Slough Borough Council

Report To:	Employment Committee
Date:	25th September 2023
Subject:	Updated Acceptable Use of Systems and Technology Policy
Lead Member:	Cllr Chandra Muvvala
Chief Officer:	Sarah Hayward, Executive Director of Strategy & Improvement
Contact Officer:	Simon Sharkey Woods, AD Chief Digital & Information Officer
Ward(s):	N/A
Key Decision:	NO
Exempt:	NO
Decision Subject to Call In:	YES
Appendices:	Appendix A – Acceptable Use of Systems and Technology Policy

1. Summary and Recommendations

Summary:

1.1 The use of technology systems and services at the Council comes with significant risk linked to information loss. To help mitigate this risk the Council needs to regularly review the Acceptable use of Systems and Technology policy and provide clear guidance for all users around the appropriate use of technology.

1.2 This report is seeking approval to adopt the latest version of the Acceptable Use of Systems and Technology Policy across the Council. Acceptance will trigger a range of actions that will communicate and embed the policy across the Council.

Recommendations:

Employment Committee is recommended to:

1.3 Approve the adoption of the latest version of the Acceptable Use of Systems and Technology Policy.

Commissioner Review

1.4 Commissioners have seen and noted the report.

2. Report

Introduction

2.1 An acceptable use of technology policy (AUP) in local government is a set of rules and regulations that govern the use of technology by employees, councillors, contractors, and other authorised users.

2.2 It is essential for the Council to mitigate risk by having a robust and up to date policy around the use of technology systems and services, that is understood by all the users of Council systems.

2.3 It is also essential for these policies to be updated regularly to take account of changing technology, and the differing levels of threat to the Council.

Background

2.4 The Council collects and stores a lot of sensitive information, such as personal data, financial information, and intellectual property. This information is valuable to attackers, who can use it to commit identity theft, fraud, or other crimes.

2.5 Poor cyber security practices can make it easier for attackers to gain access to this information. For example, if employees use weak passwords or click on malicious links in emails, they can give attackers access to sensitive information.

2.6 All councils need to take steps to protect themselves from cyber threats, regardless of their size or location. Having an up-to-date policy that is well understood by all users is one essential element to help minimise risk.

3. Implications of the Recommendation

3.1 Financial implications

3.1.1 There are no direct finance implications because of this policy.

3.1.2 Formal adoption of the policy and the subsequent embedding of it across the Council should however lower the risk of additional costs from information loss or fines.

3.2 Legal implications

3.2.1 Adopting and embedding the policy will contribute to lowering the risk of service failure across the council, lower the potential for cyber-attacks, and improve our stance in respect of the data protection act.

3.2.2 The failure to follow the policy could put the Council at risk and this could therefore lead to disciplinary action. Appropriate communication and learning will be provided before staff are expected to comply with the policy.

3.3 Risk Management Implications

3.3.1 The risk of major failures of critical services will be reduced because of adopting and embedding the refreshed policy.

3.4 Environmental Implications

3.4.1 There are no known environmental implications of this policy.

3.5 Equality Implications

3.5.1 There are no known equality implications because of this strategy.

4. Background Papers

None

Appendix A

ACCEPTABLE USE OF SYSTEMS & TECHNOLOGY POLICY

Contents

Document Control

Title	Acceptable Use of Systems and Technology Policy
Version	0.4
Date Issued	June 2023
Status	Draft
Document owner	Cyber Security Officer
Creator name	Muwa Agbo (Interim Cyber Security Officer)
Subject category	Technology/Security/Information Governance
Access constraints	For internal use only

Document Revision History

Version	Date	Author	Summary of changes
0.1	January 2023	Muwa Agbo	Version 0.1
0.2	June 2023	Simon Sharkey Woods	Updates following full review
0.3	June 2023	Simon Sharkey Woods	Updates following S&I feedback
0.4	September 2023	Simon Sharkey Woods	Updates following feedback ahead of Employment Committee

Document Distribution / Stakeholders

Name	Business/Department	Date Authorised	Version	Action
Muwa Agbo	Cyber Security Officer	N/A	0.2	P
Simon Sharkey Woods	Associate Director, Chief Digital & Information Officer	05/09/2023	0.4	P
Sarah Hayward	Executive Director, Strategy & Improvement	05/09/2023	0.3	A
DLT (Directorate Leadership Team)	Strategy & Improvement	14/06/2023	0.2	R
Union representatives	Unions	06/09/2023	0.4	R
Staff networks	Staff networks	05/09/2023	0.4	R
Employment Committee	Elected Members		0.4	A

P=Producer, C=Contributor, R=Reviewer, A=Authoriser, I=for information only

1.0 STATEMENT

This Acceptable Use of Systems and Technology policy sets out how Slough Borough Council's information systems and equipment may be accessed and used.

Council systems and devices are provided to staff for business purposes only to enable them to access the systems and data required to effectively undertake their work. Limited use of Council systems for personal reasons is permitted, if it is always in compliance with this policy, does not impact on the individual's work or that of others and is not excessive in terms of time or resources consumed.

Use of the council's systems must be authorised by line managers. Users should be aware that any data they create on the Council's systems (including anything pertaining to themselves) is deemed to be the property of the Council. Users are responsible for exercising good judgment regarding the reasonableness of personal use and for complying with this and other policies – see: the Local Code of Conduct for Employees.

It is the responsibility of all users to be aware of this policy, understand what it means and to comply with it. Failure to follow the requirements within this policy may result in disciplinary action.

Prohibited Use of Council Systems

- Any use of Council systems for unauthorised purposes may be regarded as improper use of facilities.
- Breach of this policy will be treated very seriously and could lead to disciplinary action, including summary dismissal.
- Where evidence of misuse is found, the Council will undertake a more detailed investigation in accordance with the Disciplinary Policy & Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation. See Disciplinary Policy & Procedure.

1.1 PURPOSE

This Policy defines the requirements on Council staff for acceptable use of Slough Borough Council's systems and devices to ensure all technology and information resources are protected.

1.2 SCOPE

This Policy applies to Councillors and to all of Slough Borough Council's personnel, irrespective of location or status, including temporary staff, volunteers, contractors/agency workers, consultants and third parties who have access to the Slough Borough Council's systems and devices. The Policy covers the use of resources accessed from the Council, including, but not limited to:

- Physical and paper records
- Internet
- E-mail
- Instant messaging tools
- Computers and laptops
- Servers and network infrastructure
- Electronic records, including those stored on USB data keys and other removable media.
- Software and Software-as-a-Service (SaaS)
- Telephony systems
- Smartphones, 'hand-held' and tablets.

1.3 ROLES AND RESPONSIBILITIES

Executive Directors and Associate Directors are responsible for ensuring awareness and compliance of this policy within their Directorate.

The Associate Director, Chief Digital & Information Officer is responsible for ensuring the maintenance, regular review and updating of this Policy. Revisions, amendments, or alterations to the Policy shall be issued and communicated as appropriate.

All users must: -

- Comply with the contents of this Policy.
- Seek advice if any aspect of this Policy is unclear or when uncertain of any of the requirements set out in it.
- Report any suspected information security breaches or non-compliance of this Policy immediately.

Line Managers

- Ensure staff understand and comply with this Policy.
- Ensure any incidents/suspected breaches are reported immediately.
- Monitor ongoing compliance within their team.

Compliance with Data Protection Legislation

Staff must ensure that any collection, storage, or processing of personally identifiable information must only be carried out in compliance with the requirements of the applicable Data Protection legislation (such as the General Data Protection Regulation (GDPR) Data Protection Act 2018.

Regularly refreshed Data Protection Awareness training is mandatory to ensure that all staff understand and apply the appropriate principles in their work.

Reporting Information Security Incidents/Breaches

All actual or suspected security incidents/breaches must be reported to your Line Manager and/or the ICT Service Desk. (Astro ServiceDesk Portal)

Information Security incidents/breaches include, but are not limited to:

- Loss/theft/leakage of sensitive data (on paper/waste/post or electronic data stored on removable media or portable devices such as laptop/USB stick/CD etc).
- Unauthorised access to information, systems, or premises.
- System misuse by a user or multiple users.
- IT Security breaches (e.g., malicious code infections – virus and worms; Denial of Service attacks; internal/external hacking; encryption failure).
- Where Personal Information is impacted, please refer to SBC Data Breach reporting standards.

Contact your line manager and/or the ICT Service Desk and Data Protection Officer (DPO) for further information and guidance.

1.4 POLICY

Computer Equipment

User Responsibilities

- All IT devices and software which have been assigned to a user remains the property of **Slough Borough Council**.
- **Slough Borough Council** IT equipment or software **must not** be modified in any way.
- Users must protect all IT equipment which is provided against loss, theft, and unauthorised access:
    - Always ensure that the equipment is physically secure, including when it is in transit and at fixed locations, e.g., offices or home.
    - Avoid leaving equipment unattended in public locations, e.g., when travelling or in a public place, such as a restaurant.
- Usernames and passwords must never be written down in a way which is not secure or be shared with anyone.
- Direct connection of non-SBC and/or personal equipment (e.g., your own or another organisation's smartphones, tablets, gaming or lifestyle devices, USB data keys or unauthorised file storage devices) to the council's wired and wireless networks is not permitted, except where specifically provided for by an IT service, such as a guest wireless network and where it has been expressly and specifically approved by ICT Service Desk.
- Storing council data on personal devices such as tablets, mobile phones or laptops is prohibited.
- Sensitive or confidential information of any nature (especially special category and personal data**) must** only be stored on Slough Borough Council's network, within permitted restricted areas (accessible to authorised members of staff) and must not be copied to or saved on unencrypted or non-Council data storage devices. This is in accordance with Slough Borough Council's compliance with GDPR Data Protection Act 2018 data management and prevents sensitive information from being completely lost or stolen.
- Immediately report any lost or stolen equipment to the ICT Service Desk by calling 01753 944199 and DPO (Data Protection Officer).

Secure Disposal and Re-use of Equipment

All devices issued to users must be returned to the ICT Service Desk for disposal and/or re-use when the user leaves the Council, or the device is no longer required. Any information and software on the device will be securely wiped before disposal or re-use of the equipment. Devices must under no circumstances be retained by departments when a person leaves, or just "passed on" to other users.

Wireless Networks/Non-SBC Networks

- Unauthorised access to private wireless unsecured networks is an offence under the Communications Act 2003 and therefore is prohibited.
- Where access to public networks (typically Wi-Fi hotspots) is permitted staff should satisfy themselves that the service is reputable and should be particularly wary of services which are unprotected by passwords.

Protection against Malware

Malware (i.e., computer viruses, spyware and other forms of malicious code which exploit any vulnerabilities in software programs) can cause loss and damage to information, software, and IT equipment.

Users must ensure that:

- Viruses or malicious code are not introduced into Slough Borough Council's network by downloading unauthorised or suspect software from the internet or from software, hardware and/or computer media (such as DVDs and USB storage devices) onto any Slough Borough Council device or system.
- The controls that Slough Borough Council has implemented on the IT devices it owns remains in place as they are there to minimise the threat of malicious software and must not be circumvented, changed, or removed in any way.
- If a user is suspicious about the presence of a virus or potential malware on the device/system, the user must stop using their device immediately and contact the ICT Service Desk and inform their Line Manager
- If users receive a suspicious e-mail, they must not open it or any attachments, as this may activate a virus or other form of malware. Immediately contact the ICT Service Desk **and** inform their Line Manager at the earliest possible opportunity.

If any software is required to be installed onto any Slough Borough Council device, a request must be placed via the Astro Service Desk. Non-standard software requests require approval from your line manager to verify the intended use is for council business. Non-standard requests will be reviewed by the Technical Design Authority, chaired by the Associate Director, Chief Digital & Information Officer.

Cyber Security

Council devices will often be connected to or have access to the internet. Such access, although often unavoidable, poses specific risks to corporate systems and data. Users of council systems and services will complete all mandated and relevant security training and will act diligently to apply best practice.

Use Outside of the UK

Using council-owned IT devices and accessing council services and information from locations outside of the UK poses specific risks and is therefore prohibited. In exceptional circumstances, with written permission from the relevant Executive Director (who would have discussed this with the Director of HR) a request to work remotely for business needs may be approved.

User Access Control

Each device connected to Slough Borough Council's network is a potential gateway to systems and information. Consequently, every user has a personal responsibility to ensure that they control access to their devices by diligently complying with the access control procedures.

Accessing someone else's device or account without permission is not permitted and may result in disciplinary action.

User Responsibilities

- Press Ctrl-Alt-Delete, or the Windows key and L, to lock the screen, when the device is left unattended. Always lock your device once you have finished using it. Do not walk away from your desk or workstation with the device open, accessible, and unlocked.
- Ensure that smartphones are always protected with a confidential PIN or passcode
- Your username and password must never be disclosed to anyone else, apart from when requested to do so during a support issue or update being managed by a member of the ICT&D team. Once the repair or update has been completed you must change your password.
- If your password's security has been compromised, you must change it immediately and notify the ICT Service Desk at the first available opportunity. Failure to do so could be a disciplinary matter.
- Do not disable, interrupt, or change the security configuration settings of any Slough Borough Council-owned equipment.

Passwords

What is the standard for a password?

The objective is to create a strong password that will withstand attempts to 'crack' it, at least for a reasonable length of time. For example, any word in the dictionary can be cracked within seconds by widely available password breaking programs, whereas a well-constructed password can take a day or more to crack and should deter all but the most determined hackers.

Strong passwords are created using the following rules:

1. Passwords must be nine characters or greater for all users.
2. Passwords must be twelve characters or greater for all system administrators.
3. Characters must be a mix from some or all the following groups:
   a. A minimum of One English Uppercase characters (A to Z)
   b. A minimum of One English lowercase characters (a…z)
   c. Based 10 digits (0…9)
   d. Non-alphanumeric characters selected from the following:
   ! " $ % ^ & * ( ) - _ = + [ ] { } ; : ' @ # ~ , < . > / ? \ |
   e. Do not use £, € or a SPACE
4. Passwords must not contain all or part of the user's name or job function, or any term (like a birthday, a partner's name, pet's name, or a street address) that could be easily guessed or researched.
5. Simple substitutions (such as 1 for I, 0 for O, 5 for s etc.) in recognisable words – i.e., words found in a dictionary – provide no real protection and must not be relied upon.
6. Similarly, commonly used, or easy to guess combinations or series such as 1234abcd, A5DFghJK, $taRwaR$, 1passw*d etc. must not be used.
7. The same password cannot be used for the next 10 times of change of password on the system.

Here's a couple of examples which show how the requirements on character use in passwords can be met/exceeded (do not copy them, invent your own):

- Coffee75train^fish
- Baseball4dinner!river

Please do NOT use any word in this list. Additionally, please do NOT include your personal details in your password, for example:

- Current partner's name
- Child's name
- Other family members' name
- Pet's name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team

Clear Desk and Screen

- When disposing of classified or sensitive information, they **must be** placed in an approved confidential waste container or shredded

- Documents must be immediately retrieved from printers, photocopiers, and fax machines. Do not print sensitive data or documents and leave the printouts to collect later. Any staff handling hard copies of classified or sensitive information must take appropriate steps to ensure their protection.
- Laptops, mobile telephones, swipe cards and other portable assets must be locked away in, for example, secure lockers and not left unattended for extended periods, such as on desks.

Communication Security

Caution must be taken when using telephones, voicemail, answering machines, facsimiles and recording equipment (e.g., photographic, video and audio equipment) to protect classified and sensitive information. It is crucial that before conducting a telephone conversation in an open plan office area or outside of Slough Borough Council premises, you must consider the nature of the topic you are about to discuss. If the conversation is of a classified or sensitive nature, ensure there is no risk of eavesdropping or accidental hearing of the conversation by moving to a separate room or a location where you are sure you cannot be heard by others. If you cannot do this for practical reasons, arrange for the call to take place another time, elsewhere, where security can be certain.

Similar caution should be taken whilst using laptops and other portable devices (especially in public areas) to ensure that your screen cannot be overlooked.

Users must take care when transmitting information, material or data via e-mail or other electronic means. When sending or receiving sensitive information, material, or data, ensure that the information is not compromised. If you are unsure, always check the recipient’s phone number/email address to ensure that it is correct before sending the information. Ensure that the information is collected immediately from the printer or facsimile and that all sensitive information in physical format is destroyed when no longer needed by shredding or using confidential waste containers.

Internet Use

Acceptable use of the Internet is deemed as accessing the Internet for legitimate business purposes.

The following are regarded as unacceptable use, regardless of whether it is for business or personal use:

- Excessively browsing websites which are not or cannot be justified as work-related.
- Any activity that may adversely impact or damage the reputation of Slough Borough Council
- Downloading data or material that infringes any copyright, trademark, patent, trade secret or other proprietary rights of a third-party. If you are unsure, always check first.
- Downloading any unlicensed or ‘hacked’ illegal software or content.
- Accessing any website that contains sexually explicit or offensive material, regardless of whether the website had previously been deemed acceptable. You must notify your line manager if you inadvertently visit an inappropriate / unacceptable site.
- Non-compliance with copyright law and all applicable licences, which may apply to software, files, graphics, documents, messages, and other material you wish to download or copy.
- Knowingly accessing or sending:
    - material or data likely to facilitate an illegal act.
    - Information about, or software designed for, breaching security controls or creating computer viruses.
    - Material that is obscene, sexually explicit, defamatory, incites or depicts violence, or describes techniques for criminal or terrorist acts.
    - Material that is illegal under local or international law.
- Compromising security controls of Slough Borough Council or any other organisation
- Knowingly circumventing any system that protects privacy or security
- Accessing any information, data or not intended for you

Digital Communication

This Policy applies when using Slough Borough Council's digital communication services such as email, Microsoft Teams, SharePoint, Viva Engage (Yammer), and online public forums (e.g., Chat Groups, newsgroups, social media on any network. All usage of Slough Borough Council's email service must be regarded as the property of the Council and must not be considered for private or personal non-business communications.

You must:

- Take care to ensure that intended email recipients are carefully selected before sending emails. Ensure the 'bcc' function is used when necessary to hide the addresses of recipients.
- Always check the content of an e mail chain you are forwarding in case you are inadvertently sharing personal data.
- If an email is received in error, the originator must be informed of the error as soon as practical.
- Avoid sending unnecessary messages, especially using 'Reply All' to large circulation lists or with large attachments.
- Be cautious of emails received from unknown and unexpected sources. Do not open suspicious emails and their attachments or web links, as these may contain malicious software. You must alert the ICT Service Desk for advice and assistance
- Seek legal advice before entering any email communication that could later be interpreted as contractual. Care shall be taken to ensure that the content of emails remains objective (not subjective) as far as possible, and that individual comments that could lead to dispute or legal action are not included.
- Report the receipt of messages containing racist, sexual, religiously offensive, sexist, homophobic or any other otherwise offensive remarks or media which contravenes the Code of Conduct/Zero Tolerance policy immediately to your line manager.
- Only use Slough Borough Council provided digital messaging and collaboration systems.
- Ensure confidential messages sent outside of the council's network are encrypted as required by data classification requirements.
- Do not send confidential work-related messages and information to personal email addresses, other personal messaging systems, or share on social media.
- Do not send debit or credit payment card details in clear text over digital communication technologies such as email, instant messaging, SMS, chat applications on Slough Borough Council IT, systems, or devices.
- Do not use any Slough Borough Council technology to run or engage in any form of personal or non-council business for hire or reward.

1.5 ONLINE STORAGE

Online storage services such as Google Drive, Dropbox, etc. must not be used to store SBC information. SBC information must always reside on services that have been contracted by the council or directly on the SBC network.

Use of social media

This policy must be adhered to in connection with the use of social media by Council staff for business reasons. In terms of personal social media sites, staff must also ensure that;

- Personal social media sites are not accessed from Slough Borough Council's equipment and devices.
- Personal social networking sites are not used to make derogatory or harmful comments, nor express opinions about Slough Borough Council, its employees, customers or third parties. You should not express extreme views or use abusive language on social media sites using credentials that identify you as a Slough Borough Council employee and thereby bring the council into disrepute.
- Details of service users must not be named, or any specific reference should be made to any Slough Borough Council work carried out in respect of them via any personal social networking site.

Monitoring

Slough Borough Council monitors the use of Internet, email, and network traffic to protect its interests and to maintain the effectiveness, integrity, and security of council information. As a result, users cannot consider the use of Slough Borough Council's technology equipment and services as private to them.

Excessive or inappropriate use of monitoring tools is not permitted and may result in disciplinary action.

Monitoring will be undertaken for the purpose of:

- Providing evidence of business communications to establish the existence of facts.
- Ascertaining compliance with regulatory practices or procedures relevant to the business
- Ascertaining or demonstrating the standards which are achieved or ought to be achieved by users of the systems in the course of their duties.
- Investigating or detecting the unauthorised use of a resource
- Preventing or detecting crime
- Ensuring the effective operation of the systems.

Any activity that contravenes Slough Borough Council's policies may be intercepted and held for further investigation.

1.6 PRINTING

Slough Borough Council maintains office based multi-function devices. This facility enables staff to print, scan, copy and fax.

General Guidance

- Printing is expensive and has a significant environmental impact, therefore wherever possible staff should avoid the need to print by storing, editing, and sharing documents in electronic format.
- If you do need to print, please do so as efficiently as possible by: -.
    - Printing in duplex (double-sided) as standard
    - Printing in B&W (Greyscale) not colour.
    - Use multi-image-per-page printing where possible.

Printing Securely

Prints and faxes may contain sensitive information and it is the responsibility of every Council employee to manage print in a responsible manner. Therefore, staff should always maintain secure print practises.

You must:

- Ensure prints are collected promptly from printers.
- Check that all pages have printed BEFORE leaving the printer
- Check that original documents placed in the scanner/copier area are retrieved.
- Delete your unwanted print jobs from the print device queue if no longer required. As part of MFD set up, any unprinted documents will be automatically purged after a set period.
- Ensure that ALL waster print material is disposed of according to its sensitivity.
- When disposing of classified or sensitive information, they **must be** placed in an approved confidential waste container or shredded.
- If a print device runs out of paper, or jams whilst releasing a print or copy job, the owner of that print or copy job must ensure paper is reloaded or jam cleared to complete the task.
- Any printed material found lying on a print device should be passed to the owner. If the owner is unknown, it should immediately be put to confidential waste and not left on the print device.
- It is the responsibility of every Council employee to inform ICT Service Desk of any noticed concerns/faults with a print device.

Printing at Home

By default, printing at home is NOT enabled and any member of staff requiring printing at home must submit a business case for approval of their Associate Director or Executive Director.

If printing at home the same rules apply as printing in the office. In addition, staff should be especially mindful of secure print storage and destruction.

You must:

- ensure that other family members do not have access to the printer whilst it is being used for SBC work.
- store all work documents in a secure, locked location.
- Securely dispose of (shred) any unwanted documents. If a suitable cross-cut shredder is not available staff should store unwanted prints securely until such time as they can be returned to the office and securely disposed of in one of the office-based approved confidential waste containers.
- ensure that BEFORE disposing of their personal printer ALL paper is removed and the print queue buffer and memory are cleared.

1.7 BUSINESS APPLICATIONS

All software used on the council's network and devices must be evaluated and approved through the Technical Design Authority (TDA) process.

Directorates or users wanting to procure new business applications or software MUST engage with the TDA via the Astro ServiceDesk portal prior to any purchase or use taking place.

Failure to do so will lead to implementation delays, additional cost from the supplier and will be treated as a direct contravention of this policy.

1.8 OVERSIGHT

Information Security colleagues will undertake a risk-based sample of oversight activities against the requirements of this Policy throughout each year, including for example:

- management of assets
- user access management
- data transfers
- mobile device user agreements completion
- removable media read/write access management.
- clear desk reviews
- physical security reviews.

Non-compliances will be reported to the Senior Information Risk Officer (SIRO) and the Associate Director, Chief Digital & Information Officer as appropriate.

1.9 REVIEW AND MAINTENANCE

This Policy shall be reviewed annually, or after a notable change, by the Governance, Reporting & Compliance Manager to ensure it remains adequate and fit for purpose.

2.0 SUPPORTING DOCUMENTATION

This Policy is supported by the following documents:

- Information Security Policy – In progress
- Data Classification and Handling Procedure -— In progress
- Local Code of Conduct for Employees
  5.3 - Local Code of Conduct for Employees.pdf (slough.gov.uk)
- Disciplinary Policy
  Disciplinary Policy Final V2 Oct 20
- Smart Working Policy
  Smart Working Policy