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: Corporate

Please ask for: Rachel Whillis

Direct Tel: 01276 707319

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

Wednesday, 17 March 2021

To: The Members of the **Employment Committee**
(Councillors: Colin Dougan (Chairman), Cliff Betton (Vice Chairman), Sharon Galliford, Josephine Hawkins, Rebecca Jennings-Evans, Alan McClafferty, Sashi Mylvaganam, 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, Adrian Page, Morgan Rise and Kristian Wrenn

Dear Councillor,

A meeting of the **Employment Committee** will be held on **Thursday, 25 March 2021 at 7.00 pm**. The agenda will be set out as below.

Please note that this meeting will be recorded and live streamed on https://www.youtube.com/user/SurreyHeathBC

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.

To agree the minutes of the Appointments Sub Committee meeting held on 30 September, 12 October and 19 October 2020 and 17 February 2021 and to ask the Chairman of this meeting to sign the minutes.

13 Exclusion of Press and Public

The Committee is advised to RESOLVE that, under Section 100A(4) of the Local Government Act 1972 (as amended), the public be excluded from the meeting for the following items of business on the ground that they involve the likely disclosure of exempt information as defined in the paragraphs of Part 1 of Schedule 12A of the Act, as set out below:

Item	Paragraph(s)
14	1
15	1

Part 2
(Exempt)

Report to be circulated separately.

To review those items or parts thereof which can be released as information available to the public.

Minutes of a Meeting of the Employment Committee held on 28 January 2021

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

+	Cllr Sharon Galliford	+	Cllr Sashi Mylvaganam
+	Cllr Josephine Hawkins	+	Cllr Graham Tapper
+	Cllr Rebecca Jennings-Evans	+	Cllr Victoria Wheeler
+	Cllr Alan McClafferty		

+ Present

Members in Attendance: Cllr Peter Barnett, Cllr Rodney Bates and Cllr Valerie White.

25/EC Minutes

The minutes of the meeting held on 8 October 2020 were agreed and would be signed at the next available opportunity.

26/EC Grievance Policy and Procedure for Statutory Officers and non-Statutory CMT members

The Committee was informed that the Grievance Policy and Procedure for Statutory Officers and non-Statutory CMT Officers introduced in 2019 had been reviewed. The Policy had been amended to ensure that complaints were handled in line with the procedures set out in the Council's Constitution. In addition, the Policy had been updated to ensure it consistently referred to 10 working days' notice.

RESOLVED that the revised Grievance Policy and Procedure for Statutory Officers and non-Statutory CMT Officers, as set out at Annex A to the agenda report, be agreed.

27/EC Disciplinary Policy and Procedure for Statutory Officers and non-Statutory CMT members

The Committee was informed that the Disciplinary Policy and Procedure for Statutory Officers and non-Statutory CMT Officers introduced in 2019 had been reviewed. The Policy had been amended to change references from five working days to ten working days. References to committees and sub committees had also been updated to reflect the procedures set out in the Council's Constitution.

It was noted that the procedures concerning the appointment of independent investigators from a list provided by the Joint Negotiating Committee Joint Secretaries referred to in paragraphs 8.2.2 and 8.3.2 were in line with standard practice.

RESOLVED that the revised Disciplinary Policy and Procedure for Statutory Officers and non-Statutory CMT Officers, as set out at Annex A to the agenda report, be agreed.

28/EC Pensions Discretion Policy

The Committee was informed that the Council was a participating employer in the Local Government Pension Scheme (LGPS) and, as an employer, was under a under a legal duty to prepare and publish a written statement of its policy relating to certain discretionary powers under the Regulations which applied to the LGPS. The Council also had a duty to formulate, publish and keep under review a Statement of Policy in respect of how those powers were applied where they related to the payment of compensation to employees whose employment was terminated as a result of redundancy or certain other reasons.

Members were advised that the Policy had previously been reviewed in January 2020, where a number of changes had been made. It was not proposed to make any further changes at this time.

RESOLVED that no amendments be made to the current Pensions Discretions Policy.

29/EC Policy and Procedure for Fixed Term, Casual and Temporary Workers

The Committee was informed that a new amalgamated Policy Procedure for Fixed Term, Casual and Temporary Workers had been produced. The policy had also been reviewed and updated to ensure it was in line with the latest UK employment legislation.

RESOLVED that the new Policy Procedure for Fixed Term, Casuals and Temporary Workers, as set out at Annex A to the agenda report, be agreed.

30/EC Agile Working Policy 2021/22

The Committee considered a new Agile Working Policy, which updated and replaced the previous Off-Site Working Policy. The new Policy reflected the changes to working practices which had come about due to COVID-19 and ensured there was clarity around new ways of working.

RESOLVED that the Council's Agile Working Policy, as set out at Annex A to the agenda report be agreed.

31/EC Pay Settlement 2021/22

The Committee was informed that pay negotiation discussions had been ongoing since November 2020 and a number of meetings had taken place with Members and Staff Representatives. It was noted that no percentage cost of living award for 2021/22 had been offered by the Council but negotiations were ongoing in relation to alternatives in the form of additional holiday and one-off payments to staff earning under a specified salary.

At the Joint Staff Consultative Group meeting that morning, a majority of members of the Group present at the meeting had agreed the following recommendation:

(i) that no percentage cost of living award be agreed for 2021/22;

(ii) that a non-contractual additional day's leave be awarded to all staff in 2021/22, to be taken on Christmas Eve, or where the member of staff is required to work on Christmas Eve, added to their annual leave entitlement for 2021/22;

(iii) a non-consolidated payment of £250 be made to staff earning less than £28,000 FTE; and

(iv) to note that Staff Representatives, whilst recognising the current position, wish to see a pay increase for 2022/23.

It was advised that this recommendation had not received a majority of support from both the Member and the Staff sides, as required by the Joint Staff Consultative Group's Constitution. However, the recommendation from the Group had been supported by Staff Representatives and it was recognised that Members were able to propose other options at this meeting.

The Committee considered the recommendation from the Joint Staff Consultative Group and supported the proposal concerning the additional day's leave for 2021/22. It was reported that staff unable to take Christmas Eve as leave due to work requirements would have the day added to their leave entitlement. It was also recognised that, if necessary, management discretion could be used in order to respect different cultural and religious practices.

Members discussed the recommendation for a one-off payment of £250 for staff earning less than £28,000 FTE. It was reported that there were 95 staff members earning £28,000 or less, which would result in expenditure of £23,750. It was also noted that an award of £250 was equivalent to a 1% increase for staff earning £25,000 and a 0.8% increase for a member of staff earning £28,000. During the discussion, Members raised a number of matters for consideration, including the national pay offer, the current economic situation, increases to the cost of living, and the cost in relation to the Council's overall budget. Following this discussion it was agreed by a majority not to recommend to Full Council that a one-off payment of £250 be made to staff earning under £28,000.

RECOMMENDED to Full Council

(i) that no percentage cost of living award be agreed for 2021/22;

(ii) that a non-contractual additional day's leave be awarded to all staff in 2021/22, to be taken on Christmas Eve, or where the member of staff is required to work on Christmas Eve, added to their annual leave entitlement for 2021/22; and

(iii) To note that Staff Representatives, whilst recognising the current position, wish to see a pay increase for 2022/23.

32/EC Work Programme

The Committee considered its Work Programme for the remainder of the municipal year.

RESOLVED that the Work Programme for 2020/21, as set out at Annex A to the agenda report, be agreed.

33/EC HR Matter

The Committee was advised that the item would be deferred for consideration at its next meeting.

Chairman

Information Security Policy

Summary

This report provides the Employment Committee with information regarding the Council's Information Security Policy

Recommendation

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

1. Resource Implications

1.1 There are no additional revenue or capital cost implications arising from the report.

2. Key Issues

2.1 This 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.

2.2 This policy sets the framework for protecting and securing our information assets in SHBC. 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 us of our systems
- Comply with GDPR legislation

2.3 The Information Security Policy was last reviewed in March 2020. A further review has been carried out and the proposed changes are set out at Annex A.

3. Options

3.1 The Committee has the option agree the revised Information Security Policy with or without any further amendments it considers appropriate.

4. Equalities Impact

4.1 Completed.

5. Consultation

5.1 The revised Policy was considered by the Joint Staff Consultative Group at its meeting on 11 March 2021.

Annexes	**Annex A – Information Security Policy**
Background papers	**None**
Author/contact details	**James Rutter – ICT Manager** **James.rutter@surreyheath.gov.uk**
Executive Head	**Louise Livingston, Executive Head of Transformation**

SURREY HEATH BOROUGH COUNCIL

INFORMATION SECURITY POLICY v2021

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 ~~2018~~
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

This policy should be read in conjunction with:

- Data Protection Policy
- Data Security Breaches Policy
-

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 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.

Network passwords are set to force a change every 90 days.

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 3 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 ~~Desktop~~Workstations

All desktops and ~~direct access~~ 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 ~~direct access~~ 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

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 ~~Portable & hand-held~~Laptop & Mobile equipment

Users of ~~portable computer~~laptop & mobile equipment are responsible for the security of the hardware and the information it holds at all times ~~on or off council sites~~. 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.

~~Portable computers must have appropriate access protection, for example passwords and encryption software and must not be left unattended in public places.~~

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

~~Power on passwords should be used on portable ICT equipment to protect the device from unauthorised access.~~

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~~phones~~ 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 ~~such as MSN or Yahoo~~ 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

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.

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 ~~IG~~ 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 Council is moving towards storage of documents and files into the Box platform. By March 2019, it is anticipated that the majority of documents and files currently stored by the Council should be withon the main filer will be stored in the Surrey Heath Borough Council Box environment instead. Each user will be provided with a team environment and a personal environment within the Box platform.

During the transition phase to Box, all documents and electronic files should be stored on either shared network drives, the Council's Electronic Document Records Management System or within the Surrey Heath Borough Council Box environment.

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. and never stored on a local c:\drive or similar.

Documents may be stored on personal network drives or within the personal Box environment if it is confidential or personal and these types of documents should always be protected with a password on personal network drives.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 several times during the working day, 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. Box has a recover facility up to a period of 90 days should a file be corrupted or deleted by mistake.

Where possible work files and documents should be stored on structured workgroup shared box drives folders such as GEN drive where colleagues can access work in your absence.

Personal documents should be stored on the users ~~H:\ drive or~~ personal Box ~~area preferably in a folder called PERSONAL~~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~~, or~~ Surrey Heath hardware or Surrey Heath cloud services.

~~Files which have a large file size can impact on other network users by slowing down the network and affecting backup routines. Care should be taken when creating or transferring large files onto the corporate network, especially video files and photographs. It is preferable to keep these types of files to a minimum and discuss possible alternative storage options with the ICT Team. Creating duplicates in different locations on the network should be avoided where possible. Backup copies of large files should be removed as soon as possible and not kept indefinitely. The Records Management Policy provides policy and guidance when creating, storing, retaining and sharing records.~~

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 ~~during absence~~

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~~archive 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~~public folder~~ 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

Data Protection Policy

Summary

This report provides the Employment Committee with information regarding the Council's Data Protection Policy.

Recommendation

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

1. Resource Implications

1.1 There are no additional revenue or capital cost implications arising from the report.

2. Key Issues

2.1 The Data Protection Policy sets out the framework for compliance with the requirements of the Data Protection legislation and provide guidance to all council staff to help them understand the importance of their role in maintaining the security and confidentiality of personal data

2.2 The Data Protection Policy been reviewed and the proposed changes are set out at Annex A.

3. Options

3.1 The Committee has the option agree the revised Data Protection Policy with or without any further amendments it considers appropriate.

4. Proposals

4.1 It is proposed that the revised Data Protection Policy is adopted.

5. Equalities Impact

5.1 Completed.

6. Consultation

6.1 The revised Policy was considered by the Joint Staff Consultative Group at its meeting on 11 March 2021.

Annexes	**Annex A – Data Protection Policy**
Background papers	**None**

Author/contact details	**Sally Turnbull – Information Governance Manager** **Sally.Turnbull@surreyheath.gov.uk**
Executive Head	**Gavin Ramtohal, Head of Legal Services**

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
22 February 2021		Sally Turnbull	Reviewed and updated
To be further updated with approval			

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
To be updated		

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	Box:\ICT Policies and Documentation\Data Protection Policy\Data Protection Policy 2018	Geraldine Sharman
To be updated			

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 the printer.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).

~~**1.4.**~~**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 ~~any~~ 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 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 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 ~~i~~Impact A~~a~~ssessments 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 Executive Head of Corporate ~~Finance~~ 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 Database and agree and sign off their Service's retention and disposal schedule.

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 ~~may be~~is required ~~for~~ where ~~certain types of~~any processing of personal information will be undertaken on a regular basis ~~processing~~ 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 ~~who require training~~ complete Data Protection e-learning training as part of their induction.~~the first available Information Governance training course after their start date. Information Governance training is held quarterly~~

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 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 Management 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 ~~all people's~~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 ~~Data Protection Officer or~~ 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 inductionattend one of the regular Information Governance courses for new staff run by the Information Governance Manager. 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
- WhistleblowingSpeak 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 ~~2020~~ and reflect if necessary, any changes in guidance

~~**Geraldine Sharman**~~
~~**Information Governance Manager**~~
~~**November 2018**~~

Records Management Policy

Summary

This report provides the Employment Committee with information regarding the Council's Records Management Policy.

Recommendation

The Committee is advised to RESOLVE that the Records Management Policy, as set out at Annex A to this report, be agreed.

1. Resource Implications

1.1 There are no additional revenue or capital cost implications arising from the report.

2. Key Issues

2.1 The Records Management Policy sets out the standards for good records management to help ensure that the council have the right information at the right time to make the right decision and help ensure it meets its obligations under Data Protection legislation.

2.2 Records Management is briefly covered in the Information Security and Information Governance Strategy, however by adopting a specific Records Management Policy that sits alongside these policies we aim to ensure a more robust management of records by giving council staff more specific instructions on day to day management of records, ensuring records in whatever form they take are; accurate, reliable, ordered, complete, useful, up to date, are not kept for longer than necessary and are secure.

3. Options

3.1 The Committee has the option agree the new Records Management Policy, with or without any further amendments it considers appropriate.

4. Proposals

4.1 It is proposed that Records Management Policy is adopted.

5. Equalities Impact

5.1 Completed.

6. Consultation

6.1 The Records Management Policy was considered by the Joint Staff Consultative Group at its meeting on 11 March 2021.

Annexes	**Annex A – Records Management Policy**
Background papers	**None**
Author/contact details	**Sally Turnbull – Information Governance Manager** **Sally.Turnbull@surreyheath.gov.uk**
Executive Head	**Gavin Ramtohal, Head of Legal Services**

RECORDS MANAGEMENT POLICY

Document history

Date	Version	Author	Changes made
Feb 21	1.0	Sally Turnbull	Initial version

Approvals

Name	Signature	Role/Title	Date
Stuart Field		ICT Manager	Jan 21
James Rutter		ICT Manager	Jan 21
Gavin Ramtohal		Head of Legal Services and DPO	Jan 21
Sally Turnbull		Information Governance Manager	Jan 21
JSCG			

Document Filename and Location:

Filename: Surrey Heath Records Management Policy

Format	Version	Filepath	Owner
Draft	Draft 0.1		Sally Turnbull
Published			

Format	Version	Filepath	Owner

1. INTRODUCTION

1.1 Information, in all its forms, whether electronic, paper-based or staff knowledge, is Surrey Heath Borough Councils (SHBC) second most important resource after our people. Records Management is at the heart of the way in which we deliver service to the public. If we do not have consistent and accurate records we cannot optimise our efficiency or measure the improvements; in order to achieve this, our records should be:

(a) **Available** - Records will be available to those who need it, and who have the permissions to view or use it. We will avoid information overload and target information where it is needed.

(b) **Accessible -** Our records should be clearly identified and easily found when needed by anyone who needs to access it.

(c) **Electronic** - Our records and documents will be stored electronically. Over time, we will evolve our policies such that we will endeavour to only keep paper records where there is a legal requirement to do so.

(d) **Secure** - Records will be protected and retained as appropriate. We will record the confidentiality of information. Non confidential information will be openly published.

1.2 All records created and received by the Council, and its external service providers where they are processing information on the Council's behalf, are the property of the Council, and must not be used for any activity or purpose other than official Council business.

1.3 Failure to manage records properly within SHBC exposes the council to a significant financial, legal, confidentiality, public relations and potentially manpower-shortage risk.

2. PURPOSE

2.1 This policy sets out the Council-wide policy for records management standards that should be adhered to by all staff working with SHBC records including permanent and temporary employees including those who are agile working, working off-site and working jointly with partners, elected members, volunteers, contractors, secondments and work experience placements.

2.2 The Records Management Policy is about how Surrey Heath receives, creates, communicates, stores, uses and distributes the information we need to deliver our services and corporate objectives.

2.3 This policy applies to all the Council's information and data sets in all formats - paper, electronic (including graphical, audio, photographic and video files) and, so far as feasible, staff knowledge, including those that the Council creates, holds on behalf of others or shares with third parties or partner organisations. All information, records and data sets including emails need to be stored in a manner that allows effective retrieval and allows the relevant retention rules to be applied.

2.4 The Policy will add value to the information resources used by the authority and will promote efficiency. It will show customers and citizens that the Council has a commitment to providing high quality information and takes its role as the custodian of information seriously.

3. OBJECTIVES

3.1 The objectives of the Records Management Policy are:

(a) To instil an understanding of the importance, and an appreciation of the potential, of effective records management.

(b) To help develop awareness, understanding and to promote the application of good practice in handling information, and develop efficiency and effectiveness in this area.

(c) To support SHBC's ambition to improve processes, to improve customer services, to become more efficient and to reduce costs.

(d) To meet legislative and regulatory requirements and apply best practice.

4. RELEVANT LEGISLATION

4.1 Good records management must be managed in accordance with current legislation and existing professional standards. These include the following;

- Local Government Act 1972
- Local Government (Access to Information) Act 1985
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulation 2004
- Re-use of Public Sector Information Regulations 2015
- Public Records Act 1958 and 1967

- Human Rights Act 1998
- Lord Chancellors Code of Practise for Records Management
- In addition certain records will be subject to other legislation covering their subject area.

As well as key legislation there are useful guidance and procedures that should be consulted to ensure good records management these include;

- ICO guide to 'Records Management and Security'
- Cabinet Office 'Data Handling Procedures in Government'
- LGA 'Data and Transparency'

5. RELATIONSHIP WITH EXISTING POLICIES

5.1 This policy should be read in conjunction with the following related polices and guidance's;

- Information Security Policy
- Data Protection Policy
- Information Governance Strategy
- Email Guidance
- Corporate Style Guide
- Disciplinary Policy
- Offsite Working Policy

6. KEY DEFINITIONS

6.1 A "Record" is information held by the Council that relates to a specific topic, area of work or an individual. The record can be held in paper or electronic format

6.2 'Personal Data' is information that relates to an identified or identifiable person who could be identified, directly or indirectly based on the information.

6.3 "Records Management" is the planning, control, organisation and training activities relating to the creation, distribution, utilisation, storage, retrieval, maintenance, protection, preservation and final disposal of all types of records required for the conduct of the Council's activities

6.4 A "Records Retention Schedule" is a policy that defines how long records must be kept and provides disposal guidelines for how data items should be discarded. Records retention schedules are determined by the record type and the business, legal and compliance requirements associated with the data.

7. ROLES AND RESPONSIBILITIES

7.1 Corporate Management Team (CMT)

Are responsible for ensuring that the business areas they have responsibility for have processes and procedures in place that support this policy.

7.2 Data Protection Officer (DPO)

Is responsible for setting strategic direction and ensuring that policies and processes are in place for the safe management of information. The DPO is supported in this role by the Information Governance Manager.

7.3 **Information Asset Owner (IAO)**

Are responsible for ensuring appropriate information management practices including access controls and record retention and destruction are in place for their information assets (electronic and paper).

7.4 **Information Governance Manager**

Is responsible for working with the DPO to set strategic direction, ensuring that policies and processes are in place for the safe management of information.

7.5 **ICT**

Is responsible for providing and maintaining the secure infrastructure to enable information users to have access to information they require to deliver their services. In conjunction with Information Asset Owners and information users, the ICT Service will work towards the automation of the Council's archiving and records retention policy using cost effective and approved technology solutions.

7.6 **Line Managers**

Are responsible for ensuring their staff are aware of their information management responsibilities and arrangements for access to information, and that staff are appropriately trained or experienced.

7.7 **All staff**

All staff, elected members, contractors, consultants and agents ("information users") are responsible for managing records in accordance with this policy and related procedures. When leaving the Council, all staff must ensure that key Council records for which they are responsible remain accessible.

8. CREATION OF RECORDS

8.1 Records should be created and captured in a timely manner. This should either be done by someone who has direct knowledge of the event or transaction, or generated automatically as part of a routine operation.

8.2 Where appropriate, when creating records current corporate templates should be used for all documentation both physical and electronic.

8.3 Website content should be produced in compliance with The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018.

8.4 Records should have meaningful titles and where applicable include indexes/metadata so that they can be retrieved quickly and efficiently

8.5 To reduce duplication which can lead to incorrect records being updated or available, records should be centralised with version control and dated.

8.6 Records should be complete and accurate enough to allow staff (including any successors) to undertake all actions for which they are responsible.

8.7 The creator of the record is responsible for ensuring that it is accurate, of good quality, relevant, up-to-date, and if includes personal, sensitive or confidential information it is secure.

8.8 ICT should ensure appropriate backup arrangements are in place for electronic records (including restoration of backups and disaster recovery if electronic records are damaged).

9. STORAGE

9.1 To maximise efficiency, reduce costs, enable appropriate access and sharing and minimise risks, records must always be stored securely in corporate repositories, these include:

(a) **Filing cabinets**, physical storage accommodation for records should be clean and tidy, to prevent damage to the records, and securely protect against unauthorised access.

(b) **Microfiche or archiving system** (Alchemy) If applicable

(c) **The internet and intranet**. Both are extensive and contain a great deal of corporate information, including Committee reports and agendas (via the ModernGov platform), and a range of services and e-forms.

(d) **Microsoft Office and outlook**. All staff use the corporate systems, and calendars are generally open. Use of e-mail helps to share information but email should not be use as a storage of records instead records should be moved to the relevant service system or Box folder.

(e) **Box**. Each staff member has their own personal box folder, information of a confidential or sensitive nature should be stored within your own box folder and should be password protected. Only SHBC related data must be stored on Box. All services areas have their own box folder. Some of these are made available for corporate use either generally or on request while others are held and used locally within the service. The centralised filing structures in Box enable services to share documents and improve the security of our records. Box governance standards including access management, retention periods and classifications should be set when setting up box folders especially when the information being stored is of a personal or confidential nature.

(f) **Specialist Software Systems**. Specialist systems are used in some areas – these include; Northgate in Revenues and Benefits, Uniform in Planning, Licensing, Enforcement, Tree Protection, Listed Building and Land Charges, Civica in Finance, Xpress in Electoral Registrations and iKen in Legal. Access to these systems should be on a need to know basis and records should be managed in line with this policy.

(g) **Customer Relationship Management (CRM).** The Plan Alpha CRM system holds documents and records of all customer contacts through Customer Services, together with additional information from some contacts through other services. Access to Plan Alpha should be on a need to know basis and records should be managed in line with this policy.

(h) **Geographical Information System (GIS)**. We have established a corporate platform for mapping information, with integration into a number of key databases, and browser-based delivery through the Xmap mapping services. Our Local Land and Property Gazetteer is the definitive source for addressing in the council and publishes nightly address change updates to the National Land and Property Gazetteer. Access to the GIS system is managed by ICT.

(i) **USB drives / memory sticks and other removable media**. In the majority of circumstances ICT will no longer supply removable media such as USB sticks to staff as they are no longer required. Additionally ICT monitoring systems will prevent their usage on SHBC supplied equipment. Removeable medias must not be used for permanent storage of records. If you are required to transfer records, on most occasions, you are advised to use the sharing tools within Box

which are secure and timely. Only removable media supplied by ICT Services should be used with SHBC systems, all removeable media supplied by ICT are encrypted to the correct standard.

9.2 Avoid storing duplicates (e.g. avoid paper/electronic overlaps, e.g. store a single copy of electronic information to be shared through use of box links) and routinely destroy unnecessary information (in accordance with the corporate retention schedule);

9.3 If the record being stored includes personal or sensitive data additional security measures must be taken to ensure that only staff that need to know have access to the data, this will include, setting access controls to specific staff, ensuring password are set to access the records and for physical records ensure they are securely locked away. Additionally, Box sharelinks can be set to expire a certain number of days after they have been created.

10. RECORDS RETENTION AND DISPOSAL

10.1 The retention and disposal schedule ~~that are~~is maintained by the IAO in each service area and centrally managed within the Information Governance Department, helps the Council to meet its statutory obligations to ensure that information is retained for the correct period of time and then disposed of appropriately. It is unlawful to retain information for longer than necessary.

10.2 Electronic information should be treated in the same way as physical information; therefore, electronic information, where the system allows, must be disposed of once it has reached its set disposal date.

10.3 Each department/section should have a records retention schedule/policy in place which will outline the appropriate retention periods for records. These retention periods should be based on legislative requirements and common practice in the sector. The retention periods listed in the schedule are the minimum length of time which the data, information and records must be kept. retention schedules should be regularly reviewed (at a minimum every three years).

10.4 Where systems have the functionality to set retention periods on records or groups of records, it is recommended that an intended disposal or review date is captured when creating the electronic records.

10.5 IAO will review records in accordance with the retention schedule, when they are no longer required for on-going business or specific legal or regulatory purposes, records will be securely destroyed.

10.6 At the end of the retention period, the record should be assessed to see whether it ought to be selected for permanent preservation, e.g. if it is of historical interest. Such records should either be retained by the Council or be offered to the Surrey History Centre for archiving

10.7 Records that could be subject to a Freedom of Information or Data Protection request must not destroyed unless the approved retention period has been met.

11. CLASSIFICATION

11.1 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.

12. BUSINESS CONTINUITY

12.1 Information Asset Owners are responsible for identifying the data, information and records (regardless of the media in which they are stored) which are considered to be business critical and to ensure that the business critical elements are included in individual service unit business continuity plans.

12.2 It is the responsibility of ICT to ensure that backups are created to the agreed standards and to establish an effective back-up restoration regime to ensure that when back-ups need to be restored they remain fit for purpose.

13. DATA PROTECTION, PRINCIPLES OF RECORDS MANAGEMENT

13.1 Information which is subject to security controls i.e. personal, sensitive, confidential data, will be identified, and will be held and used in accordance with a Data Protection regime appropriate to the nature of the information.

13.2 Public information will, so far as reasonably possible, be made available without charge.

13.3 Information will be retained, archived and disposed of according to a records retention schedules.

13.4 The Council has an Information Asset Register (IAR) that identifies the information assets owned by the Council. The IAR is subject to an annual review and any risks identified will be reported to the Information Governance Manager.

13.5 Email and c:\ drives will not be used to store council information, staff should only store case work and other council information in the location agreed by their IAO this will usually be a specific system used by that department or Service Area or another corporately agreed location within the Council network.

13.6 The IAO will ensure that where new systems that store personal data or any sharing of personal data with third parties is to be undertaken a Data Protection Impact Assessment is completed before the sharing can take place.

13.7 Where records are being shared or systems accessed by third party data processors, contracts with the appropriate Data Protection and records management clauses regarding the agreed and approved methods of information handling are included.

14. MONITORING AND REVIEW

14.1 This policy will be reviewed when required or at the minimum at least every 5 years. The Information Governance Manager will regularly monitor compliance with the policy procedures and guidelines making any amendments and improvements as necessary.

This page is intentionally left blank

Social Networking Policy

Summary

This report provides the Employment Committee with information regarding the Council's Social Networking Policy

Recommendation

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

1. Resource Implications

1.1 There are no additional revenue or capital cost implications arising from the report.

2. Key Issues

2.1 The Social Networking Policy aims to provide guidelines for the effective and safe use of social networking to promote and develop the Council's 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.

2.2 The Social Networking Policy was last reviewed in 2018. A further review has been carried out and the proposed changes are set out at Annex A.

3. Options

3.1 The Committee has the option agree the revised Social Networking Policy with or without any further amendments it considers appropriate.

4. Equalities Impact

4.1 Completed.

5. Consultation

5.1 The revised Policy was considered by the Joint Staff Consultative Group at its meeting on 11 March 2021.

Annexes	**Annex A – Social Networking Policy**
Background papers	**None**

Author/contact details	**Sally Turnbull – Information Governance Manager** **Sally.turnbull@surreyheath.gov.uk**
Executive Head	**Gavin Ramtohal, Head of Legal Services**

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) ~~and~~ content sharing websites, web conferencing sites and collaboration tools ~~(~~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~~Dignity and Respect at Work Policy
- Communication guidelines
- ~~Whistleblowing~~Speak up Policy Policy

- Safeguarding Policy
- Mobile Phone Agreement
- ~~Surrey Heath Borough Council Policy for dealing with 'unreasonably persistent' and 'unreasonable' complaint behaviour~~
- 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 and MS Teams

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 ~~and 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 ~~the~~ Marketing and Communications~~Media and Marketing~~ Team ~~Contact Centre~~ 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 ~~Media and Marketing~~Marketing and Communications Team ~~corporate 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 and must not use background screens so it is clear nobody else is present

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~~1998~~. In particular, not sharing personal or confidential information inappropriately, checking location of information if using new social networks and ensuringe it is acceptable under the Data Protection legislation~~Act 1998~~.

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~~Speak up Policy 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 ~~c~~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

National Graduate Development Programme

Summary

This report provides the Employment Committee with information about the Local Government Association's (LGA) 'National Graduate Development Programme' (NGDP), and recommends that the Council seeks to join this scheme and create a new post of 'Graduate Trainee'.

Recommendation

The Employment Committee is advised to RECOMMEND to Council that the Council creates a new post of 'Graduate Trainee' and that it seeks to recruit to this role via the Local Government Association's National Graduate Development Programme, subject to the necessary budget increase.

1. Key Issues

1.1 The LGA's National Graduate Development Programme (NGDP) has run since 2002. Councils employ graduates for a two-year contract, where they undertake at least three different service placements. The LGA provide a complimentary training and development offer which includes working towards an ILM (Institute of Leadership and Management) Level 7 qualification.

1.2 The LGA carries out a central multi-stage recruitment exercise, (which last year attracted over 5,000 applicants) and refer successful applicants to Councils who carry a local interview process.

1.3 Officers have experience of the programme from previous authorities and consider that the scheme can bring considerable benefits and very high-calibre candidates seeking a career in local government.

1.4 SHBC has run a very successful summer student internship programme since 2017. In 2020, eight interns were employed July – September working in Economic Development, Planning Policy, Human Resources, Housing, Community Services, Revenues & Benefits and Transformation. Despite the need for remote working this programme brought great benefits to the Council and the interns and the LGA published a blog written by the Council about the programme in November 2020. This year's programme is currently being advertised and has attracted a large number of applications already.

1.5 It is clear from the Council's experiences with the intern programme that there would be a number of areas of work across the authority that could be greatly benefited by the Council having access to a flexible graduate trainee resource.

1.6 There is also the potential to link closer together our intern, apprenticeship (the Council normally has four or five apprentices in post across different services) and graduate programmes focusing on raising the profile of local government careers and 'growing our own' talent within the sector. To support last year's intern programme several staff undertook mentoring training, so these programmes can also offer development benefits for existing staff.

1.7 If the Council signed up to this year's NGDP programme local interviews would take place in June and a start date of Autumn 2021 for the trainee.

1.8 If the recruitment exercise did not result in a successful appointment then the proposal would be to use the agreed funding to extend the current internship programme to employ graduates.

2. Resource Implications

2.1 The creation of this post would require a budget increase.

2.2 The salary requirement for the NGDP Management Trainees is NJC (National Joint Council) spinal column point (scp) 20 (currently £25,921). This is virtually equivalent to the Council's local payscale SH4.16, which (including on-costs) equates to £33,956 per annum.

2.3 The national pay negotiations for 2021/22 are still underway and are unlikely to be concluded until after the deadline for signing up to the programme.

2.4 In addition a one-off fee covering recruitment, learning & development and the ILM qualification of £2,800 is payable.

2.5 At **current NJC SPC levels** the estimated costs in the coming years to employ one Management Trainee (including on-costs) would be:

- 2021/22 - £22,700 (assuming a start date of 1 September)
- 2022/23 - £34,000
- 2023/24 - £36,800 (assuming a further trainee was employed starting September 2023) or £14,200 if the post was not re-recruited to.

2.6 The Graduate Trainee's salary would need to reflect any national increases in pay to continue to reflect NJC SPC 20.

3. Options

3.1 Option 1 – take no action – focus instead on the Council's summer intern programme.

3.2 Option 2 (recommended) – Create a Management Trainee post and join the NGDP for 2021/22, noting the resource requirements above.

4. Proposals

4.1 The Employment Committee is advised to RECOMMEND to Council that the Council create a new post of 'Graduate Trainee' and that we seek to recruit to this role via the Local Government Association's National Graduate Development Programme, subject to the necessary budget increase.

5. Supporting Information

5.1 LGA's NGDP Council Information Pack 2021/22.

6. Corporate Objectives And Key Priorities

6.1 The new role would deliver a new flexible resource to support the Council in the achievement of the objectives in its Annual Plan. This links to objective TRA7 – a new Workforce Plan.

7. Equalities Impact

7.1 The LGA website states that *"The NGDP aims to provide a diverse pipeline of talented future leaders for local government and is committed to continuous improvement with respect to equality, diversity and* inclusion". A Equality, Diversity and Inclusion Review was carried out in2019 which resulted in a number of changes to their processes. There is currently an NGDP BAME network and an NGDP Women's network.

8. Consultation

8.1 The Chief Executive and Corporate Management Team were initially consulted on the proposal, and fully support it.

8.2 This report was also considered and supported by the Joint Staff Consultative Committee at its meeting on 11 March 2021.

Annexes	None
Background Papers	LGA's NGDP Council Information Pack 2021/22. LGA Workforce Blog November 2020
Author/Contact Details	Sarah Bainbridge, Senior Organisational Development Advisor, sarah.bainbridge@surreyheath.gov.uk
Head of Service	Louise Livingston - Executive Head of Transformation

This page is intentionally left blank

Proposal to Continue the Agreement with Elmbridge Borough Council to Share the Monitoring Officer Function

Summary

The Committee is asked to consider the proposal as set out in this report.

Recommendation

The Committee is advised to RESOLVE that the arrangements for sharing a Monitoring Officer with Elmbridge Borough Council continue for a further 6 months.

1. Background

1.1. At the October 2020 Employment Committee meeting, the Committee resolved to recommend to Full Council the appointment of Gavin Ramtohal as the shared Monitoring Officer for the Council and Elmbridge Borough Council. This was on the basis that the initial agreement would be for a trial period of 6 months to provide both Councils with the opportunity to assess whether the arrangement is working and whether they wish to continue. The Committee also recommended to Full Council that completion of the agreement is delegated to the Executive Head of Transformation.

1.2. Clause 9 of the Contract provides as follows

"*The term of this Agreement shall be six months initially from and including the Commencement Date whereupon it may be terminated by either Authority without notice. If not terminated, the Agreement shall continue from month to month until ended by either Authority giving not less than one month's notice of termination to the other*."

1.3. At the October 2020 Full Council meeting, the Council accepted the recommendations.

1.4. The Monitoring Officer is satisfied that the agreement is working well and, as far as he is aware, Elmbridge Borough Council is satisfied with the arrangement. However, there is a short term impact due to market related difficulties recruiting legal staff into vacant posts. Two recruitment exercises have failed to appoint a property solicitor and that post remains vacant. The impact of this has been less delegation and hence this would need to be kept under review, particularly if these difficulties persist post onshoring of the JPUT. The flexibility regarding termination should accommodate these concerns moving forwards and legal services is working with HR regarding future recruitment and options.

1.5. Due to the issues highlighted in paragraph 1.4, the stated benefits of developing staff knowledge and experience by more delegation have not yet materialised.

2. The proposal

2.1. The Committee is advised to resolve to continue the contract as permitted by the existing contract on a rolling basis. This would mean that the contract would continue from May 2021 until either Council decides to end the contract by giving the other at least one month's notice. Continuation with the arrangement accords with the Council's direction to drive more efficiencies through partnership working. Any decision to continue with the shared Monitoring Officer is also subject to Elmbridge BC agreeing to continue with the arrangement.

2.2. The Committee is asked to note the concerns outlined in paragraph 1.4.

3. Options

3.1. The Committee can endorse the recommendation that the arrangements for sharing a Monitoring Officer with Elmbridge Borough Council continue for a further 6 months.

3.2. Alternatively, the Committee has the option to recommend to Full Council that the Contract is terminated with the effect that the arrangement would terminate.

4. Legal and Governance implications

4.1. Section 1.10 of the Committee's terms of reference confirms "*To consider any recommendations for senior management restructures and make recommendations to the Full Council*."

4.2. The arrangement would continue to take effect under section 113 of the Local Government Act 1972.

Annexes	None
Background Papers:	None
Author:	Louise Livingston– Executive Head of Transformation louise.livingston@surreyheath.gov.uk
Executive Head of Service:	Louise Livingston – Executive Head of Transformation

Urgent Action

Summary

To advise the Employment Committee of urgent action taken by officers pursuant to the Scheme of Delegation of Functions to Officers.

Wards Affected
Not applicable

Recommendation

The Executive is advised to NOTE the urgent action taken under the Scheme of Delegation of Functions to Officers.

1. Resource Implications

1.1 The resource implications are as set out at Annex A.

2. Key Issues

2.1 In accordance with the Scheme of Delegation of Functions to Officers, urgent action has been authorised. The decision relates to the creation of the role of Head of Planning and disestablishing the role of Executive Head of Regulatory. Further details on the decision are set out at Annex A to this report.

3. Options

3.1 There are no options for the Executive to consider as the action has been taken.

4. Supporting Information

4.1 The Scheme of Delegation of Functions to Officers, provides for the Chief Executive, Executive Heads of Service and Heads of Services to determine, after appropriate consultation, matters of an urgent nature which are not in contravention of established policies of the Council, budgets set, or are key decisions, which will not admit of delay until the next ordinary meeting of the Council, Executive or Committee concerned. All such decisions which are executive matters have to be reported to the next meeting of the Executive.

Annexes	**Annex A - Urgent Action Decision Form**
Background papers	**None**
Author and contact details	**Rachel Whillis – Democratic Services Manager** **rachel.whillis@surreyheath.gov.uk**

Head of service	**Richard Payne – Executive Head of Corporate**

Surrey Heath Borough Council
Scheme of Delegation of Functions to Officers

Urgent Action Form – Regulatory Function

Consultation by Chief Executive or Executive Head of Service or Head of Service involved with relevant Chairman (or Vice Chairman) of the relevant Committee

To Councillor	Colin Dougan
Chairman of	The Employment Committee
To Councillor	Cliff Betton
Vice Chairman of	The Employment Committee
Proposal	To convert the post Executive Head of Regulatory to Head of Planning services. The reason for this is to focus all planning related functions into one service.
Background	The Executive Head of Regulatory manages a number of areas including; Housing, Family Support, Private Sector Housing, Disability Facility Grants, Planning (development management), Planning Policy, Building Control, Land Charges, Technical Support and Drainage. The role was introduced in 2012 when a flatter structure was put in place which consisted of 6 Executive Heads and 2 Heads of Service. Planning is one of the key core services delivered by the Borough Council that has key objectives and targets it has to achieve with a high impact on the Boroughs residents. This service area attracts a lot of legislative changes and has the responsibility of delivering a Local Plan. The role gives advice on enforcement to demonstrate to the public that the Council will take appropriate action when planning is contravened. It can also attract a lot of enquires/ complaints and requires a lot of attention at a senior level. This new role will be part of the new Management Structure, therefore this urgent action will then be shared with Full Council so that if this is agreed all Councillors will be aware. The Head of Planning would manage: Planning (development management), Planning Policy, Building Control, Land Charges, Technical Support and Drainage. The remaining services currently managed by the Executive Head of Regulatory will be managed by Executive Head Community on a temporary basis pending the full management restructure. These include: Housing, Private Sector Housing and Disabled Facility Grants and Family Support.
Options	1. To agree the dis-establishing of the Executive Head

	Regulatory and establishing of the Head of Planning 2. To remain with the current post of Executive Head Regulatory
Risk of delaying the decision	The role Head of Planning is vital to the Borough Council and with the current incumbent retiring its vital that the post is advertised and recruited to as soon as possible, so that the Council has the right level of skill and expertise and so not too to put too much pressure on the existing team Planning resource is limited with public sector competing with the private sector so recruitment may take some time.
Legal advice	Decision making protocol sort from Gavin Ramtohal Head of Legal and Richard Payne Executive Head Corporate.
Resource implications	The cost of the current post Executive Head Regulatory would be reduced to that of a Head of Service so there would be reduced costs.
Contact Officer for further information	Louise Livingston – Executive Head Transformation
Decision Making Officer – Chief Executive/ Relevant Executive Head	Damian Roberts – Chief Executive (Head of Paid Service)

Signe [redacted] Dated 11 March 2021

I agree with the above action proposed

Signed Dated

Chairman of Employment Committee

Signed By email 1/3/21

Dated

Vice Chairman of Employment Committee

Signed By email 2/3/21

Rachel Whillis

From: [redacted]
Sent: 01 March 2021 15:05
To: Louise Livingston; Cllr Colin Dougan
Cc: Damian Roberts; Gavin Ramtohal; Richard Payne; Rachel Whillis
Subject: RE: Urgent Action Employment Committee Feb 2021

Louise

Happy to sign this off.

Rgds
Colin

From: Louise Livingston [mailto:Louise.Livingston@surreyheath.gov.uk]
Sent: 01 March 2021 14:45
To: Cllr Colin Dougan <colin.dougan@surreyheath.gov.uk>
Cc: [redacted] Damian Roberts <Damian.Roberts@surreyheath.gov.uk>; Gavin Ramtohal <Gavin.Ramtohal@surreyheath.gov.uk>; Richard Payne <Richard.Payne@surreyheath.gov.uk>; Rachel Whillis <rachel.whillis@surreyheath.gov.uk>
Subject: Urgent Action Employment Committee Feb 2021

Private & Confidential

Dear Colin

Please find attached the urgent action I am asking you to sign off as the chair of the employment committee which proposes changing the Executive Head Regulatory post to a Head of Planning post.

As this will be a permanent change to the management structure if you are in agreement we will then ask the vice chair for sign off and then share with the Employment Committee for any comment. The employment committee urgent action will then go on to Full Council for urgent action sign off.

Also please note we have yet to talk to the teams affected by this change this won't happen until we have all the appropriate sign offs.

If you have any questions please don't hesitate to contact me.

Kind regards

Louise

Louise Livingston
Executive Head Transformation

Surrey Heath Borough Council
01276 707403
Louise.livingston@surreyheath.gov.uk
www.surreyheath.gov.uk

Rachel Whillis

From: Cllr Cliff Betton
Sent: 02 March 2021 10:40
To: Louise Livingston
Cc: Damian Roberts; Gavin Ramtohal; Richard Payne; Rachel Whillis; Cllr Colin Dougan; [redacted]
Subject: Re: Urgent Action Employment Committee Feb 2021

Dear Louise,

I am happy to sign off on this as it looks to me exactly what we were proposing in our budget at the full council meeting.

[redacted]

BSc, FRSB, CBiol, FIEMA, CEnv, FRSC.
Chairman, Audit and Standards Committee,
Surrey Heath Borough Council.
Liberal Democrat Councillor,
Frimley Green Ward
[redacted]

From: Louise Livingston <Louise.Livingston@surreyheath.gov.uk>
Date: Monday, 1 March 2021 at 16:16
To: Cllr Cliff Betton <Cliff.Betton@surreyheath.gov.uk>
Cc: Damian Roberts <Damian.Roberts@surreyheath.gov.uk>, Gavin Ramtohal <Gavin.Ramtohal@surreyheath.gov.uk>, Richard Payne <Richard.Payne@surreyheath.gov.uk>, Rachel Whillis <rachel.whillis@surreyheath.gov.uk>, Cllr Colin Dougan <colin.dougan@surreyheath.gov.uk>, [redacted]
Subject: RE: Urgent Action Employment Committee Feb 2021

Dear Cliff

I am writing to you in your capacity as vice chair of the employment committee to seek your sign off for the attached urgent action.

The urgent action is pertaining to the change of the role Executive Head of Regulatory to a Head of Planning the document hopefully explains why we want to make these changes and the reason for doing it by urgent action rather than waiting for the Committee meeting and Council meeting.

As this will be a permanent change to the management structure we are seeking the sign off of both the chair & vice chair the paper will then be sent to the Employment Committee and they will be given a short period of time to raise any concerns. The employment committee urgent action will then go on to Full Council for urgent action sign off this is signed off by the Mayor and Leader and shared with all Councillors.

Also please note we have yet to talk to the teams affected by this change this won't happen until we have all the appropriate sign offs.

If you have any questions please don't hesitate to contact me.

Kind regards

Louise

Louise Livingston
Executive Head Transformation

Surrey Heath Borough Council
01276 707403
Louise.livingston@surreyheath.gov.uk
www.surreyheath.gov.uk

From: [redacted]
Sent: 01 March 2021 15:05
To: Louise Livingston <Louise.Livingston@surreyheath.gov.uk>; Cllr Colin Dougan <colin.dougan@surreyheath.gov.uk>
Cc: Damian Roberts <Damian.Roberts@surreyheath.gov.uk>; Gavin Ramtohal <Gavin.Ramtohal@surreyheath.gov.uk>; Richard Payne <Richard.Payne@surreyheath.gov.uk>; Rachel Whillis <rachel.whillis@surreyheath.gov.uk>
Subject: RE: Urgent Action Employment Committee Feb 2021

Louise

Happy to sign this off.

Rgds
Colin

From: Louise Livingston [mailto:Louise.Livingston@surreyheath.gov.uk]
Sent: 01 March 2021 14:45
To: Cllr Colin Dougan <colin.dougan@surreyheath.gov.uk>
Cc: [redacted] Damian Roberts <Damian.Roberts@surreyheath.gov.uk>; Gavin Ramtohal <Gavin.Ramtohal@surreyheath.gov.uk>; Richard Payne <Richard.Payne@surreyheath.gov.uk>; Rachel Whillis <rachel.whillis@surreyheath.gov.uk>
Subject: Urgent Action Employment Committee Feb 2021

Private & Confidential

Dear Colin

Please find attached the urgent action I am asking you to sign off as the chair of the employment committee which proposes changing the Executive Head Regulatory post to a Head of Planning post.

As this will be a permanent change to the management structure if you are in agreement we will then ask the vice chair for sign off and then share with the Employment Committee for any comment. The employment committee urgent action will then go on to Full Council for urgent action sign off.

Also please note we have yet to talk to the teams affected by this change this won't happen until we have all the appropriate sign offs.

If you have any questions please don't hesitate to contact me.

Kind regards

Louise

Louise Livingston
Executive Head Transformation

Surrey Heath Borough Council
01276 707403
Louise.livingston@surreyheath.gov.uk
www.surreyheath.gov.uk

SURREY HEATH DISCLAIMER

Minutes of a Meeting of the Appointments Sub Committee held on 30 September 2020

+	Cllr Cliff Betton	+	Cllr Alan McClafferty
+	Cllr Sharon Galliford	+	Cllr Victoria Wheeler
+	Cllr Josephine Hawkins		

+ Present

5/A Appointment of Chairman

It was proposed, seconded and

RESOLVED that Councillor Alan McClafferty be appointed as Chairman for the meeting.

6/A Exclusion of Press and Public

In accordance with Section 100A(4) of the Local Government Act 1972, the public, including the press representatives, was excluded from the meeting for the consideration of the following items of business on the ground that they involved the likely disclosure of exempt information as defined in the paragraph of Part 1 of Schedule 12A of the Act, as set out below:

Minute	Paragraph
7/A	1
8/A	1

7/A Appointment of Chief Executive

The Sub Committee agreed a long list of candidates to be invited to interview for the post of Chief Executive.

8/A Review of Exempt Items

The Sub Committee reviewed the item which had been considered at the meeting following the exclusion of members of the press and public, as it involved the likely disclosure of exempt information.

RESOLVED that the items considered remain exempt for the present time.

Chairman

Minutes of a Meeting of the Appointments Sub Committee held on 12 October 2020

+	Cllr Cliff Betton	+	Cllr Alan McClafferty
+	Cllr Josephine Hawkins	+	Cllr Victoria Wheeler
+	Cllr Sharon Galliford		

+ Present

9/A Appointment of Chairman

It was proposed, seconded and

RESOLVED that Councillor Alan McClafferty be appointed as Chairman for the meeting.

10/A Exclusion of Press and Public

In accordance with Section 100A(4) of the Local Government Act 1972, the public, including the press representatives, was excluded from the meeting for the consideration of the following items of business on the ground that they involved the likely disclosure of exempt information as defined in the paragraph of Part 1 of Schedule 12A of the Act, as set out below:

Minute	Paragraph
11/A	1
12/A	1

11/A Appointment of Chief Executive

The Sub Committee agreed a shortlist of candidates to interview for the post of Chief Executive.

12/A Review of Exempt Items

The Sub Committee reviewed the item which had been considered at the meeting following the exclusion of members of the press and public, as it involved the likely disclosure of exempt information.

RESOLVED that the items considered remain exempt for the present time.

Chairman

This page is intentionally left blank

Minutes of a Meeting of the Appointments Sub Committee held on 19 October 2020

+	Cllr Colin Dougan	+	Cllr Sashi Mylvaganam
+	Cllr Sharon Galliford	+	Cllr Victoria Wheeler
+	Cllr Alan McClafferty		

+ Present

13/A Appointment of Chairman

It was proposed, seconded and

RESOLVED that Councillor Alan McClafferty be appointed as Chairman for the meeting.

14/A Exclusion of Press and Public

In accordance with Section 100A(4) of the Local Government Act 1972, the public, including the press representatives, was excluded from the meeting for the consideration of the following items of business on the ground that they involved the likely disclosure of exempt information as defined in the paragraph of Part 1 of Schedule 12A of the Act, as set out below:

Minute	Paragraph
15/A	1
16/A	1

15/A Appointment of Chief Executive

The Sub Committee interviewed candidates for the post of Chief Executive.

RECOMMENDED to Full Council that the post of Chief Executive and Head of Paid Service be offered to Mr Damian Roberts, subject to the requirements of Part 4 of the Constitution in respect to the offer of employment as a chief officer of the Council being satisfied.

16/A Review of Exempt Items

The Sub Committee reviewed the item which had been considered at the meeting following the exclusion of members of the press and public, as it involved the likely disclosure of exempt information.

RESOLVED that the decision remain exempt at the present time pending the decision of the Full Council

Chairman

This page is intentionally left blank

Minutes of a Meeting of the Appointments Sub Committee held on 17 February 2021

+	Cllr Colin Dougan	+	Cllr Graham Tapper
+	Cllr Sharon Galliford	+	Cllr Victoria Wheeler
+	Cllr Alan McClafferty		

+ Present

17/A Appointment of Chairman

It was proposed, seconded and

RESOLVED that Councillor Alan McClafferty be appointed as Chairman for the meeting.

18/A Exclusion of Press and Public

In accordance with Section 100A(4) of the Local Government Act 1972, the public, including the press representatives, was excluded from the meeting for the consideration of the following items of business on the ground that they involved the likely disclosure of exempt information as defined in the paragraph of Part 1 of Schedule 12A of the Act, as set out below:

Minute	Paragraph
19/A	1
20/A	1

19/A Appointment of Head of Investment and Development

The Sub Committee interviewed candidates for the post of Head of Investment & Development.

RESOLVED that the post of Head of Investment & Development be offered to Mr Stephen Wilkinson subject to the requirements of Part 4 of the Constitution in respect to the offer of employment as a chief officer of the Council being satisfied.

20/A Review of Exempt Items

The Sub Committee reviewed the item which had been considered at the meeting following the exclusion of members of the press and public, as it involved the likely disclosure of exempt information.

RESOLVED that the decision be made public following

(i) confirmation that the requirements of Part 4 of the Constitution in respect to the offer of employment as a chief officer of the Council are satisfied; and

(i) the acceptance of the appointment.

Chairman

Work Programme

Portfolio:	n/a
Ward(s) Affected:	n/a

Purpose

To agree the work programme for the 2021/22 municipal year.

Background

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

2. Meetings have been scheduled for the 2021/22 municipal year as follows:

- 8 July 2021
- 7 October 2021
- 27 January 2022
- 24 March 2021

Proposal

3. 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.

Recommendation

4. The Committee is advised to RESOLVE that the work programme for the 2021/22 municipal year be agreed, as set out at Annex A.

Background Papers: None

Author: Rachel Whillis – Democratic Services Manager
rachel.whillis@surreyheath.gov.uk

Head of HR/Service: Richard Payne – Executive Head of Corporate

Employment Committee
Work Programme
2021/22

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

- 8 July 2021
- 7 October 2021
- 27 January 2022
- 24 March 2021

The following work for the 2021/22 municipal year has been identified for consideration by the Employment Committee:

Meeting	Topic	Source
8 July 2021	**Probation Policy**	**HR (new)**
	House Rules	**HR (review)**
	Safeguarding Policy	**HR**
	Pay Policy Statement	**HR**
7 October 2021	**Leave and Special Leave**	**HR (review)**
	Sickness Absence Policy	**HR (review)**
	Flexible Working Policy & Procedure	**HR (review)**
	Health and Safety	**HR/Health and Safety Officer**
	Climate Change Policy	
27 January 2022	**Agile Working Policy**	**HR (review)**
	Recruitment Policy and Procedure	**HR (review)**
	Pay negotiations 2022/23	**HR**
	Pensions Discretion Policy – if any amendments are made	**HR**
	Family Friendly Policy	**HR**
24 March 2022	**Pay Settlement 2022/23**	**HR**
	Data Breaches Policy	**ICT/HR**
	Information Security Policy (Review)	**ICT**
	Data Protection Policy	**ICT**
	Social Networking Policy (Review)	**HR/ICT**

	Employment Stability Policies and Procedures	**HR (review)**

To be allocated:

Annual report on the use of the Speak Up Policy

This page is intentionally left blank