SURREY HEATH BOROUGH COUNCIL

INFORMATION SECURITY POLICY ~~v2021~~v2022

1. Message from the Chief Executive

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

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

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

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

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

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

Chief Executive

2. Introduction

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

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

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

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

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

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

3. Training and Awareness

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

4. Responsibilities

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

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

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

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

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

2.0 Password Policy

2.1 Purpose and scope

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

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

2.2 Network user accounts

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

2.3 Okta Single Sign on

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

2.4 Application passwords

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

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

2.5 User responsibility

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

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

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

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

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

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

2.6 Temporary passwords

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

2.7 Network password standards

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

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

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

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

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

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

The password must NOT contain your login name.

2.8 Past passwords

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

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

2.9 ICT Passwords and 1Password

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

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

2.10 Misuse of passwords

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

2.11 Passwords for documents

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

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

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

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

Information Security Policy

3.0 Starters, Change of access and Leavers Policy

3.1 Purpose and scope

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

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

3.2 New accounts and system access

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

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

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

3.3 Name changes

Name change requests should be logged with the ICT Service Desk

3.4 Job or role change

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

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

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

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

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

3.5 GSi Convergence Framework (GCF) Network access

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

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

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

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

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

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

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

3.6 Account closure

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

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

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

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

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

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

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

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

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

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

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

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

3.8 Work Experience students

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

Please refer to the Work Experience policy for further guidance

3.9 Suspension of accounts

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

3.10 Building Access

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

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

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

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

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

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

4.0 Patch Management Policy

4.1 Purpose

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

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

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

4.2 Windows Server Update Service (WSUS) Patch Management

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

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

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

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

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

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

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

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

4.3 Workstations

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

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

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

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

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

4.4 Application Software

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

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

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

4.5 Cloud Services

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

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

5.0 Virus and Malicious Software Management Policy

5.1 Purpose and scope

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

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

5.2 What is a virus or malicious software?

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

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

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

5.3 Personal and third party equipment

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

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

5.4 Anti-virus software

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

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

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

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

5.5 Email scanning

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

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

Information Security Policy

6.0 Physical and Environmental Security Policy

6.1 Purpose and scope

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

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

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

6.2 Physical Access Controls

General access to buildings should require appropriate levels of control.

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

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

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

6.3 Manual workstation lock

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

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

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

6.4 Automatic workstation lock

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

6.5 Laptop & Mobile equipment

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

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

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

Passwords should never be stored with the device.

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

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

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

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

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

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

6.6 Equipment installation

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

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

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

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

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

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

6.7 Equipment and media disposal

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

Electrical device disposal should be compliant with WEEE legislation.

6.8 Return of equipment

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

6.9 Network Availability

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

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

6.10 Remote access

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

Okta

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

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

Watchguard Access Portal

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

Azure Virtual Desktop

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

6.11 Third party access

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

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

Access Requests

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

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

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

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

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

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

Third Party Remote Use Agreement

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

Confidentiality

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

Unique Supplier Authentication

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

Host Security

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

6.12 Virtual Private Networks

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

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

7.0 Internet Usage Policy

7.1 Purpose and scope

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

7.2 Use

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

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

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

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

7.3 Misuse

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

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

- any illegal activity

7.4 Copyright

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

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

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

7.5 Provision of Access

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

7.6 Personal Use

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

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

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

Printing from the internet for personal use is not permitted.

8.0 Secure Data Transfer Policy

8.1 Purpose and scope

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

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

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

8.2 Physical security

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

8.3 Electronic security

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

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

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

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

8.4 Media

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

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

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

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

8.5 Email

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

Transportation

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

Government Secure Email

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

Protective marking

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

Processing of Credit/Debit card payments and PCI compliance

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

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

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

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

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

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

9.0 Data Storage Policy

9.1 Purpose and scope

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

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

9.2 Storing documents and files

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

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

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

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

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

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

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

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

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

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

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

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

10.0 ICT Procurement Policy

10.1 Purpose and scope

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

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

10.2 Procurement

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

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

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

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

10.3 Cloud software

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

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

11.0 Email Management Policy

11.1 Purpose and scope

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

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

11.2 Using emails

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

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

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

11.3 Speed of response

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

11.4 Email content expectations

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

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

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

The forwarding of chain mail or jokes is not permitted.

11.5 Misuse of email

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

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

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

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

11.6 Personal email

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

11.7 Access to staff emails

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

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

11.8 Sensitive Personal Data

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

11.9 Email retention

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

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

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

11.10 Email forwarding

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

11.11 Management of Public Folders/Shared Mailboxes

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

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

12.0 Secure Government Email Policy

12.1 Purpose

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

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

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

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

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

Information Security Policy

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.

Information Security Policy

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