAR is a simple way to help Council Officers understand and manage the Council's information assets and the risks relating to those assets.

Examples of information assets within Surrey Heath are Chipside, Adelante, complaints database, Lagan, planning application history.

The Council's IAR includes the following information:

- Identification of each information asset
- Where our information is held
- Who the Information Asset Owner is
- Why we keep it
- Who is allowed to access it
- How long we keep it

2.8. Processing

Processing is defined as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

2.9. Special Category Data

This is personal data consisting of information relating to any of the following:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health and Social Care
- Sex life
- Sexual orientation

Special category personal data is subject to much stricter conditions of processing. Personal data relating to criminal convictions and offences are not included within special category data per se but similar extra safeguards apply to its processing. The Council must be able to demonstrate that the processing is strictly necessary and satisfies one of the conditions in Schedule 8 of the DPA2018 or is based on consent

3. Roles and Responsibilities

3.1. All staff will ensure that:

- Consider whether the information they are working on contains personal data and then use it in accordance with this policy and the six data protection principles of the UK GDPR

- they complete regular mandatory Data Protection training as required

- they follow the Data Protection Policy and understand how it works, otherwise disciplinary action may be taken against any Borough Council employee who breaches any instruction contained within it, or following from, the UK General Data Protection Regulation and Data Protection Act 2018. Compliance with the Data Protection Policy forms part of Staff Terms and Conditions.

3.2. Data Protection Officer

- this is a statutory post. The Council's Data Protection Officer is the Head of Legal Services

- will inform and advise the Council and its employees about their obligations to comply with both the UK General Data Protection Regulation and the Data Protection Act 2018

- monitor compliance with the Data Protection legislation, including the assignment of responsibilities, audits.
- provide advice about Privacy By Design and Data Protection Impact Assessments and monitor their performance
- co-operate with the Information Commissioner's Office (ICO)
- act, where necessary, as the contact point for the ICO on issues relating to the processing of personal data

3.3. Senior Information Risk Owner (SIRO)

- the SIRO has overall strategic responsibility for governance in relation to data protection risks.
- act as advocate for information risk in the Corporate Management Team
- include information risk in the Annual Governance statement
- review information management on the Corporate Risk Register
- in liaison with the Data Protection Officer, Information Governance Manager and Heads of Service ensure the Information Asset Owner roles are in place to support the SIRO role
- within Surrey Heath, the Strategic Director, Finance and Customer Services ~~Executive Head of Corporate~~ acts as the SIRO.

3.4. Information Asset Owners (IAO)

- these are members of the Wider Management Team. Their role is to understand what information is held by their service, what is added and removed, how information is moved and who has access and why. They will assist in the production of the Information Asset Register and agree and sign off their Service's Register which include the retention and disposal schedule for their service.

3.5. Executive Heads/Heads of Service will:

- ensure compliance with Data Protection legislation within their services and liaise with the Data Protection Officer where necessary
- identify the services they provide and any specific processes they are responsible for that involves the use of personal information
- appoint, when required, any Information Asset Owners for their services who will be responsible for each information asset or system within the service
- Any new project, where personal data is being collected, must consider and build in privacy from the beginning. This is called Privacy By Design and is a requirement of UK GDPR.

- A Data Protection Impact Assessment is required where any processing of personal information will be undertaken on a regular basis e.g. involving IT systems, third part sharing, CCTV or body worn cameras whereby there may be a risk to the individual. The Information Governance Manager must be informed and involved at an early stage.

- ensure staff complete any mandatory data protection training

- ensure contracts, where personal data processing is involved, adequately covers data protection, including if a data processor is involved, they are made aware of their responsibilities under data protection legislation.

3.6. HR service will ensure the following arrangements are in place:

- where necessary, ensure Baseline security checks (personnel checks for prospective staff) are carried during the recruitment process

- to ensure that new members of staff are made aware of this policy document at induction stage

- to ensure that all new starters and temporary staff complete Data Protection e-learning training as part of their induction.

3.7. ICT Manager

- Responsible for creating, implementing and maintaining the Council's Information Security Policy to reflect changing local and national information security requirements.

- Reviewing with the Information Governance Manager the requirement for a DPIA when new systems are installed.

3.8. The Information Governance Manager will:

- act under the authorisation of the Data Protection Officer and carry out day to day duties, including liaising with the ICO

- ensure that the Data Protection Policy and associated documents are kept up to date and communicated to staff in an appropriate manner

- provide technical guidance on specific sectors and issues and will keep such guidance up to date

- arrange and carry out the provision of advice and training to staff

- be responsible for notifying that the Council holds personal information about living people and the payment of the registration fee to the Information Commissioner's Office in accordance with the Data Protection (Charges and Information) Regulation 2018 and keeping an internal record in relation to all personal data processed

- complete subject access requests (which should be made in writing using the Council's pro forma request, if possible). Enquiries about Data Protection should be addressed to the data protection mailbox

- keep up to date with changes in the law and guidance on Data Protection legislation

- advise on and ensure any data sharing is compliant with the UK General Data Protection Regulation and Data Protection Act 2018 including Schedule 2, Part 1, Paragraph 2 requests

- advise on and draft, as required, Data Sharing Agreements and DPIA's

4. Data Protection Principles (Article 5 of the General Data Protection Regulation)

4.1. UK GDPR applies to any processing of personal information and requires compliance with the Data Protection principles. The six principles lie at the heart of the UK GDPR. Processing includes virtually anything that can be applied to information, including acquisition, storage and destruction as well as active use. This includes CCTV images, photographs and digital images.

4.2. Personal data should be:

a) processed lawfully, fairly and in a transparent manner
b) collected for specified, explicit and legitimate purposes
c) adequate, relevant and limited to what is necessary
d) accurate and where necessary kept up to date
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed and
f) processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4.3. Anyone who processes personal data about people must make sure that:

- they respect the individual's data protection rights

- all electronic and manual filing systems conform to the six Data Protection Principles

- be accountable and able to demonstrate, where necessary, compliance with the principles. Accountability is central to UK GDPR.

5. Lawful basis for processing

The lawful basis for processing (using) personal data is set out in the UK GDPR. At least one of these must apply whenever the Council processes personal information:

- **Consent:** the data subject has given clear and unambiguous consent for the Council to process his/her personal data for a specific purpose. Another lawful basis should be considered before using this one

- **Contract:** the processing is necessary for a contract that the Council has with the data subject, or because the data subject has asked the Council to take specific steps before entering into a contract

- **Legal obligation:** the processing is necessary for the Council to comply with the law (not including contractual obligations)

- **Vital interest:** the processing is necessary to protect someone's life

- **Public interest:** the processing is necessary for the Council to perform a task in the public interest or in the exercise of official authority vested in the Council

- **Legitimate interest:** the processing is necessary for the purposes of legitimate interests pursued by the Council or a third party except where such interests are overridden by the interests of the data subject. This requires balancing the Council's interests against the individual's interests. However, this basis is not available to processing carried out

6. Surrey Heath Borough Council's commitment to Data Protection

6.1. Surrey Heath Borough Council is a Data Controller as defined in the UK GDPR and DPA2018 and is registered with the Information Commissioner's Office and as such all officers, contractors and volunteers have a responsibility for data protection.

6.2. Surrey Heath Borough Council is committed to compliance with Data Protection legislation. The Council will carry out the following:

- fully observe regulations and codes of practice regarding the fair collection and use of personal information (this includes but is not limited to codes of practice issued by the Information Commissioner)

- meet its legal obligations to specify the purposes for which information is used through the appropriate use of Privacy Notices on application forms, web pages, CCTV signs and via telephone. In other words through whatever means personal information is collected

- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements, i.e. not collect information "just in case"

- check and maintain the quality of information used

- ensure adequate recordkeeping for personal data

- apply checks to determine the length of time information is held, ensuring it is up to date and is not kept for longer than is necessary regardless of its format.

Members of staff will adhere to the Council's Retention and Disposal Policy to ensure the information is held for only as long as is necessary.

- ensures every person managing and handling personal information is appropriately trained to do so
- ensure that the rights of people about whom information is held can be fully exercised under the legislation
- take appropriate technical and organisational security measures to safeguard personal information specifically by means of the Information Security Policy and subsidiary policies
- not disclose personal data, either within or outside the organisation, to any unauthorised recipient. Breaches will be managed in line with the Data Security Breach Policy and Procedure
- ensure that personal information is not transferred outside of the European Economic Area, including storing information in the Cloud, without suitable safeguards. Discussions will take place with the Data Protection Officer or Information Governance Manager before transferring any information overseas

7. Rights of Data Subjects

7.1. The UK GDPR has enhanced individuals rights concerning their personal data. Their rights are as follows:

- the right to be informed about how their information will be used
- the right of access to their personal information (normally known as Subject Access Requests)
- the right to rectification, which is the right to require the Council to correct any inaccuracies
- the right to request the erasure of any personal information held by the Council where the Council no longer has a basis to hold the information
- the right to request that the processing of their information is restricted
- the right to data portability
- the right to object to the Council processing their personal information
- rights in relation to automated decision making and profiling

7.2. Not all rights are absolute and will depend upon the lawful basis on which the Council is relying to process the personal data. Decisions will be made on a case by case basis.

7.3. Data subjects (this includes employees and councillors) have the right to access personal data held about them (this includes factual information, expression of opinion, and the intentions of the Council in relation to them, irrespective of when the information was recorded), the right to prevent processing likely to cause damage or distress and the right to have inaccurate data rectified, blocked, erased or destroyed.

7.4. The Council will arrange for the data subject to see or hear all personal data held about them as long as it does not adversely affect the rights and freedoms of others, and no restrictions apply which prevent disclosure of the personal data. The information will be provided within 1 calendar month of a Subject Access Request being received in writing including, where necessary, two pieces of information to prove identity.

7.5. Where the Council is unable to process the request within the timeframe, the data subject will be notified as soon as possible of any potential delay, the reasons for such a delay, and the date when their information will be made available. The Council may extend the time period for processing and responding to a request by a further two months depending upon the complexity. Where a data subject request is considered unfounded or excessive, the data controller may either:

- charge a reasonable fee to provide the information, or
- refuse to act on the request

7.6. Any queries regarding individual rights under Data Protection, or any requests for personal information whether from the person themselves or from a third party must be referred to the Information Governance Manager or the data.protection@surreyheath.gov.uk email.

8. Data Sharing and Data Matching

8.1. Unauthorised disclosure of personal data is a criminal offence. Such data may only be disclosed for registered purposes to:

- the person themselves
- employees of the Council as required in the course of their duties
- members of the Council whereby a UK GDPR Article 6 or Article 9 legal basis applies
- promote the prevention and detection of fraud and crime
- the Courts under direction of a Court Order
- Other Government authorities whereby there is a legal or statutory requirement
- Third parties whereby a UK GDPR Article 6 or Article 9 legal basis applies.

8.2. Appropriate information sharing protocols must be in place before personal information will be shared with other agencies, unless required to do so by law. These protocols will be reviewed, amended and updated on a regular basis. They must comply with the Information Commissioner's Data Sharing Code. Surrey Heath Borough Council is a signatory of the Surrey Multi Agency Information Sharing Policy (MAISP). Any information shared with signatories of MAISP must comply with this. A list of the signatories can be found on the Surrey County Council website

8.3. The Council is required to collect, use and share certain types of personal information to comply with different laws – examples would include Council Tax and Electoral Registration information.

8.4. The Council will comply with the Information Commissioner's guidance on data matching. The Council is a participant of the National Fraud Initiative and the Surrey Counter Fraud Partnership.

9. Contractual and partnership arrangements

9.1. In the event that the Council enters into a contract with a third party which involves, collecting, processing, handling, securing or disposing of information at any level there needs to be contractually binding data protection clause in the contract. Specific care should be taken in respect of services provided online and via 'the cloud'.

9.2. Such mandatory provisions will identify the roles and responsibilities of the "data controller" and "data processor" in relation to activities carried out during the life, and after termination of, the contract.

9.3. Where the parties are data controllers jointly or in common, the Council will liaise with the other relevant parties to ensure that all processing complies with DPA2018. The responsibilities of each data controller should be expressly and clearly laid out.

10. Training

10.1. Data Protection training is mandatory for all employees of the Council. All new employees will complete Data Protection e-learning as part of their induction. Annually, all employees will complete the Data Protection e-learning package or attend a refresher course if provided.

10.2. Separate training will be arranged for Members at induction and regularly thereafter.

11. Links with Other Policies

The Data Protection Policy will have an impact and relationship with the following policies:

- Information Security Policy
- Data Security Breach Management Policy and Procedure
- Speak up Policy
- Social Media Policy
- Capability Policy
- Recruitment Policy and Procedure
- Regulatory and Investigatory Powers Act 2000 Policy and Procedure
- Homeworking Policy
- Data Protection Policy for Home Working
- Off-site Working Policy
- Disciplinary Policy and Procedure
- Grievance Policy and Procedure

- Anti-fraud and Corruption Policy
- Individual Rights Procedures

12. Review

12.1. This policy will be reviewed in 2023 and reflect if necessary, any changes in guidance

Surrey Heath Borough Council
Employment Committee
6 April 2022

Data Security Breaches Policy

Strategic Director/Head of Service	Gavin Ramtohal
Report Author:	Sally Turnbull, Information Governance Manager
Key Decision:	no
Wards Affected:	n/a

Summary and purpose

This report provides the Employment Committee with information regarding the Council's Data Security Breaches Policy which is an annual item on the agenda.

The policy has been amended to reflect we are no longer part of EU as detailed in section 1.6 and now reflects UK GDPR. 3.1 also reflects the job role changed for SIRO

Recommendation

The Committee is advised to RESOLVE that the revised Data Security Breaches Policy, as set out at Annex A to the report, be adopted.

1. Background and Supporting Information

1.1 The Data Security Breaches Policy is to be reviewed annually. If there is a need to change it before the annual review it will come back for recommendation sooner.

1.2 The proposed revisions to the Policy were considered by the Joint Staff Consultative Group at its meeting on 29 March 2022.

2. Reasons for Recommendation

2.1 The Data Security Breaches Policy needs to be kept under review and will be presented to the Committee annually unless there is a requirement to change it sooner.

3. Proposal and Alternative Options

3.1 The adoption of the Data Security Breaches Policy for the next 12 months when it is reviewed again unless it requires reviewing before this anniversary.

Annexes
Annex A – Data Security Breaches Policy

Background Papers
n/a

DATA SECURITY BREACH MANAGEMENT POLICY AND PROCEDURE

Document history

Date	Version	Author	Changes made
18 September 2014	Version 1.0	Geraldine Sharman	None made by JSCG
8 August 2019	Version 2.0	Geraldine Sharman	Revised version
12 March 2020	Version 2.1	Sally Turnbull	Policy review
February 2022	Version 2.2	Sally Turnbull	Policy Review

Approvals

Name	Signature	Role/Title	Date
Belinda Tam		Human Resources Manager	11/09/19
Julia Hutley-Savage		Data Protection Officer	12/02/20
Kelvin Menon		Senior Information Risk Owner	05/09/19
Stuart Field		ICT Manager	29/09/19
James Rutter		ICT Manager	02/01/20
Cllr Paul Deach		Portfolio Holder	
		Recommended by JSCG to go forward to the Executive and then full Council	
		Recommended for approval to Full Council	
		Approved by Full Council	

Document Filename and Location:

Format	Version	Filepath	Owner
Draft	2.0	Box\Information Governance\ICT Policies and Documentation\Data Protection Breaches Policy\1908 Data Security Breaches Policy	Geraldine Sharman
Final version	2.1	Box\Information Governance\Policies and Documentation\Data Protection breaches policy\2022 review	Sally Turnbull

1. INTRODUCTION

1.1 Surrey Heath Borough Council (SHBC) is committed to ensuring that all personal data we process, including that of colleagues and customers, is managed appropriately and in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) (collectively referred to as "Data Protection legislation")

1.2 As SHBC processes personal data it is committed to ensuring all unauthorised or unlawful processing, loss, destruction of or damage to data (personal data breaches) are swiftly identified and reported within the Council and, where appropriate to the Information Commissioner's Office and affected individuals.

1.3 Human Resources may deal with negligent or malicious non-compliance with this policy through the disciplinary process.

1.4 Under the Data Protection Act 2018 and UK General Data Protection Regulation, Surrey Heath Borough Council is a Data Controller. This is a "person" who determines the purposes for which and the manner in which any personal data are, or are not to be processed. The sixth Data Protection principle states that organisations, which process personal data, must ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

1.5 As well as defining SHBC's policy, this procedure lays out the actions, once a breach has occurred.

1.6 ~~GDPR standards and ICO guidance will need to continue after the UK leaves the EU. The role of the DPO and need for reporting to the ICO will continue. GDPR will be known as UK GDPR~~.

2. SCOPE

2.1 This policy and procedure applies to all users of SHBC's information, data, information systems and the Council's physical buildings. It applies to not only staff and members but also where appropriate contractors, agency staff, service providers, consultants and anyone else engaged to work in the organisation and encompasses data, information, software, systems, and paper documents.

2.2 This policy should be read in conjunction with other relevant policies, including but not limited to:

- Data Protection Policy
- Information Security Policy
- Disciplinary Policy
- Social Media Policy
- Whistle-blowing Policy and Procedure

All staff, including all new starters, must read this policy as this forms part of the Staff Terms and Conditions.

2.3 Other useful documents:

- ICO Information Security Guide
- ICO Guidance on Personal Data Breaches
- A29WP Guidelines on Breach Notification
- Act Now Blog post

3. RESPONSIBILITIES

3.1 The **Senior Information Risk Owner (SIRO) (**Strategic Director, Finance and Customer Services~~Executive Head of Finance~~**)** has overall responsibility for deciding whether to report personal data breaches to the ICO and/or to affected individuals but will delegate minor breach notification to the Data Protection Officer/Information Governance Manager. The Information Governance Manager and SIRO will meet on a regular basis to discuss Data Handling and Data Protection.

3.2 The Head of Legal acting as **Data Protection Officer** has overall responsibility for monitoring compliance with this procedure. They will work, where necessary, with the Information Governance Manager, receiving and processing incident reports, assessing risk and advising the SIRO accordingly, and liaising with the ICO and the public as appropriate.

3.3 Although the Data Protection Officer has overall responsibility for monitoring compliance with this procedure, they will delegate the day-to day management of breaches to the **Information Governance Manager**, including receiving and processing incident reports and assessing the risk. In the absence of the Information Governance Manager, the Data Protection Officer will manage any breaches. The Information Governance Manager, will be the main contact with the Information Commissioner's Office.

3.4 **Executive Heads**, through Information Asset Owners, are responsible for ensuring that all staff are aware of their responsibilities to report incidents; for assisting the Data Protection Officer/Information Governance Manager in their duties through providing all appropriate information and support relevant to an incident; for continuing with appropriate incident management and mitigation.

3.5 **All staff** are responsible for immediately reporting any incident or breach affecting personal data held by the Council.

4. TYPES OF BREACH

4.1 A number of factors could cause data protection breaches. The following is a list of examples but it is not exhaustive and there may be others which will need to be considered at the time of the breach:

- loss or theft of data

- loss or theft of equipment on which data is stored
- inappropriate access controls allowing unauthorised use, both electronic and paper
- equipment failure
- human error in dealing with personal information including both electronic and paper
- unforeseen circumstances such as fire or flood
- hacking attack on the Council's ICT systems
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it
- unauthorised access into secure areas

5. NOTIFICATION OF BREACHES ONCE DISCOVERED

5.1 Instances of the loss of personal data are rare in the Council, however, the consequences to its reputation and the potential impacts on individuals of the loss of personal information means we need to take swift action in the event of a loss.

5.2 The person who discovers/receives a report of a breach must inform the Information Governance Manager and Data Protection Officer immediately. Notify any breach discovered outside of normal working hours as soon as is practicable during the next working day however any serious breaches that could cause serious adverse effect or media interest must be reported as a matter of urgency. The contact email address for data protection is data.protection@surreyheath.gov.uk

5.3 The Information Governance Manager and/or the Data Protection Officer, will then decide whether to involve other departments e.g. Human Resources, ICT.

6. ASSESSING THE RISKS

6.1 The Information Governance Manager will carry out the initial assessment of the breach on the day it is reported and consider whether the event meets the UK GDPR definition of a personal data breach.

6.2 During this initial assessment, a risk assessment of the impact and likelihood of impact on the rights and freedoms of the affected individual's, data subjects, will be undertaken this must be completed within 72 hours of the breach being reported.

6.3 This will consider the risks to the affected individuals arising from the personal data breach including adverse impact on their:

- Privacy
- Personal financial interests

- Other material damages
- Health and safety
- Emotional wellbeing
- Other non-material damages

6.4 In considering the risk, the Information Governance Manager will have support and advice from the Data Protection Officer and relevant Executive Head or Head of Service and other colleagues as required.

6.5 Factors to be considered (these factors are not exhaustive):

- The type of breach
- The nature, volume and sensitivity of the personal data breached
- How easy it is to identify individuals
- The potential consequences for individuals
- Any special characteristics of the data subject (for example they are children or otherwise venerable)

6.6 Some data security breaches will not lead to risks beyond the possible inconvenience to those who use the data to do their job, for example if a laptop is irreparably damaged or lost, or in line with the Information Security Policy, it is encrypted, and no data is stored on the device. There will be a monetary cost to the Council by the loss of the device but not a security breach.

6.7 Whilst these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of customer data, whereby the data may be used to commit identity fraud.

6.8 Helpful tips for assessment of risks (these tips are not exhaustive):

- what type of data is involved?
- how sensitive is it? Is it sensitive personal details as defined by the Article 9 of UK GDPR (e.g. housing benefits) or other data types which are sensitive because of what might happen if it is misused (e.g. bank account details).
- if data has been lost or stolen, are there any protections in place such as encryption?
- what has happened to the data?
- can the data be restored or recreated?
- how usable is the lost data?
- if data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk
- what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people

- how many individuals' personal data is affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- who are the individuals whose data has been breached? Are they staff, customers, clients or suppliers?
- what harm can come to those individuals because of the breach? Are there risks to physical safety or reputation, financial loss, fraudulent use or a combination of these and other aspects of their life?
- are there wider consequences to consider such as a risk to loss of public confidence in one of the service areas?

7. REPORTING PERSONAL DATA BREACHES TO THE AFFECTED INDIVIDUALS

7.1 As part of the risk, consider whether the person/people whose information has been breached should be informed. Inform the person/people concerned, as suggested by guidance from the Information Commissioner unless to inform them will cause additional or undue distress/stress.

7.2 If the Data Protection Officer considers the personal data breach a high risk, a report will be provided to the SIRO including a recommendation on whether to report the breach to the affected individuals.

7.3 If the SIRO decides to notify the individuals, consider the following:

- what is the most appropriate method of communication? Always bear in mind the security of the medium as well as the urgency of the situation
- the notification should include as a minimum, a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach
- give the individuals clear advice on what they should do to protect themselves and what the Council are willing to do on their behalf
- provide a means of contacting SHBC for further information. This could include a named individual, a helpline number, a web page or a combination of all of these.

8. APPOINTMENT OF LEAD INVESTIGATOR

8.1 The Information Governance Manager will, in consultation with others, if necessary, decide who the Lead Investigator should be, who needs to be involved and will work with them to manage the breach. The Information Governance Manager is responsible for advising services on assessing the impact of any data breach of the Data Protection legislation. This can include recommendations to restore data security. The Information Governance Manager will appoint a lead investigator will for serious breaches but could be appointed for minor breaches if the Information Governance Manager did not understand enough about the breach.

8.2 The Lead Investigator could be any of the following:

- a member of Audit and Investigations
- Executive Head
- Information Governance Manager
- a member of Human Resources
- a combination of the above

8.3 The Information Governance Manager will decide whom to notify.

8.4 Inform the Senior Information Risk Owner (SIRO) of any minor breaches at the Information Governance Managers regular review meetings. For serious breaches (i.e. the extent of the 'damage'), the SIRO must be informed immediately, the Chief Executive and Head of Transformation will also be made aware

8.5 The Lead Investigator/SIRO must also consider whether the police need to be informed. This could be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. If credit card numbers are lost then tell the appropriate bankcard provider.

8.6 If necessary, consider notifying all staff to prevent additional breaches.

8.7 The Information Governance Manager will maintain a log with the details of all breaches. This will include who the Lead Investigator is, when the breach occurred, who is involved and what action must be taken after the breach.

9. INVESTIGATION PROCEDURE

9.1 Begin investigation immediately on receipt of notification. Complete urgently and wherever possible within 72 hours of the breach being discovered/reported. Carry out, if necessary, a further review of the causes of the breach and recommendations for future improvements once the matter has been resolved

9.2 The next state, in most cases, would be to investigate the breach by the Lead Investigator. The Lead Investigator should ascertain whose data was involved in the breach, the person or people responsible for the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

9.3 Breaches will require not just an initial investigation, decision on the severity and containment of the situation but also a recovery plan including, where necessary damage limitation. This may often involve input from ICT, HR, Legal, Information Governance and the appropriate department. In some cases, contact with external stakeholders or suppliers may be required.

9.4 The Lead Investigator will establish the questions for interviews and then meet with the participants. This could be (but is not limited to or necessarily all of them) witnesses, victims and perpetrators, senior managers.

9.5 The Lead Investigator will identify if there is a need for expert advice from either professional advisers or Legal Services.

9.6 Issues to be addressed during the investigation will include:

- the date when the breach occurred
- the date when the breach was identified to SHBC and by whom
- the type of data and the number of records involved
- its sensitivity
- the circumstances of the release
- what protection is in place (for example encryption)
- what has happened to the data?
- whether the data could be put to any illegal or inappropriate use
- how many people are affected?
- what group of people has been affected (the public, suppliers etc)
- whether there are wider consequences of the breach

9.7 The Lead Investigator, via the Information Governance Manager, will keep an electronic record of all activities during the investigation. This could include the actions taken to mitigate the breach and lessons learnt. The reason for this is that the records may need sharing if there are actions by the police, Information Commissioner's Office, legal proceedings or Audit.

9.8 There could be a number of investigations going on at any one time for example by Human Resources and ICT.

9.9 The Information Governance Manager will assist the Lead Investigator, where necessary. This could include informing the Information Commissioner's Office, calculating the severity of the incident, collating reports, implementing actions from the Information Governance report.

9.10 If systemic or on-going problems are identified, draw up an action plan to correct. If the breach warrants a disciplinary investigation (for example due to negligence), the Lead Investigator should pass on any relevant information to Human Resources who will make the final decision on sanctions against staff.

9.11 The Lead Investigator should produce a report for the SIRO and be written with it in mind that it may be shared with the ICO.

9.12 The report must address the following:

- establish the facts (including those that may be disputed)

- include a chronology of events including the containment, recovery and how the breach has been investigated
- a risk analysis
- a commentary of the weight of evidence
- action to minimise/mitigate effect on individuals involved including whether the victims have been informed
- whether any other regulatory body and been informed and their response
- recommendations to reduce the chance of the same breach happening again

10. CONTAINMENT

10.1 At the same time as an investigation is happening, containment and recovery must also happen.

10.2 The Lead Investigator must ascertain whether the breach is still occurring. If so, it must be stopped immediately and minimise the effect of the breach. This will involve liaison with appropriate staff. Examples might be the ICT Manager authorising the shutdown of a computer system or stopping the delivery of electronic mail.

10.3 Media and Marketing may need telling of a breach if there is a possibility of information published on the Internet or the press told and their assistance is required in managing a media response.

11. REPORTING PERSONAL DATA BREACHES TO THE INFORMATION COMMISSIONER'S OFFICE

11.1 The UK GDPR places a duty on all organisations to report certain types of data breach to the Information Commissioner's Office

11.2 In the case of a personal data breach, the Council shall without undue delay and, where feasible, no later than 72 hours after becoming aware of breach, notify the ICO, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual. A reason for the delay, if notification is not within 72 hours, is required along with the notification.

11.3 The UK GDPR states that a personal data breach must be reported to the ICO if the breach is likely to result in a risk to the rights and freedoms of the individuals concerned. By this, it means discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. It also requires that this be on a case-by-case basis. There is no need to notify the ICO if there is not a risk to persons' rights and freedoms.

11.4 After carrying out a full assessment of the risk, the decision as to whether or not to inform the ICO would normally rest with the Senior Information Risk Owner. If the

decision is to notify the ICO, the Information Governance Manager or if not available, the Data Protection Officer will act as liaison with the ICO.

11.5 The Data Protection Officer or Information Governance Manager in conjunction Human Resources will also need to consider whether any officer concerned with the breach will be subject to disciplinary procedures.

11.6 Providing all information may not be possible in the initial response but it should contain the minimum recorded in the log. Use either the online reporting tool or via the telephone. Failing to notify a breach when required to do so can result in a fine up to €10 million.

12. REVIEW

12.1 A policy review will take place after a serious breach or after legislative changes, important changes in case law or guidance.

Report a breach - https://ico.org.uk/for-organisations/report-a-breach/

Surrey Heath Borough Council
Employment Committee
6 April 2022

Social Networking Policy

Strategic Director/Head of Service	Gavin Ramtohal
Report Author:	Sally Turnbull, Information Governance Manager
Key Decision:	no
Wards Affected:	n/a

Summary and purpose

This report provides the Employment Committee with information regarding the Council's Social Networking Policy which is an annual item on the agenda.

The policy has been amended to include that some social networking use may be applicable to FOI/EIR (8.3)

Recommendation

The Committee is advised to RESOLVE that the revised Social Networking Policy, as set out at Annex A to the report, be adopted.

1. Background and Supporting Information

1.1 The Social Networking Policy is to be reviewed annually. If there is a need to change it before the annual review it will come back for recommendation sooner.

1.2 The proposed revisions to the Policy were considered by the Joint Staff Consultative Group at its meeting on 29 March 2022.

2. Reasons for Recommendation

2.1 The Social Networking Policy needs to be kept under review and will be presented to the Committee annually unless there is a requirement to change it sooner.

3. Proposal and Alternative Options

3.1 The adoption of the Social Networking Policy for the next 12 months when it is reviewed again unless it requires reviewing before this anniversary.

Annexes
Annex A – Social Networking Policy

Background Papers
n/a

SURREY HEATH BOROUGH COUNCIL

SOCIAL NETWORKING POLICY

Social Networking Policy

1 Introduction

The main purpose of the Social Networking Policy is to provide guidelines for the effective and safe use of social networking to promote and develop Surrey Heath Borough Council's (SHBC) services, and to ensure employees and workers are aware of how they should conduct themselves when using social networking sites both at work and outside of work. There are also specific safeguarding issues that employees or workers who work closely with children or vulnerable adults need to be aware of. Please refer to the SHBC Safeguarding Policy for more information.

The Council are committed to making the best use of all available technology and innovation to improve the way we do business, this includes embracing social networking. The Council is pro social networking. However, we have a responsibility to ensure it is used appropriately by all.

2 Definitions

The term 'social networking' is given to websites, online tools, Apps and other ICT which allow users to interact or collaborate with each other either by sharing information, opinions, knowledge and interests. The term 'Blogs' refer to online diaries. Other platforms include message boards, podcasts, social networking (such as Twitter, Facebook, Instagram and Snapchat) content sharing websites (such as YouTube, Slack, and Flickr) and web conferencing sites such as Zoom and MS Teams.

3 Scope

The Social Networking Policy will apply to all employees and workers (including fixed term, casuals, agency staff, contractors and work experience students, volunteers as well as permanent staff) employed on Council business, including those working with partner organisations. This policy should be read in conjunction with the following policies and all other relevant policies will apply:

- Information Governance Strategy and Policy
- Information Security Policy
- Data Protection Policy
- Disciplinary Policy
- Code of Conduct for Officers
- Bullying and Harassment Policy
- Communication guidelines
- Whistleblowing Policy
- Safeguarding Policy

- Mobile Phone Agreement
- Vexatious and Persistent Complaints Policy and Procedures

The Council reserves the right to conduct investigations where a breach of the Social Networking Policy is suspected. Breach of this policy may be dealt with under the council's disciplinary policy. Serious cases may be treated as gross misconduct leading to dismissal.

Misuse of social networking websites (both inside and outside of work, if work information is involved) can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against the individual responsible for the content and/or the council.

4 Policy Statement

The Social Networking Policy covers all forms of social networking which include (but are not limited to):

- Facebook, Instagram, Snapchat, Nextdoor and other social networking sites
- Twitter, WhatsApp, discussion forums and other blogging sites
- YouTube and other video clips and podcast sites
- Zoom, MS Teams and other web conferencing sites
- LinkedIn
- All forms of collaborative tools including Slack, Trello and Chatter

5 Equality Assessment

The Council's equality scheme demonstrates its commitment to equality internally and externally and ensures that all sections of the community are given an opportunity to contribute to the wellbeing of the community. An equality impact assessment has been carried out on this policy and procedure.

The Council ensures that consultation is representative of the community and that consideration is given on how to consult hard to reach groups and will positively learn from responses.

6 Principle and Aims

6.1 The Council recognises that social networking is an effective communication mechanism which can be used alongside other communication methods. This policy is not intended to restrict employees and workers from using social

networking at work and at home, but to make them aware of the risks they could potentially face with how they share information.

6.2 To ensure that when social networking is used to communicate with the public, stakeholders and partners by all SHBC staff in the performance of their duties, that it is, aligned to the Council's communication guidelines.

6.3 To ensure that the reputation of SHBC is protected and the Council is not brought into disrepute.

6.4 To ensure that any SHBC communication through social networking meets legal requirements.

6.5 To ensure that all SHBC social networking sites are easily identifiable as originating from the Council and correctly apply the Council's logo according to brand guidelines.

6.6 To prevent the unauthorised use of Council branding on employee or workers' personal social networking sites.

6.7 To ensure that SHBC employees and workers are aware of cyber-bullying and defamation and that this would be deemed as a disciplinary offence and/or a criminal offence.

6.8 To ensure inappropriate language is not used on any SHBC presences or posts, and SHBC core values are considered at all times

6.9 To ensure content remains professional at all times.

7 Policy and Procedure

7.1 If employees and workers make reference to the Council on a personal internet site, they should follow these guidelines:

- Do not engage in activities over the internet that could bring the Council into disrepute.
- Do not use the Council logo on personal web pages.
- Do not reveal information which is confidential or sensitive to the Council – consult your manager if you are unsure. Do not discuss existing or proposed policies on social networking websites.
- Do not include contact details, personal details or photographs of service users or staff without permission.
- Do not make offensive comments about the Council, members, colleagues, suppliers or residents of Surrey Heath on the Internet. This may amount to cyber-bullying or defamation and could be deemed a disciplinary offence and/or a criminal offence.
- Do add a disclaimer to your profile stating that opinions are your own.
- Personal accounts should not be used to comment on Social Media postings regarding SHBC on behalf of SHBC. For a consistent response employees

and workers should notify the Marketing and Communications Team for Council-related postings.

7.2 If employees and workers create a social networking site from Surrey Heath Borough Council, they should follow these guidelines:

- Do not engage in activities over the internet that could bring the Council into disrepute. Do not reveal information which is confidential or sensitive to the Council – consult your manager if you are unsure. Do not discuss existing or proposed policies on social networking websites.
- Do not include contact details or photographs of service users or staff without permission.
- Do not make offensive comments about the Council, members, colleagues, suppliers or residents of Surrey Heath on the Internet. This may amount to cyber-bullying or defamation and could be deemed a disciplinary offence and/or a criminal offence.
- Ensure naming conventions remain professional and where linked to an individual, forename and surname combination should be used

7.3 If employees and workers are considering any social networking campaigns they should firstly consult the Marketing and Communications Team for guidance.

7.4 Employees and workers should be mindful of the information they post on sites and make sure personal opinions are not published as being that of the Council. Misuse of such sites in a manner that is contrary to this and other policies could result in disciplinary action.

7.5 Employees and workers must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords which can make you vulnerable. In addition, employees and workers should:

- ensure that the correct privacy settings are set;
- ensure that no information is made available that could provide a person with unauthorised access to the Council and/or any confidential information.

7.6 If using social networks for investigations, e.g. recruitment or debt recovery, all staff must seek advice from Corporate Enforcement or Legal Services. Failure to do so may constitute a breach of the Regulation of Investigatory Powers Act (RIPA). No covert social networking profiles must be set up or used.

7.7 Social networking should not be used for decision making. They are only to be used for ideas and ad-hoc communication. Decisions should only be communicated via formal methods of communication that allows for a formal letter to be created and kept such as email.

7.8 If using video conferencing sites all staff must conduct themselves in a professional manner ensuring

- You do not use the messaging function within web conferences to share personal or confidential information.
- Meetings are not recorded unless all participants have consented to be recorded and processes are in place for the secure storage, retention and destruction of the recording.
- If the web conference is with members of the public a password to access the meeting is set.
- You are aware of your surroundings, ensuring no confidential or personal information is seen, this could include members of the public in the background.

If the discussion is of a confidential or sensitive nature the conference must take place in a private area

8. Legal issues and points around the use of social networking and websites

8.1 Employees and workers should be familiar with the legal areas outlined below before writing about colleagues or sharing information about the Council. Examples of social networking activities outlawed under the Consumer Protection from Unfair Trading Regulations include:

- Creating fake blogs ('ghosting')
- Falsely representing oneself as a customer
- Falsely advertising on social networking sites
- Libel and defamation

8.2 Employees and workers must comply with the UK General Data Protection Regulation and Data Protection Act 2018. In particular, not sharing personal or confidential information inappropriately, checking location of information if using new social networks and ensuring it is acceptable under the Data Protection legislation.

8.3 In the same way as email and text messages, certain uses of Social networking including MS Teams and WhatsApp may be subject to Freedom of Information Act and the Environmental Information Regulation. Staff should make every effort to avoid using these medias for Council business. Whereby they are used the message must be downloaded and stored in a appropriate place on the Council network.

8.3 Defamation

8.3.1 Defamation is the act of making a statement about a person or company that is considered to harm reputation, for example, by lowering others' estimation of the person or company, or by causing them to lose their rank or professional standing. If the defamatory statement is written down (in print or online) it is known as libel. If it is spoken, it is known as slander. There are exceptions to

this - posting a defamatory statement online or recording it on a podcast would both be examples of libel.

8.3.2 An organisation may be held responsible for something an employee has written or said if it is on behalf of the Council or on a Council-sanctioned space. The Council will take appropriate action in line with the disciplinary policy and procedure should a defamation incident occur. Action can also be taken against anyone repeating libellous information from another source, so careful checks are needed before quoting statements from other blogs or websites. This can also apply to linking to defamatory information. Staff should consider whether a statement can be proved before writing or using it - in law, the onus is on the person making the statement to establish its truth. An organisation that provides a forum for blogging can be liable for defamatory statements they host.

9. REPORTING PROCEDURE

9.1 As per the Council's Whistleblowing Policy and Data Security Breaches Policy, the Council encourages staff who suspect wrong-doing to report it, as it helps perpetuate the integrity of the Council, even if suspicion proves unfounded.

In the event you become aware of the misuse of social networking you should report this to your manager immediately. If reporting the incident to your manager is not possible please speak with Human Resources.

If an investigation into the misuse of social networking is required the Information Governance Manager may conduct the investigation.

Document revisions

Document revised (date)	Details of revisions made	Version
09/01/15	Updates	5
09/03/15	Updates	6
03/06/16	Updates	7
16/08/17	Updates	8
15/03/18	Updates	9
March 2021	Updates	10

Surrey Heath Borough Council
Employment Committee
6 April 2022

Organisational Change Policy and Procedure

Strategic Director/Head of Service	Louise Livingston
Report Author:	Julie Simmonds, HR Manager
Key Decision:	No
Wards Affected:	n/a

Summary and purpose
Review and implementation of a new look and more information Policy for use during Transformations.

Recommendation

The Committee is advised to RESOLVE that the revised Organisation Change Policy (previously referred to Employment Stability Policy) be adopted.

1. Background and Supporting Information

1.1 The Organisation Change Policy and Procedure (Annex A) replaces the existing Employment Stability Policy and Procedure which was last reviewed in 2009 (Annex B). As the Employment Stability Policy was reviewed a number of years ago there was a lot that needed to change regarding the layout and to ensure it was a lot more informative to staff in the event they find themselves in a proposed restructure of their Team or Service.

1.2 Key considerations/changes following consultation with the Joint Staff Consultative Group are attached at Annex C to this report

2. Reasons for Recommendation

2.1 Current policy needs reviewing to make it clear, less room for different interpretations and more informative.

3. Proposal and Alternative Options

3.1 Propose adoption of the new Organisational Policy and Procedure to replace Employment Stability Policy and Procedure.

4. Contribution to the Council's Five Year Strategy

4.1 Adoption of clear process for any Transformations for the benefit of SHBC and staff.

5. Resource Implications

5.1 n/a

Annexes

Annex A – Organisational Change Policy and Procedure
Annex B – Employment Stability Policy and Procedure
Annex C – Key considerations/ changes discussed with JSCG

ORGANISATIONAL CHANGE POLICY

Contents

Organisational Change - Overview

Who does this policy apply to?

It is the responsibility of Surrey Heath Borough Council to ensure that all employees, regardless of length of service who are affected by reorganisation and/or redundancy are treated fairly and consistently, in line with current legislation.

Where can I get more information?

If you need more information or advice once you have read this document, you should contact:

- A member of the Human Resources Team.
- Or a staff/trade union representative.

Employees responsibilities and entitlements under this procedure

- You have the right to be consulted personally and/or through your trade union representative on workforce and organisational changes
- You are entitled to be considered for suitable alternative employment, with a statutory four-week trial period
- You are entitled to receive assistance to help find another job, including time off to look for other work or to attend training
- If your post is declared redundant, you have the right to appeal against that decision

Human Resources responsibilities

- Human Resources will provide appropriate support and advice to managers and employees on the procedure and guidance on all related organisational processes such as consultation arrangements, redeployment procedures and requirements so as to ensure that redundancy issues are dealt with appropriately, in accordance with employment legislation and "Best Practice".
- Attend formal meetings to take notes, ask clarifying questions, provide advice on the procedure and ensure the meeting is conducted fairly.
- Ensure that any records are held in a confidential manner and in accordance with the principles contained within the Data Protection Act 2018.

Management responsibilities

- Provision of information to staff and the union representatives
- Consultation with staff and union representatives.
- Make recommendations relating to selection criteria to be used in the event of compulsory redundancy.
- Presenting the management's case at the appeal hearing
- In the absence of the above, this responsibility would be delegated to the most senior nominated person. Managers must seek advice before commencing any action under these procedures.

1. Introduction

From time to time it is necessary to review the services that the Council provides and the organisational structure that is required to deliver these services. To ensure that it continues to deliver quality services, changes may sometimes be required.

The Council is committed to avoiding compulsory redundancy, wherever possible, but sometimes it is unavoidable. Where a reduction in the number of employees is necessary, for example due to the re-organisation of departmental structures or budgetary constraints, alternatives to redundancy will be considered. The Council will consult about ways of reducing the numbers of employees to be dismissed and mitigate the consequences of dismissal.

The purpose of this policy and procedure is to provide a framework for ensuring the fair and reasonable treatment of all employees who are potentially affected by reorganisation and/or redundancy. The policy complies with relevant legislation and encompasses the redundancy consultation, selection, redeployment and contract amendment processes.

2. Definitions

Redundancy is a "form of dismissal which happens when an employer needs to reduce the size of its workforce" and occurs when:

- "The employer has ceased, or intends to cease, continuing the business", or
- "The requirements for employees to perform work of a specific type, or to conduct it at the location in which they are employed, has ceased or diminished, or are expected to do so".

Situations which may result in the need for redundancies could include:

- Amalgamation of departments
- Budgetary constraints
- Reorganisation of management or departmental structures

3. Objectives

To minimise the uncertainty and anxiety of staff affected by reorganisations and service reductions thorough consultation with individual staff and trade union representatives when reorganisations and/or service reviews are undertaken;

To minimise compulsory redundancies; and

To ensure that the Council retains the skills and expertise to ensure that it can meet future service needs.

4. Equality Impact Assessment

Equality Impact Assessment (EIA) is a systematic way of taking equal opportunities into consideration when making a decision, thus ensuring the organisation meets the requirements under the Equality Act 2010, and the public sector equality duty.

An EIA would be undertaken at the formative stage, so that it is integral to the restructuring/reorganisation as required. Undertaking an EIA does not delay or prevent managers from taking difficult decisions when restructuring / reorganising. Instead, it provides a record of the decision making process enabling managers to demonstrate their decisions are considered, fair, transparent and take account of the needs and impacts on different groups. For further guidance, please contact the Human Resources Manager.

5. Procedure

Stage 1 – Proposals and Consultation

- Informal Consultation

Employees will be informed as early as reasonably practicable that a reorganisation is being considered.

- Formal Consultation – Initial Proposals
  Consultation is a legal requirement and the Council will fully consult with staff where restructures and/or changes are proposed and where there is the potential for staff numbers to be affected. Where it is not possible to hold a face-to-face meetings, we will conduct the consultation process remotely. The Council's policy must be followed. The Trade Union and Labour Relations (Consolidation) Act 1992 provides Trade Union representatives with the opportunity of reasonable time for consultation and sufficient information to understand the requirement to reduce the workforce.

  If fewer than 20 staff are at risk of being dismissed there is no statutory requirement on the period of consultation. Best practice is to consult for a period of 30 days although in some instances a shorter period of consultation may be appropriate.

- **Statutory Notification Requirements**

  If between 20 and 99 employees may be dismissed as redundant, notification to the Secretary of State for Business, Energy and Industrial Strategy (BEIS) must be made 30 days before the first dismissals take effect.

  If 100 or more employees may be dismissed as redundant, at least 45 days notification must be given. These periods are the same as minimum periods permitted for consultation.

  The notification form is called a "HR1". It is obtained from the Redundancy Payment Office, or it may found on the internet at www.insolvency.gov.uk. The form is completed and submitted by Human Resources. The notice must be via the form and must be given in the specified manner. Although there are minimum periods over which formal consultation must take place

with employees and trade union representatives, consultation will begin at the earliest opportunity.

- ## Consultation document

The consultation stage of the process involves advising all relevant recognised trade unions and staff likely to be affected by any potential redundancies (before decisions which may result in redundancy). The manager, with advice from Human Resources, will then produce a consultation/briefing document which should outline the following:

Background

The reasons for the employer's decision

The number and descriptions of the employees at risk The total number of employees in each category

The proposed method for selection for dismissal

The proposed method of carrying out the dismissals, having due regard for the relevant notice periods that employees are entitled to

The proposed method of calculating redundancy payments. Current and proposed organisational charts

Impact on budget

If need be, a thorough job analysis should have taken place to identify and determine in detail the particular job duties and requirements.

Timescales including formal consultation meetings, 1-1 and date proposed new structure is proposed to come in to effect and the earliest date for redundancies to be effective.

Contact details for consultations

The consultation document will then be presented to the Chief Executive at CMT, if it is agreed that consultation can commence, then this should be circulated to the appropriate Trade Union prior to the first consultation meeting with the manager and Human Resources.

The consultation/briefing document should be given to affected staff, employee/trade union representatives so that they can make comments on the proposed changes. At the consultation meetings, the manager should outline the consultation/briefing document and address any questions from staff and employee/trade union representatives. Notes from the consultation meeting will be typed up by Human Resources and shared with the individual within 5 days of the meeting being held.

- ## Timeline

At the start of the consultation process, a timetable must be devised by Human Resources and the manager setting out prospective dates for the required stages of the redundancy process (e.g. end of consultation process, selection for redundancy meeting, redundancy appeal meetings). See Appendix 2

- ## During Consultation:

Meaningful consultation will be undertaken with a view to reaching agreement as to:

- ways of avoiding dismissals;
- ways of reducing the numbers to be dismissed; and ways of mitigating the consequence of any dismissals, which may include:

  natural wastage;

  restrictions on recruitment;

  consideration for voluntary redundancy;

retraining and redeployment to other parts of the Council.

reduction or elimination of overtime;

job-sharing,

reduction in hours;

termination of temporary or agency staff contracts.

Consultation with individuals should be taken throughout the reorganisation/ service review. At the end of the consultation period, the manager will consider any additional proposals and comments and an updated/final consultation document should be circulated to the affected staff and Trade Union Representatives. Care should be taken to ensure staff understand the timetable and process which would be followed.

Absent employees

All affected staff should be invited to the consultation meetings. Staff who are absent due to secondments, long term sickness, maternity/adoption/shared parental leave or career breaks should be included in redundancy consultation and selection processes in the same way as other affected employees, although it may be necessary to change how they are consulted if they are absent from work. Failure to properly consult these groups of staff about possible redundancy is likely to be unlawful discrimination.

Keeping Records

Copies of all letters sent during redundancy process should be retained and full notes of all formal meetings should be taken and retained on file for reference at later stages of the procedure.

5.2 Stage 2 – Measures to Avoid Compulsory Redundancies

The Council has a responsibility to its workforce to avoid compulsory redundancies wherever possible. Opportunities for redeployment and

retraining should be utilised in line with guidelines in this policy and the financial implication of these initiatives. Examples of minimising compulsory redundancies are listed above under "during consultation". Discussions with employees, Staff and trade unions can also include the following consideration:

- Seeking Volunteers for Redundancy

  If appropriate, staff should be asked to consider volunteering for redundancy before any method of selection for compulsory redundancy is put in to operation.

The Council must mitigate against the risk of losing workers with key skills and must ensure the retention of a balanced workforce, which is appropriate to meet the Council's future needs. Staff will not be disadvantaged on the grounds of any protected characteristic.

5.3 Stage 3 – Application of Selection Criteria

Below are examples of selection criteria that can be applied:

Assimilation

There are two categories of assimilation: direct assimilation and competitive assimilation.

Direct Assimilation

Where a review has taken place and a job remains the same or is only marginally different, the post holder should be assimilated without assessment. Staff will have assimilation rights, where there is a high match between the post in the current structure and the post proposed in the new structure.

Competitive Assimilation

This is where there is more staff than jobs available. Selection in these circumstances is by competitive interview between staff with assimilation rights. Appointment/s must be made to all posts as a result of this exercise.

Ring–Fenced Interview

This occurs when the essential requirements of the new and old job do not match but there are some similarities in the new job. All staff within the affected group should be interviewed. There is no requirement for appointments to be made to the new posts.

An employee put at risk may be offered an interview for all posts which could be deemed to constitute suitable alternative employment.

There is no right of appeal against the outcome of a redeployment interview but employees may request a feedback.

Qualitative Criteria/Exercise

Where the number of jobs in the new structure is less than the number of existing employees, objective criteria will be used to select for redundancies and may include, among other things, skills and qualifications, in addition to qualitative criteria, for example work performance (as identified through the Council's appraisal process); flexibility and attitude; attendance; timekeeping and disciplinary record. In using attendance as a selection criterion, it is essential that the reasons for, and extent of any, absences are clearly understood and discretion would be applied to those covered by the Equality Act 2010

In the case of any qualitative criteria being used, a comparative analysis of the information relating to all those in the area at risk will be undertaken.

Competitive Interview

In some cases, it will be appropriate for new posts to be advertised internally and externally. In this event, staff who have not been considered

for the post initially may apply and be considered competitively with other internal and/or external candidates.

Outcome of Selection Criteria

Once the change has been implemented, the manager will write to each member of staff letting them know the outcome as it affects them. In some cases, this may be a contractual change and therefore a copy should be placed on the Individual's Personnel/HR file confirming the variation to the contract of employment.

6 Notice Periods

Depending on length of service the Council must meet the statutory minimum periods of notice which are:

The Council will give the minimum notice in termination of employment as detailed in your Terms and Conditions of Employment. However, depending on length of service the Council must also meet the statutory minimum periods of notice which are:

Period of Continuous Employment	Minimum Notice
Four weeks or more but less than 2 years	1 week
Two years or more but less than 12 years	1 week for each year of continuous employment
Twelve years or more	Not less than 12 weeks of notice

6.1 Working during notice of dismissal

Staff who have not been successful in being appointed to new posts in the reorganisation will need to be given notice of termination and informed of their rights.

- Employees will normally remain at work during their notice periods.

- The Council may ask employees to carry out alternative duties during their notice period and this may be for a different part of the Council. Typically, this will be required where a post has been deleted but the employee's notice period has not expired. The Council will consult with the employee and will take individual circumstances into consideration.

- In exceptional circumstances, the council may agree for an employee to leave the organisation with pay in lieu of the notice period and without a redeployment search, where it is in the interests of both parties

- In exceptional circumstances, the Council may require employees not to attend work during their notice period but to be on call should their services be required. This is known as garden leave.

- If an employee requests to leave prior to the expiry of the notice period (even though there may be a possibility of redeployment), they will not be entitled to receive pay in lieu of the remaining period. Depending on the circumstances, the right to a redundancy payment could also be affected.

- During the notice period, the employee is entitled to reasonable time off to look for other employment, attend external interviews or training for future employment. The employee should follow normal processes for notifying their manager of planned time-off.

7 Suitable Alternative Employment

7.1 Offers of Alternative Work

Any reasonable alternative job offer should be put in writing, even where it is believed that it may be rejected. The offer should detail how the new employment differs from the old and must be made before the previous contract ends. The offer must be for the new job to start either immediately after the end of the old job, or after an interval of not more than four weeks, and include provision for a statutory four-week trial period. (Where the termination takes effect on a Friday, Saturday or Sunday, four weeks commences from the following Monday).

When determining if an alternative role within the organisation is 'suitable alternative employment' the following factors should be considered:

- the training, qualifications of the employee;
- previous experience
- whether the new job would represent a drop in earnings / status
- any problems involved for the employee if the employment is in a different place
- any evidence that similar offers had previously been regarded as suitable for the nature of employees affected.

It should be made clear to the employee that an alternative job offer is considered by the Council to be 'a suitable alternative job offer' and that refusal to accept the offer will lead to the loss of redundancy and severance entitlements. Only if the employee has reasonable grounds for refusing the alternative post will redundancy entitlements be retained.

If the employment offered is considered to be 'suitable alternative employment' and the employee refuses the offer, the manager, in consultation with the Human Resources Manager will consider the employees reasons for refusing the offer. If it is considered that the employee

has reasonable grounds to refuse the offer, alternative employment will continue to be sought and the employee will retain their entitlement to redundancy payments. If the employee's reasons for refusal are not considered to be reasonable, the employee will be informed and entitlement to redundancy and severance payments will be lost.

Should an employee refuse an offer of employment that is not considered to be 'suitable alternative employment', they will retain their right to a redundancy payment and further redeployment opportunities will continue to be sought.

The Council, as in all areas of its employment practices, will seek to make reasonable adjustments for employees with disabilities in relation to redeployment.

7.2 Statutory Trial Period

An employee who is under notice of redundancy has a statutory right to a trial period of four weeks in an alternative job where the provisions of the new contract are materially different from the original. During the trial, the employee can assess the suitability of the job and the line manager can assess the suitability of the employee.

A formal job offer made through redeployment initiatives, which includes a statutory trial period, should either accompany the formal notice of redundancy or be sent as soon as possible thereafter.

This trial period can be extended to a maximum of 8 weeks, for retraining purposes only, by written agreement of both parties, setting out the date on which the trial period ends and the employee's terms and conditions after it ends. Agreement to a longer trial must be reached before any trial period begins and specific reference should be made to the retraining aspects of the post that lead to the requirement for an extended trial. At least four weeks of the trial period must be performed after the expiry of the original contract to meet statutory requirements.

If the trial period is successful, employment in the new job will continue and the employee will have no further entitlement to a redundancy payment.

7.2.1 Unsuccessful Trial

If the employee commences a trial period but consideration is being given to terminating the new contract within or at the end of the four weeks, by the employer or the employee, the employee will be invited to a meeting with the appropriate manager and a Human Resources representative to discuss the implications. Whether or not the employee will retain their entitlement to redundancy and severance payments will depend upon, as a minimum, the following factors:

- the suitability of the alternative post offered
- any reasons put forward by the employee as to why the post offered may not be a suitable alternative
- any failure by the employee to fully co-operate during the trial

The outcome of the discussions and decisions taken at this meeting will be confirmed in writing.

If the termination was due to a reason unconnected with redundancy, e.g. misconduct, there will be no entitlement to redundancy or severance payments. Full contractual notice will have been given to coincide with the day on which the previous contract ended. No further notice will therefore be due if the employment is terminated during or at the end of the four week trial period.

8. Salary Protection Arrangements

Where an employee is redeployed to a post which is lower graded than their previous post, protection will apply for up to one grade

difference only. The employee will receive pay protection for a period of twelve months after which the rate of pay for the lower paid job will apply.

Protection will apply to basic pay for the employee's substantive post only. Additional payments such as overtime or Essential User Car Allowance and any other allowances, enhancements or benefits relating to the employee's previous post or working patterns are excluded from protection.

It is the hourly rate of pay that is protected. If the hours of the new post vary from the old post, the protected salary will be paid for the contracted hours worked in the new post only. For example if the individuals deleted post was for 37 hours and the job holder was on Spinal Column point 4.18 but the new post is for 30 hours on Spinal Column Point 4.17 the hourly rate of Spinal column 4.18 is protected and the individual will be paid this hourly rate for 30 hours.

Performance related pay awards will be applied as applicable to the post to which the award relates in the year that redeployment takes place. i.e. If an increment is awarded for performance in the old, higher graded post, protection will be recalculated incorporating the higher point on the substantive scale that the employee would have achieved.

9 Agreement to dismissal on the grounds of redundancy

All potential redundancies will be referred to the Human Resources Manager who will co-ordinate and oversee the process. Trade Union Representatives (where appropriate) will be informed of all potential redundancy situations. Redundancy dismissals must be agreed by Chief Executive (or the Chief Executives designate) in consultation with the HR Manager/Head of HR, Performance and Communications before they are actioned.

10. Redundancy Payments

Where an employee is made redundant and has over 2 years continuous local government service, the following conditions shall apply:

(i)The redundancy payment shall be based on all continuous Local Government Service up to a maximum of 20 years.

(ii)All redundancy pay will be calculated on age, the contractual weeks' pay (except where the statutory redundancy pay limit is greater) and number of years in the job. You can calculate your statutory redundancy pay here.

(iii)Contractual entitlement or statutory provision, whichever is the greater, up to a maximum of twelve weeks pay will be paid

Any redundancy payments made under this scheme which are related to length of Local Government service shall exclude any period of service in respect of which a redundancy payment has already been made.

Any requirement for repayment of training, upon the termination of employment with the Council will be waived in respect of staff being made redundant

11. Pension payments

When the employee who is being made redundant is 55 years of age or over and has been a member of the Local Government Pension Scheme for two years or more, they will receive the current value of their pension immediately, on the termination of their employment.

This applies in the case of both voluntary and compulsory redundancies.

Redundancy Payments	Regulation 5, Compensation Regulation 2006	Whether to base redundancy pay on actual pay where actual pay exceeds the statutory maximum under the Employment Rights Act 1996 (£508.00 from April 2018).	Surrey Heath Borough Council will base the calculation of a week's pay for redundancy on actual pay if it is higher than the statutory limit.	Both the Executive Head of Transformation and the Head of Paid Service.
Compensation for loss of Employment	Regulation 6, Compensation Regulations 2006	Whether to pay compensation to a person whose employment ceases • by reason of redundancy; • in the interest of the efficient exercise of the employing authority's functions; or in the case of a joint appointment, because the other holder of the appointment leaves.	Surrey Heath Borough Council will only award compensation for loss of employment in exceptional circumstances.	Both the Executive Head of Transformation and the Head of Paid Service.

Please refer to the Pensions Discretion Policy for further information.

12 Stage 4 - Appeals procedure

There will be a right of appeal against redundancy decisions to the Chief Executive (or the Chief Executives designate). Appeals must be lodged within 10 working days, of the decision being confirmed in writing, setting out the grounds for the appeal.

Grounds of appeal can either be the following:

The employee appealing against the decision; to be made redundant has to submit an appeal in writing based on either the following grounds:

- The Organisational Change procedure was not followed and applied properly.
- The employee's post should not be deleted as it is not a redundancy situation.
- The selection criteria has not been applied fairly or objectively.

Possible outcomes of an appeal are:

- Appeal rejected and no change to the decision to dismiss on grounds of redundancy
- Appeal successful, in which case the manager may have to return to stage 1 of the procedures.

13 Support for redundant employees/staff "at risk"

Additional assistance

All employees should speak to Human Resources if they have further queries. Redundancy can be traumatic experience for employees especially for staff who have worked for many years in a stable environment. The Council has an employee assistance service, which is provided by Employee Assistance Helpline.

Appendix 1 – Summary of Stages

Stages	Summary of actions
Informal Stage	Commence consultation with staff Brief staff on background and reasons for change. Engage staff and seek ideas/comments to inform final proposal. Outline timeframe, process and, method by which to be consulted.
Liaise with HR with draft formal consultation document	
Stage 1 - Proposals and Formal Consultation	Consultation with staff and union: Proposal considered by Chief Executive at CMT; if approved then consultation commences with the following outlined: Number and description of roles (current job analysis) Current and proposed organisation charts Proposed method of selection Proposed method of carrying out dismissals Proposed method of calculating payments
Stage 2 – Investigate methods of avoiding compulsory redundancy	The Manager, with support from Human Resources, investigate ways of avoiding compulsory redundancy, including: Natural Wastage / Job Sharing / Reduction in hours / Restriction on recruitment / Reduction or elimination of overtime / Termination of temporary or agency staff
Stage 3 – Application of criteria	Revises criteria if necessary following consultation Adopts criteria for selection Informs affected staff about the result of selection (in writing) Chief Executive at CMT considers restructure and redundancy dismissals
Stage 4 – Appeal Procedure	Employee appeals against dismissal. Appeal Hearing Manager/ Chief Executive: Makes its decision – which is final Notifies decision to employee in writing.

Appendix 2 – Sample Timetable

Start Date	Actions	Responsibility
As early as possible	Initial consultation with recognised trade union and staff on potential redundancies, where possible. Manager identifies number of posts but not names.	Senior Manager
Date	Formal consultation starts	
Follow statutory timeline if more than 20 staff	Initial proposal considered by Chief Executive at CMT; if approved then consultation commences: Conducts meeting with trade union and staff in impacted area(s) Proposed consultation document circulated Proposed method of selection Proposed method of carrying out dismissals Proposed method of calculating payments and estimates for impacted staff Discussions on pension implications	Chief Executive, Senior Manager and Human Resources
During consultation	Further joint meetings if necessary and 121 meetings. Encourages questioning	Senior Manager and Human Resources
After consultation (30 days)	Conclusion of formal consultation	
1 week after consultation ends	Chief Executive takes final decisions on restructure and, if appropriate, posts to be lost Consider selection criteria and methods to be used, taking account of matters raised by staff and trade union during consultation Letters to trade union and staff informing them of the outcome of the consultation period and the chosen selection criteria	Chief Executive, Senior Manager with support from Human Resources
1 week after conclusion of consultation letter is sent out	Administering selection criteria	Senior Manager
1 week after selection tests	Staff are notified of selection criteria	Senior Manager
1 week after outcome of tests	Issue of notice of termination due to redundancy	Senior Manager and Human Resources
Date:	Search for suitable role in the Council – redeployment opportunities	Senior Manager and Human Resources

Date:	Appeal	Chief Executive and Human Resources
Date:	Outcome of appeal sent in writing	Chief Executive
Date:	Implementation of new structure	Senior Manager and Human Resources

Appendix 3 Frequently Asked Questions

What is the correct procedure for managing change?

The correct procedure for managing change includes consultation with staff and unions, advising of the proposed structure, proposed selection criteria and consideration of alternatives proposals put forward by staff.

What should the consultation be about?

Consultation must be undertaken 'with a view to reaching an agreement' and must cover ways of avoiding dismissals, reducing the numbers to be dismissed and setting out the consequences of the dismissals. Therefore during consultation employees are asked to put forward proposals/ideas for the new structure. However the organisation is not obliged to adopt all or any of the proposals put forward by the employees.

Can I volunteer to be made redundant?

You can, and it will be considered. This is normally requested by the employee during the consultation period and there is no automatic right to this. Request for voluntary redundancy would be approved as per management discretion and service needs.

When will I know if I'm being made redundant?

At the end of the consultation period staff will be provided with a copy of the final consultation document which will state the new structure and implementation date. Following the selection process, staff that are at risk of redundancy will be given formal notice of redundancy in writing; at this point they will be considered as a redeployee until the end of their notice period.

What selection process will be used?

Direct assimilation will occur where there is a high match between the post in the current structure and the post proposed in the new structure. If, however there are more staff than jobs available then competitive assimilation will take place and all staff with assimilation rights will be interviewed for the post and the appropriate appointment will be made.

What options are available if I don't have assimilation rights?

When the essential requirements of the new and old job do not match but there are similarities in the new job, all staff that are at risk of redundancy, who are at a similar grade should be interviewed to determine suitability to post. This is called ring-fenced interviewing.

If there are new posts in the structure will they be advertised externally?

It may be appropriate to advertise internally and externally. Staff not considered for the post initially as part of the selection process will still have the option to apply.

What right do employees who are under notice of redundancy have to take time off work?

Staff that are at risk of redundancy have the right to take reasonable paid time off work to look for new employment or make arrangements for training for future employment. What is 'reasonable' will depend on the individual circumstances of the case and will also be down to the discretion of the line manager.

Will I be offered alternative employment?

Employers should, where possible, make an offer of suitable alternative employment. The employee should also actively seek employment.

If more than one staff (in the redeployed pool) are interested in a suitable alternative vacant role, you will still be required to complete an application form and be interviewed to determine suitability to post.

Under the Employment Rights Act 1996, the employee will not be entitled to a redundancy payment if they unreasonably refuse a suitable alternative offer or unreasonably terminate the contract during the trial period in the new role.

If alternative employment is found, will I be able to try out the new job?

Yes, the employee is entitled to a four-week trial period in the new job. The trial period may be extended for the purposes of retraining (if appropriate), but only if the agreement is made in writing before the employee starts work under the

new contract and it specifies the date on which the period of retraining will end and the terms and conditions that will then apply.

If during the trial period the employee or employer terminates the new contract, the employment will still be ended by reason of redundancy on the date on which employment on the old contract ended.

Can there be more than one trial period regarding suitable alternative work?

Yes. If it becomes apparent during a trial period that the new job is unsuitable, the employer can offer an alternative, if available.

In a redundancy situation can I refuse an offer of suitable alternative employment?

An employee can't be forced to accept an offer of alternative employment; however if the offer is not taken the right to a redundancy payment will be lost.

Also if alternative employment is found which you take and there is no break in service, the right to a redundancy payment will be lost.

If I'm offered a less paid position, will the organisation be obliged to continue paying me at the same level?

Pay protection is for a maximum of 12 months in line with your terms and conditions of employment.

If I am made redundant will I be offered a redundancy payment?

To be eligible for a redundancy payment, an employee must be continuously employed for a period of not less than two years.

How is redundancy calculated?

Redundancy is calculated according to a person's age & length of service at the intended last day of service. This provides the number of week's

redundancy a member of staff is entitled to which is then multiplied by the current weekly salary. Note, only current hours worked & salary earned is taken in to consideration for redundancy purposes.

APPENDIX H

EMPLOYMENT STABILITY POLICY
(Revised September 2009)

1.0 Introduction

It is the policy of the Council to avoid redundancy, wherever possible. Where it is necessary to consider redundancy, alternatives will be considered, wherever possible. In pursuance of its policy to avoid redundancy the Council will consult about ways of reducing the numbers of employees to be dismissed and mitigate the consequences of dismissal.

2.0 Avoiding Redundancy

The Chief Executive will, in consultation with the Director of Corporate Services, the Head of Corporate Resources, the Service Head concerned, Human Resources Manager and the staff and union representatives, fully explore any alternatives to redundancy. Alternatives may include the:

(i) review of and reduction in overtime working;

(ii) redeployment of employees, who might otherwise become redundant, to other vacant posts for which they might be suitable or to other areas of work where employees at risk might be redeployed;

(iii) restrictions on recruitment to similar posts;

(iv) review of work undertaken by consultants or contractors to establish whether any of this work can reasonably be transferred to Council employees whose jobs are at risk;

(v) approaching neighbouring local authorities to explore whether there are any suitable alternative roles for staff at risk of redundancy to transfer into; and

(vi) where practicable, temporary secondment or transfer of displaced staff where it is foreseen that they can be absorbed into a substantive post within a reasonable period of time, subject to periodic review.

3.0 Consultation Process

3.1 The Council will make every effort to consult with staff where restructures and/or changes are taking place and where there is a likelihood of staff numbers being affected.

3.2 As a guide, a Head of Service will consult with all affected staff about any proposals, allowing them a reasonable period of time to respond with alternative and/or additional suggestions to achieve a more effective outcome for the Service. Where appropriate, the Head of Service will include staff suggestions within proposals put forward to the Management Board for consideration. Staff will be advised of any suggestions that were not suitable for adoption and a reason why.

3.3 Staff will be advised of any changes Management Board make to the proposals before the final recommendations are put before the Executive.

3.4 With effect from the Executive's decision to disestablish posts from the establishment, the incumbents of these posts will be placed at risk of redundancy. A letter confirming this will be sent to the affected staff, explaining the reason(s) why they have been placed at risk, their right to request voluntary redundancy and their right to appeal the decision, should they so wish.

3.5 Any employee who is aggrieved by a decision to declare them redundant will have the right of appeal. If however, the grievance does not relate to the redundancy decision but to the operation of the procedures outlined in this document, it will be dealt with under the Council's Grievance Procedure.

3.6 Where a job is deleted and there is more than one person undertaking similar jobs, they will all be placed at risk of redundancy.

3.7 All staff at risk of redundancy will be ring fenced and given priority consideration for suitable alternative roles, through the normal recruitment process.

4.0 Voluntary Redundancies

4.1 Where possible, redundancy should first be considered for those who volunteer for redundancy.

5.0 Compulsory Redundancies

5.1 Where compulsory redundancies are required the Council will apply objective selection criteria, which may include considering an employee's qualifications, skills or competencies, suitability for retraining or redeployment and their sickness record. The criteria must be relevant to the requirements of the service and the job role and must be applied objectively to each potential candidate for redundancy.

5.2 When all suitable alternatives have been exhausted and the final decision to make an employee redundant has been made, they will:

(i) have their entitlement to redundancy payments fully explained to them;

(ii) be considered for appointment, secondment, transfer or redeployment to any suitable vacancy which might arise during their period of notice;

(iii) in the event of being redeployed, be offered suitable retraining for the new post;

(iv) be given all possible assistance (including reasonable time off on full pay) in finding alternative employment and pursuing agreed training opportunities;

(v) be entitled to attend redundancy or retirement counselling sessions at the Council's expense; and

(vi) have the right to a reference from the Council for use in finding alternative employment.

5.3 Where all the alternatives to redundancy have been explored and more than twenty staff are to be made redundant, the Council will consult with the trade union and staff representatives at the earliest opportunity and not later than the minimum period prescribed by law and will disclose the following information:

(a) the reason for the proposals;

(b) the numbers and the description of the employees at risk;

(c) the total number of Council employees affected by the proposal;

(d) the proposed method of selecting for redundancy;

(e) the proposed method of carrying out the dismissals; and

(f) the proposed method of calculating the amount of redundancy payments to employees who may be dismissed by reasons of redundancy.

5.4 Where there are to be twenty or more redundancies the Head of Corporate Resources will, in accordance with statutory requirements, notify the Department of Education and Employment of the proposed redundancies and will liaise with it on all matters subsequently arising as a result of the redundancies.

6.0 Redundancy Payments

6.1 Where an employee is made redundant and has over 2 years continuous local government service, the following conditions shall apply:

(i) The redundancy payment shall be based on all continuous Local Government and other relevant Service up to a maximum of 20 years.

(ii) All redundancy pay will be calculated on the contractual weeks pay except where the statutory redundancy pay limit is greater.

(iii) Contractual entitlement or statutory provision, whichever is the greater, up to a maximum of twelve weeks pay will be paid either in lieu of unworked notice or in breach of contract.

6.2 Any redundancy payments made under this scheme which are related to length of Local Government service shall exclude any period of service in respect of which a redundancy payment has already been made.

6.3 Any requirement for repayment of training, disturbance allowances or termination charges under the Council's Provided Car Scheme, upon the termination of employment with the Council will be waived in respect of staff being made redundant.

7.0 Redeployment

7.1 The Council, in discussion with the employee, will decide whether a post is considered to be suitable alternative employment and that decision will be made taking into account job content, the terms and conditions applicable to the post and location. An employee who rejects an offer for suitable alternative employment will lose their entitlement to redundancy pay. An employee who disagrees with the decision of the Council with regards to the suitability of employment will have the opportunity to appeal to the Chief Executive.

7.2 Where an employee is redeployed to another post they will be allowed a "settling-in" period of up to 4 weeks, or up to a maximum of 8 weeks by agreement of the employee and the Chief Executive after consultation with the Head of Corporate

Resources and the Human Resources Manager, during which time either the Council or the employee may terminate the arrangement if either shall find it to be unsuitable.

7.3 The appropriate redundancy benefits will then be paid, subject to the employee having made every effort to learn and apply the new skills required for the job and no other suitable alternative roles being available in the foreseeable future.

7.4 In the event of redeployment to a post carrying a lower salary, a reduction in salary shall occur 2 years after the redeployment commenced.

7.5 In the event of redeployment proving unsuitable the redundancy benefits applicable will be paid upon notification that the employee has been dismissed on grounds of redundancy.

8.0 Additional Benefits

In addition to the statutory redundancy payment the Council may also authorise the following benefits:

(i) The immediate payment of normal retirement benefits to those aged 55 and over, under the Local Government Pension Regulations 1995 as amended.

(ii) Enhancement of the statutory redundancy payment to those in the pension scheme by a multiplication factor of 2.0.

(iii) All additional redundancy payments will be made:

(a) to include all continuous Local Government Service irrespective of employer, up to a maximum of twenty years;

(b) based on actual salary if above the current statutory redundancy maximum pay; and

(c) the Council may, in appropriate cases, make payment of a lump sum for frustration of the employee's contact up to a maximum of 12 weeks pay.

The extent to which any or all of the benefits set out above will be applied in an individual case of proposed early retirement will be considered by the Council on its merits.

9.0 Selective Voluntary Early Retirement Scheme

9.1 Purpose

The Council recognises that longer serving employees, after years of productive service for the Council can reach a point where they would value a change in their work/life balance or feel that they no longer have a fresh contribution to make. Whilst the most usual course of action in these cases is for the employee to seek alternative employment, it is recognised that in certain cases alternative options should be considered.

It is stressed that this does not cover a redundancy situation but is an opportunity for

an individual employee to request that they be considered for early retirement to the mutual benefit of themselves and the Council. The scheme is designed to allow for the possibility of a suitable arrangement to be made where there is a degree of benefit on both sides.

This scheme is not to be used in cases where issues of capability, health or disciplinary matters are under consideration as there are appropriate policies dealing with each of these matters.

The purpose of the Early Retirement Scheme is to improve the council's efficiency by giving eligible officers the opportunity to leave the Council's service early upon receiving compensatory benefits. The cost of such benefits must be recouped within the same financial year and will be made by:

(i) either the non-filling of the resultant vacancy or of another vacancy in a related post which has arisen as a result of a staffing restructure made possible by the creation of the original vacancy; or

(ii) the ability to fill the resultant vacancy on either a lower salary grade or for less hours each week; or

(iii) an eventual saving resulting from the appointment of a more motivated member of staff and who would achieve an improved service provision

9.2 Eligibility

Staff will be eligible to benefit from the Early Retirement Scheme if they are:

(i) a pensionable employee currently in the scheme with qualifying service of not less than 5 years;

(ii) not less than 55 years of age;

(iii) prepared to leave the employment of the Council before the statutory age of retirement; and

(iv) agreed by the Council for mutual termination of employment in the interests of the efficiency of the service.

Staff under 55 years of age who are in the pension scheme may also benefit from this scheme but will not receive immediate pension benefits, these being deferred to normal retirement date in the usual way.

9.3 Scheme Compensation Benefits

The Council has the discretion, under Regulation 52 of the Local Government Pension Scheme, to make a compensatory payment by giving eligible staff up to 6 and 2/3rds years additional service, with all costs incurred being recouped within the same financial year.

9.4 Procedure

(i) Any member of staff who meets the criteria set out above and wishes to leave the service early should in the first instance discuss the matter with their

Service Head. Subject to their agreement, the individual should inform the Human Resources Manager in writing. The Service Head will be required to prepare a business case for the proposal for consideration by the Chief Executive.

(ii) The Chief Executive and the individual employee will agree the terms of the compensation having regard to the cost to the Council.

(iii) Compensation benefits will include up to 6 and 2/3rds added years, payment of the pension within any existing elements of the 85 year rule, and removal of the actuarial reduction for paying pension early.

(iv) In the case of the Chief Executive, Directors and Service Heads, the business case will be prepared for consideration by the Executive and any terms will be agreed by the Chief Executive and the Leader of the Council, in the case of the Chief Executive, any terms will be agreed by the Leader of the Council and the Head of Corporate Resources.

(v) As the scheme requires mutual agreement, there is no right of appeal.

10. Dismissals

10.1 The Executive will be advised where a dismissal occurs as a result of redundancy, early retirement on the grounds of redundancy or through voluntary early retirement.

10.2 Individual consultation will be a key part of the redundancy consultation process, to allow affected employees to present proposals and alternatives to redundancy.

Consultation Feedback - Suggested Position vs Staff Rep Position on reviewing SHBC Employment Stability Policy

	Present Policy	Suggested amendments	Staff Representative Suggestions (pre JSCG meeting)	Members comments (pre JSCG meeting)	Outcome from JSCG
Multiplier	Currently x1 multiplier used on weekly salary. There is a discretion of increasing this to x2 multiplier on the weekly salary.	Keep the x1 multiplier on weekly salary but remove the discretionary element.	The multiplier to be acknowledged as 2, not discretionary. The removal of the multiplier to be introduced over a period 2-3 years, on a sliding scale. We believe this acknowledges and addresses the council's need to ensure minimum costs in a redundancy situation. Whilst also addressing staff concerns over the removal of previously held perceived support and benefits. A softer and more transparent approach will be beneficial to morale. Cost is minimal when considering the number of staff likely to be affected. Use actual weeks' pay when calculating redundancy payments but use the statutory amount for the grades where it is greater than weekly pay. Real concern that SHBC is moving to the bottom in comparison to other Surrey Councils. See benchmarking information.	• Discretion, if it is to remain then must be very clear it is a discretion and clarify when it might be used • Suggested discretion of x1.5 instead of the existing x2 • Following on from above, conversations lead to circumstances when discretions could be used and no examples came to mind for a redundancy situation • Remove discretion completely so there is no ambiguity • Remove discretion but have x1.5 multiplier instead of x1 for next 2-3 years then it reverts back to x1 multiplier	• Remove the discretion and add 1.5 multiplier for the period up to 31st Mar 2023 with all restructures started before this date to have this multiplier applied • Staff reps agree with this but with a date of 31st March 2024

Protected salary	Currently 2 years protected salary and no restriction on what grade a role can be considered for as part of the redundancy process. No clarity as to whether this includes any additional allowances.	Reduce the term of the protected salary to 12 months. State it can only be applied if someone accepts a role one grade down from their redundant post. If someone does want to go to a role which is more than 1 grade then they do so without protected salary and take the role at the new grade therefore keeping continuous service. Alternatively, they can still take redundancy but will lose continuous service and will not be able to work in local government for 1 month (4 weeks to be precise) to constitute the break in service. See Modification Order here	Agree to move from 2 years protected salary to 12 months. For 1 grade drop. With regard to not allowing salary protection where there is a drop of more than 1 grade below substantive post. We recommend that this is considered, retained for 6 months. As this would be preferable where the individual is willing, rather than subjecting the Council to the cost of recruitment, redundancy cost and the loss of corporate knowledge.	• Agreement to reduce to 12 months from 2 years • Happy with suggestion from Staff Reps to keep the ability to go more than 1 grade drop but only keep protected salary for 6 mths or possibly 9 mths • General feeling of reasonable suggestion from Staff Representatives	• Agree to move from 2 years protected salary to 12 months. For 1 grade drop. • 6 months protection for more than one grade drop.
Notice periods	Currently we ask staff to work their notice period if they are being made redundant. No	Make it clear notice will need to be worked. Discuss if there are any situations where 'payment in lieu of notice' or	Would like the opportunity for payment in lieu of notice to be retained	• General rule staff work their notice and use up any annual leave but having other options like 'payment in lieu of notice' and 'garden leave' can be useful option for Employers	• General rule staff work their notice and use up any annual leave. The employer will have the option of 'payment in lieu of notice' and/or 'garden leave'.

	t clear in existing policy.	Garden leave would be applicable.			
Voluntary Redundancy	No enhanced payment for this. It would be a request as part of a restructure any staff put at risk can put in a VR request.	As is. But clarity around whether this could shorten the restructure if VR was approved	Agree Voluntary redundancy should remain as an option. Would recommend for consideration the opportunity where skills and ability are similar, and cost is the same or less, that there is an opportunity to swap packages. Allowing someone who wishes to leave to take the place of a colleague who doesn't.	• Keep this and generally good practice to allow someone to go under VR rather than compulsory redundancy • Suggestion of enhancement to 1.5 multiplier	• VR to be kept as an option and it is best practice
Link to Pensions and Pension Discretions Policy	Not clear and not linked in current policy	Clarity around pensions particularly around redundancy situations.	There is a general lack of understanding around the effect of redundancy on the individuals pension. Specifically around the 'pensions strain' whether there are enhancements that would benefit the individual being make redundant. We would like additional information or a link to the information included within the policy. Is there an opportunity to consider an enhancement in a redundancy situation?	• Not discussed	• Pension Discretions explained and pension strain explained and to be included in the document. • Retirement Policy has been added to the work programme for Jan alongside the Pension Discretions Policy
Outplacement			Would like outplacement for all staff	• In principle agree this should be available to all staff who are made redundant	• All in agreement to support outplacement
Policy to be Informative as to the processes to be followed	Current policy is old and out of date. Does not answer a lot of questions someone in a restructure process would need.	Make it a lot clearer and try to include the process as fully as possible but not tying ourselves in knots IF there is any reason why a restructure may need to be	Agree and confirmed they like the new layout	• Policy layout not discussed • Page 12 punctuation needs correcting • Make clearer that the minimum period of consultation is 30 days	

		slightly different. There would never be a reason to deviate from ACAS guidance and Gov legislation.			

Surrey Heath Borough Council
Employment Committee
6 April 2022

Work Programme 2022/23

Head of Service **Louise Livingston – HR, Performance & Communications**
Report Author: **Julie Simmonds – HR Manager**
Key Decision: **No**
Wards Affected: **n/a**

Summary and purpose
To agree the work programme for the 2022/23 municipal year.

Recommendation

The Committee is advised to RESOLVE that the work programme for the 2022/23 municipal year be agreed, as set out at Annex A.

1. Background and Supporting Information

1.1 At each meeting the Committee will consider the work programme, be advised of updates and agree amendments as appropriate.

1.2 Meetings have been scheduled for the 2022/23 municipal year as follows:

- 14 July 2022
- 13 October 2022
- 26 January 2023
- 30 March 2023

2. Proposal and Alternative Options

2.1 It is proposed that the Committee considers the list of topics listed in Annex A of the work programme and makes such amendments as appropriate.

Annexes

Annex A – proposed Work Programme for 2022/23

Annex A

Employment Committee
Work Programme
2022/23

Consultative Group meetings for the municipal year are scheduled to be held on the following dates:

- 14 July 2022
- 13 October 2022
- 26 January 2023
- 30 March 2023

The following work for the 2022/23 municipal year has been identified for consideration by the Committee.

Meeting	Topic	Source
14 July 2022	**Christmas Closure**	**HR (new)**
	Vexatious & Persistent Complaints Policy	**Contact Centre Manager (review)**
	Pay Policy Statement	**HR**
	Pay negotiations process	**HR**
13 October 2022	**Leave and Special Leave**	**HR (review)**
	Sickness Absence Policy	**HR (review)**
	Agile Working Policy	**HR (review)**
	Expenses Policy	**HR (review)**
	Speak Up Policy annual report	**HR**
	Car and Road Users Policy	**HR (review)**
	Staff Terms and Conditions of Employment	**HR (review)**
	Pay negotiations 2023/24	**HR**
26 January 2023	**Pensions Discretion Policy –**	**HR (review)**
	Pay Settlement 2023/24	**HR**
	Family Friendly Policy	**HR (review)**
30 March 2023	**Pay Settlement 2023/24**	**HR**
	Data Breaches Policy	**ICT/Information Governance (review)**
	Information Security Policy	**ICT (review)**
	Data Protection Policy	**ICT/Information Governance (review)**
	Social Networking Policy	**ICT/Information Governance (review)**