Information Security Policy Acceptable Usage Councillors

May 24

1. Document Control

Version Control

Issue Number	Issue Author	Issue Date	Reason for Issue
1.0	J Wright	Oct-18	Review & Refresh of current policy
2.0	J Wright	Feb-19	Combining of Employee Access, Acceptable Use and Password Management Policies and Rebranding
3.0	J Wright	Feb-21	Policy review
3.1	J Wright	May-21	Review to include Boston Borough Council
3.2	J Wright	Feb-22	Amendment to split Councillor & Officer requirements
4.0	J Wright	May-24	Removal of Officer requirements into a separate policy. General review of the policy wording

Approval Control

Issue Number	Approval Authority	Names	Approval Date	Due for Review
4.0	ELDC/BBC/SHDC	James Gilbert	May-24	May-27
	PSPS	Lewis Ducket	May-24	May-27

Policy Governance

Responsible	Head of ICT & Digital
Accountable	Chief Executive (PSPS), Assistant Director (ELDC/BBC/SHDC)
Consulted	Data Protection Officers, ICT Security Lead, Members Working Groups
Informed	Members

Contents

2. Policy Overview

Policy Aim

2.1 The aim of this Policy is to define the mechanisms and roles through which the Organisation will demonstrate accountability and compliance with regards to ensuring its Members are authorised and trained before accessing the ICT systems. It will define the acceptable usage of the ICT infrastructure/equipment and offer advice and guidance for password and credential management thus ensuring the continued confidentiality, integrity, and availability (CIA) of the Organisation's data. It will also provide Members with clear guidance in the acceptable and appropriate use of the Organisation's ICT equipment and services.

This policy supports The Seven Principles of Public Life

Introduction

2.2 This policy only relates to Members. The Acceptable Usage Policy for Employees is detailed in a separate policy. Where "The Organisation" is referenced, this refers to either South Holland District Council, East Lindsey District Council or Boston Borough Council.

2.3 The Organisation's intention for the publication of this policy is to strike the correct balance between protecting the Organisation, its Councillors, employees, and partners from illegal or damaging actions by individuals, either knowingly or unknowingly and preserving the Organisation's established culture of openness, trust, and integrity.

2.4 In accordance with industry 'best practices' and to comply with compliance regulations, the Organisation has prepared various Information Security policies and procedures which are intended to protect the CIA of their critical client data and their computing resources.

2.5 The purpose of this policy is to outline the acceptable use of computer equipment at the Organisation. It applies to the use of information, electronic and computing devices, and network resources to conduct the Organisation's business or interact with internal networks and business systems, whether owned or leased by the Organisation, the employee, or a third party. It establishes the principles and working practices that are to be adopted by all users for ensuring the ICT systems are used in a manner than preserves security and integrity.

2.6 Computer and telephony resources include, but are not restricted to, the following:

- Desktop computers
- Portable laptop computers
- Tablets (such as iPads)
- Terminals
- Smart phones
- Printers
- Network equipment
- Telecommunications facilities

2.7 The Organisation holds large amounts of personal and classified information. Information security is very important to help protect the interests and confidentiality of the Organisation and its customers. Information security cannot be achieved by technical means alone. Information security must also be enforced and applied by people, and this policy addresses security issues related to people.

2.8 The procedures accompanying this policy are split into 2 key stages of a Member's access to information or information systems used to deliver the Organisation's business:

a) During system usage - users must be trained and equipped to use systems securely and their access must be regularly reviewed to ensure it remains appropriate.

b) Post system access - When a Members requirement for access to information or information systems ends (i.e., when a Member no longer represents a Council ward) - access needs to be removed in a controlled manner where necessary.

Responsibilities

Role	Responsibility
The Organisation's Chief Executive	Supporting Company/Authority compliance with the policy
Member Services	Understanding the policy, ensuring it is available to Members, and advising on it.
Members	Understanding and complying with the policy.

3. Definition

3.1 The Organisation understands that to reduce the risk of theft, fraud or inappropriate use of its information systems, anyone that is given access to Organisation's information systems **must**:

- Fully understand their responsibilities for ensuring the security of the information.
- Only have access to the information they need.
- Only use the information for the purpose it was obtained.
- Request that this access be removed as soon as it is no longer required.

This policy must therefore be applied prior, during, and after any user's access to information or information systems used to deliver the Organisation's business.

Access to Organisation's information systems will not be permitted until the requirements of this policy have been met or if a user is found to be in breach of this policy.

4. Policy Statement

4.1 Members must be aware of, and understand, the following policies:

- Acceptable Usage Policy – this document

4.2 In addition, subject specific policies will be applicable where additional ICT requirements are required, for example Removable Media Policies.

5. New & Departing Members – Member Services Responsibility

General Role and Responsibilities

5.1 Member Services are responsible for ensuring that creation of new and departing Members are notified to the HR/ICT Section as soon as practicably possible, using an agreed process.

5.2 The information security responsibilities of Members must be defined and documented and incorporated into the induction process, as a minimum this will include a statement that every Member is aware of, and understands, the following Council policies:

- Acceptable Usage Policy – this document

Access to the Organisation's Information systems can be revoked if it is found Members have not reviewed and accepted this policy within one month it being released for review. The decision to revoke access will be undertaken by the Leader of the Council and/or the Chief Executive Officer.

5.3 The Organisation must ensure that all Members are aware of information security threats and concerns, their responsibilities, and liabilities, and are equipped to support organisational security policy during their Council work, and to reduce the risk of human error. It is the responsibility of all Members to immediately inform ICT should they have any concerns relating to security or permissions.

Information Security Awareness, Education and Training

5.4 All Members will receive information security awareness training at the beginning of their four-year term and as deemed necessary during this period.

All Members are actively encouraged to do the cyber security online training (Cybsafe) which is provided by the Partnership.

Departing Members

5.5 It is to be ensured that access to Organisational information assets is removed as soon as practicably possible, when no longer required by the Member. Member Services must notify the HR/ICT Section as soon as practicably possible, of the impending departure of a Member so that their access can be suspended.

The appropriate system owners will then be notified to ensure access for that Member is suspended at an appropriate time.

Return of Assets

5.6 Unless otherwise agreed, Member Services will ensure that the Member returns all the organisation's assets in their possession upon cessation of their elective period. This must include any copies of information that is not in the public domain.

6. General Use and Ownership

6.1 Organisational information that is outside of the public domain and is stored on electronic and computing devices remains the sole property of the Organisation. Members must ensure through legal or technical means that information is protected, and they should understand their responsibilities under the statutory legislation.

6.2 Members have a responsibility to promptly report the suspected or actual theft, loss, or unauthorised disclosure of the Organisation's proprietary information in accordance with the Incident Management Procedure contained within this policy.

6.3 Members have a responsibility to promptly report the suspected or actual theft, loss, or unauthorised access to ICT of any Organisational ICT provided physical asset.

6.4 Members have a responsibility to ensure ICT equipment is in suitable physical locations e.g., in a location limiting the risk from environmental hazard (such as heat, water, dust etc.) and in a location limiting the risk of theft.

6.5 Members have a responsibility to ensure any Organisational data they are processing is not visible by anyone where there exists no business need, for example, colleagues, customers, family etc.

6.6 Members have a responsibility to report any suspected or confirmed ICT Security events in accordance with the ICT Incident Management Procedure included in this policy.

6.7 Connecting to cloud-based services, for example Microsoft 365, that hold corporate information should only be conducted from a corporate device.

6.8 Authorised individuals within the Organisation may monitor equipment, systems, and network traffic at any time, in accordance with the ICT Forensics and Audit Computing Procedure.

6.9 The Organisation retains the right to monitor and access use of its data and systems/services to ensure continued compliance with this policy.

7. Security and Information

7.1 System level and user level passwords must comply with the Password Management section of this Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

7.2 Only Organisation owned devices must be connected to the ICT network.

7.3 The connection of non-Organisation owned equipment to the corporate network is strictly prohibited. Guidance should be sought from the ICT Department if this is a requirement.

7.4 Members are encouraged to exercise extreme caution when opening e-mail attachments received from unknown senders. If in any doubt as to the legitimacy of an email then the email and/or attachment should not be opened, and the email must be forwarded to suspicious.emails@pspsl.co.uk

7.5 Members are encouraged to exercise extreme caution with the transmittal of data and must not under any circumstances transmit by email or any other method, any file which they know to be infected with a virus, malware etc. unless under the express instruction if the ICT Service Desk. Members must report any suspected files to the ICT Service Desk.

7.6 Members should seek ICT support before the download of data or programs of any nature from unknown sources.

7.7 Members must not remove, replace of change configuration settings of the anti-virus system on any computer which they use to access the ICT facilities.

7.8 Members must not forward virus warnings to any person or department other than to the ICT Service Desk or suspicious.emails@pspsl.co.uk.

7.9 It is strongly advised that data should not be saved to the local drive of end user devices, doing so will result in data loss in the event of a device malfunction.

8. Email and Communications

8.1 All use of email and instant message systems, such as Teams, must be consistent with the Organisation's values and ethos of ethical conduct, safety, compliance with applicable laws and proper business practices.

8.2 The Organisation's email accounts and instant message systems, should be used primarily for Council/Ward purposes; personal communication is permitted on an appropriate basis, but non-Organisation's related commercial uses are prohibited.

8.3 All emails that are used to conduct or support official business must be sent using a "@e-lindsey.gov.uk", "@boston.gov.uk" or "@sholland.gov.uk" address.

8.4 Email should be retained only if it qualifies as a business record. Email is a business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email. Any email that required preserving as such should be held outside of the email system.

8.5 Email that is identified as a business record shall be retained according to the Organisation's Record Retention Schedule and/or Member Information Asset Registers and in accordance with current legal and regulatory requirement.

8.6 Members shall have no expectation of privacy in anything they store, send, or receive on the Organisation's email and instant message systems.

8.7 The legal status of an email message is like any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official Organisational business should be an official communication. All external email will carry the official Organisational disclaimer. A copy is available upon request to the Organisation's ICT Department.

8.8 Email must not be any less formal than memos or letters that are sent out from a particular Service or the Organisation. When sending external email, care should be taken not to contain any material which would reflect poorly on the Organisation's reputation or its relationship with customers, clients, or business partners.

8.9 Whilst respecting the privacy of Members, the Organisation maintains its legal right, in accordance with current legal and regulatory requirements to monitor and audit the use of email and instant message systems to ensure adherence to this Policy. Members should be aware that deletion of e-mail and messages from individual accounts does not necessarily result in permanent deletion from the ICT systems.

8.8 Access to another Members email is strictly forbidden unless the Member has given their consent or is the subject of a legitimate ongoing investigation. If this is the case, access will be provided by the Organisation's ICT Department upon receipt of an ICT Service Request submitted by the Chief Executive. Access to a Members email account must be absolutely necessary and must be carried out regarding the rights and freedom of the Member.

8.9 It should be noted that email, instant messages and attachments may need to be disclosed in accordance with the ICT Audit & Forensic Computing Principle.

8.10 There may be instances where a Member will receive unsolicited mass junk email or spam. It is recommended that Members delete such messages without reading them or replying to them. The Organisation employs a sophisticated email filtering solution which is used to block unwanted email as appropriate.

8.11 The Organisation's email service will not process emails in excess of 60 megabytes. Members should be aware that not all external Internet Service Providers will be able to process email of this size, therefore they should check with the intended recipient whether the email has been received.

8.12 The Organisation will ensure that email is virus checked at the network boundary and at the host, and where appropriate will use two functionally independent virus checkers.

8.13 Confidentiality of an email cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of the network.

8.14 It should be noted and understood that email is not a guaranteed delivery protocol and where guaranteed delivery is a requirement, alternate means of information transmission should be utilised.

8.15 Care should be taken when addressing all emails, but particularly where they include sensitive or confidential information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

9. Social Media

9.1 The use of social media by Members, whether using the Organisation's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy.

a) Members shall not engage in any discriminatory, disparaging, defamatory or harassing comments when utilising social media or otherwise engaging in any conduct prohibited by the Organisation.

b) Members may also not attribute personal statements, opinions or beliefs to the Organisation when engaged in social media. If a Member is expressing his or her beliefs and/or opinions, the Member may not, expressly, or implicitly, represent themselves as a representative of the Organisation. Members assume any and all risk associated with social media.

9.2 The golden rule for using social media is "if you are unsure about posting something, stop and ask for advice first before doing anything else."

9.3 Social media works in the public domain. Once something is published it is 'out there' for everyone to see and very easily it can:

- go viral.
- be altered or changed without your consent.
- be taken out of context.
- be shared around the world.

Using social media as Member is very different from using for personal use.

9.4 Members are personally responsible for the social media content they create, publish and share. Being a Member will not prevent someone else pursuing legal action following the publication of an untrue statement. In such a situation, it is likely that you will be held personally liable.

9.5 Members should be mindful of the difference between fact and opinion. They also play a central role in preventing the spread of disinformation. Think twice before you press ‘share’ or ‘retweet’.

9.6 On social media, Members should also keep in mind their responsibility in relation to confidential information, copyright, data protection, the pre-election period, and exempt reports. Members are still subject to the Code of Conduct on social media where there is an explicit link between the content posted and council business or your role as Member. As a rule, councillors should demonstrate good conduct at all times and so should act as though their public engagement on social media falls in scope of the Code of Conduct.

9.7 It is essential that Members do not publish, on any social media channel, information relating to a potential or confirmed cyber-attack on the Organisation. Social media blackout is an essential action at such times and must be strictly adhered to.

9.8 When posting to social media you should remember that:

- you are an elected representative of your council.
- what you post can affect the reputation of your council
- your council is a corporate decision-making body – you can’t, independently, make decisions for the council on social media.
- some issues and communications are best left to your council’s official social media channels, which are usually managed by officers.
- having a single voice or message can be critical in some situations – for example, in the event of major flooding.
- you don’t have to respond to or comment on everything on social media – and sometimes it’s best not to.

9.9 Think before you press ‘publish’. There is a simple test. if you would be reluctant to say something face-to-face to a group of strangers in the street, then you probably shouldn’t say it on social media.

9.10 It is strongly recommended that members refrain limit official communication to Organisational approved channels. This does not include WhatsApp, Snapchat etc. Information as to the appropriate methods of communication can be obtained from Member Services.

10. Internet

10.1 Members accept that the Organisation is not responsible for any personal transactions they enter into - for example in respect of the quality, delivery or loss of items ordered. They must accept responsibility for, and keep the Organisation protected against, any claims, damages, losses or the like which might arise from their transaction - for example in relation to payment for the items or any personal injury or damage to property they might cause.

10.2 Where using the corporate network, personal use of the internet will still be subject to the same content filtering as applied to corporate internet access and will be subject to monitoring and usage reporting.

10.3 Where using the corporate network, the provision of Internet access is owned by the Organisation and all access is recorded, logged, and interrogated for the purposes of compliance with statutory, regulatory, and internal policy requirements.

11. Unacceptable Use

11.1 The following activities are, in general, prohibited.

a) Under no circumstances is a Member of the Organisation authorised to engage in any activity that is illegal under local, British, European, or international law while utilising Organisation owned resources.

b) The lists below are by no means exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use detail in section 18.2.

c) Any unacceptable use of ICT systems/services will be subject to the Organisation's Members Policies.

12. Destroying Information

12.1 You must destroy hard copy information securely when no longer required. You can achieve this by:

- Using a crosscut shredder
- Using a confidential waste bin located within Council premises.
- You must always control access to information until it is securely destroyed.

12.2 You must not place hard copy information in open waste bins or waste skips.

12.3 You must securely delete digital information from hardware and media when no longer required.

12.4 You must consider several factors when destroying or sanitising digital information including:

- the sensitivity of the data therein
- the type of hardware or media
- the potential re-use of the hardware

12.5 Should you need specialist advice please contact the ICT Service Desk

13. System and Network Activities

13.1 The following activities are strictly prohibited, with no exceptions:

a) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution products that are not appropriately licensed for use.

b) Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Organisation or the end user does not have an active license is strictly prohibited.

c) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

d) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

e) Revealing account passwords to others or allowing use of accounts by others. This includes family and other household members.

f) Using a corporate computing asset to actively engage in procuring or transmitting material that is in violation of UK law.

g) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the Member is not an intended, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping flooding, packet spoofing, denial of service, and forged routing information for malicious purposes.

h) Executing any form of network monitoring which will intercept data not intended for the Members host.

i) Circumventing user authentication or security of any host, network, or account.

14. Email Activities

14.1 Once you send an email, you lose control over who has access to the content. Recipients can easily forward the email. The further the email gets from the person who wrote it, the less awareness there will be of its privacy and security implications. Anytime you write an email, think twice about including personal data. Remember that it could be forwarded countless times without your knowledge.

14.2 The following activities are strictly prohibited, with no exceptions:

a) Sending unsolicited email messages, including the sending of "junk mail", chain letters or other advertising material to individuals who did not specifically request such material (email spam).

b) The email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Members who receive any emails with this content from any employee/Member should report the matter immediately.

c) Unauthorised use of email header information.

d) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

e) Automatically forwarding email to a third-party email system. Individual messages which are forwarded by the user must not contain information that is not in the public domain.

f) Non-work email accounts must not be used to conduct or support official Organisation business. Members must ensure that any emails containing sensitive information must be sent from an official email address. Emails that contain sensitive/special category data should be contained within a password protected document rather than in the text of the email.

g) The unauthorised transmission to a third party of personal or confidential material concerning the activities of the Organisation.

h) The transmission of material such that this infringes the copyright of another person, including intellectual property rights.

i) Under no circumstances should personal or confidential information be emailed to a private non-Organisation email address.

Data integrity and sensitivity concerns

14.3 Member should have awareness that when an email is forwarded, there is a risk of unintended changes to the content. This can lead to inaccuracies or misrepresentations of the original information. There will be no clear record of who modified what. Furthermore, attachments or links within the original email may become outdated or compromised, potentially exposing recipients to security threats.

14.4 Members should have awareness that forwarding or using functions such as CC (Carbon Copy), BCC (Blind Carbon Copy) or reply all to an email exposes the original sender's email address and other contact details to others. This could expose the person to unsolicited communications, ads, or even targeted attacks. When it comes to personal data, only share it on a need-to-know basis.

14.5 Members should have awareness that if they forward a phishing email unknowingly or without proper scrutiny, it can spread the phishing attempt to a larger number of recipients. This can lead to an increased risk of individuals falling victim to the scam and disclosing sensitive information.

14.6 Members should consider the use the CC and BCC. They should seek to protect people's privacy by considering and avoiding the potential unintended consequences of sharing what others have written.

14.7 Members should consider the appropriate use of CC, BCC and Reply all to ensure it is appropriate for the purpose and content of the email and considering the impact to the recipient.

15. Cloud Storage (Excluding Microsoft 365)

15.1 Cloud Storage (for example, iCloud) is not to be considered as a file storage area; files are not to be retained within this area. Once transferred to or from the third party has concluded the files should be deleted.

15.2 Cloud Storage carries a risk of Virus transmission. Please ensure any files from third parties are expected and as agreed. Do not transfer a file if the third party has not informed the Member of its arrival, always enquire if unsure.

15.3 Please do not transfer Official-Sensitive information via Cloud Storage. If a Member is unsure what type of information is appropriate, please contact the ICT Department or the Date Protection Officer.

16. Mobile Data

16.1 In addition to the information contained withing this policy statement, the following details should be noted:

a) All members should seek to use Wi-Fi as their primary data transition method, where this is not achievable, mobile data may be used.

b) An Organisational data bundle is in use to support the provision of mobile data. This is a shared bundle of data that is used by all users. To ensure the Organisation does not incur significant overuse expense, it reserves the right to monitor and limit the use of Mobile data.

17. Internet Access

17.1 Access to the following categories of websites is strictly prohibited when using a corporate provided device, or a personal device connected to the corporate network. Whilst ICT utilise technology to restrict access it should not be assumed that successful access of a website means that that site is not prohibited.

17.2 These categories are neither exclusive nor exhaustive. *"Unsuitable"* material would include data, images, audio files or video files the transmission of which is illegal under

British law, and material that is against the rules, essence and spirit of this and other Organisational policies.

- Illegal
- Pornographic
- Violence
- Hate and discrimination.
- Offensive
- Weapons
- Hacking

17.3 Members must not seek to create download, upload, display or access knowingly, sites that fall within these categories or other “unsuitable” material that might be, using practical judgement be deemed illegal, obscene, or offensive.

18. Password Management

Password Creation

18.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines* below.

Password Construction Guidelines

18.2 All passwords should meet or exceed the following guidelines.

Strong passwords have the following characteristics:

- Contain at least 12 alphanumeric characters.
- Contain both upper- and lower-case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).
- A passphrase is more secure than a password e.g., imgladmypasswordisagoodone246!”£
- A 3-word phrase is recommended, substituting numbers and special characters e.g., I’mGladMyP@ssw0rdIsAS3cure1

Poor, or weak, passwords have the following characteristics:

- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backwards or preceded or followed by a number (for example, terces, secret1 or 1secret).

- Are some versions of “Welcome123” “Password123” “Changeme123”

Protecting Passwords

18.3 The following guidelines must be adhered to at all times:

a) Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.

b) Do not share passwords with anyone, including Executive Assistants, other Members, Officers, and family members.

c) Never write passwords down or store them where they are open to theft.

d) Passwords must not be inserted into email messages,

e) Passwords must not be revealed over the phone to anyone. ICT will never ask you for your password.

f) Never store your passwords in a computer system without encryption.

g) Do not use any part of a username within a password.

h) Do not use the same password to access different Organisation systems.

i) Do not use the same password for systems inside and outside of work.

Changing Passwords

18.4 All user-level passwords must be changed whenever a system prompts it to be changed.

18.5 Default passwords must also be changed immediately. If a Member becomes aware, or suspects, that their password has become known to someone else, they must change it immediately and report their concern to the ICT Service Desk.

18.6 Members must not reuse the same password within 20 password changes.

18.7 Password cracking or guessing may be performed on a periodic or random basis by the ICT Team or its chosen security partner. If a password is guessed or cracked during one of these scans, the Member will be required to change it to be following the Password Construction Guidelines.

19. Anti-virus Protection

19.1 All ICT equipment will have the latest Anti-Virus signature and Windows Update files when connected to the network. Users who work remotely must ensure that their portable computer devices are connected to the corporate network at least daily to enable the Anti-Virus software to be updated.

20. Security Updates

20.1 ICT regularly push security, operating system, and application updates to corporate provided end user devices. It is therefore essential that Members who utilise laptops connect them to the corporate network at least once a week to enable their device to obtain the updates.

20.2 Members should “restart” their end user device at least weekly in order to ensure that these updates are correctly installed. Restarting is not the same as logging off or shutting down.

20.3 Members who use Apple devices should check for and install system updates as soon as they become available.

21. Remote Working

21.1 It is the responsibility of the Organisation’s Members with remote access privileges to the corporate network to ensure that they use the same level of due diligence when using a remote access connection as they do when working directly within a Council premise.

21.2 All ICT equipment supplied to Members to facilitate remote working is the property of the Organisation. It must be returned upon the request.

21.3 Only Organisation supplied equipment is to be used for remotely accessing Organisation ICT systems and data.

22. Member Responsibility

22.1 It is the responsibility of a Member to ensure that the following points are adhered to at all times:

22.2 All Members must comply with appropriate codes and policies associated with the use of ICT equipment.

22.3 All Members must comply with the Members Access Policy – this document.

22.4 Only print out an official document as a last resort and only when there is no other means of accessing that document when required,

22.5 Report any instance where uncollected documentation has been found uncollected from a printer.

22.6 Ensure that paper documents, that are vulnerable to theft if left accessible to unauthorised people, are securely locked away in suitable facilities (e.g., secure filing cabinets) when not in use.

22.7 Paper versions of documents containing personal or confidential information must be shredded to required standards as soon as they are no longer required.

22.8 All paper documentation must not be stored with the portable computer device.

22.9 All Members are expected to undertake a Risk Assessment of their working environment in accordance with Health & Safety policies.

22.10 All Members are expected to undertake a dynamic risk assessment for their working location, to include, but not limited to, the ability for non-Organisation staff to view corporate and potentially sensitive data.

22.11 All Members have a responsibility to promptly report the theft, loss or unauthorised access of the Organisation's equipment in accordance with the ICT Incident Management Procedure section of this document.

22.12 Members must take due care and attention of portable computer devices when moving between home and another business site.

22.13 Members will not install any software on to an Organisation owned laptop computer without the prior agreement from ICT.

22.14 Members will not change the configuration of any Organisation owned portable computer device.

22.15 Members will not install any hardware on to or inside any Organisation owned portable computer device, unless authorised by a member of the ICT Department.

22.16 Members will allow the installation and maintenance of Anti-Virus updates immediately.

22.17 Members will allow the installation of software patches and updates immediately.

22.18 Members will return the device to Organisation's sites at periodic intervals to allow for the installation of major updates and changes, as deemed necessary by the ICT department.

22.19 Members will inform the ICT Service Desk of any Organisation owned portable computer device message relating to configuration changes.

22.20 Any files containing personal data or data which is business critical should be stored on the Organisation's centralised file servers wherever possible and not held on portable computer devices.

22.21 All faults must be reported to the ICT Service Desk.

22.22 Members must not deliberately remove or deface any asset registration number.

22.23 Members requests for upgrades of hardware or software must be approved by an authorised individual. Equipment and software will then be purchased and installed by a member of the ICT Department.

22.24 No family members may use the ICT equipment. The ICT equipment is supplied for the staff members' sole use.

22.25 The Members must ensure that reasonable care is taken of the ICT equipment supplied. Where any fault in the equipment has been caused by the Members, in breach of the above paragraphs, the Organisation may recover the costs of any repair.

22.26 The Members will seek advice from the Organisation before taking any supplied ICT equipment outside the United Kingdom. The equipment may not be covered by the Organisation's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel.

22.27 The Organisation may at any time, and without notice, request a software and hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All Members must co-operate fully with any such audit.

22.28 All removable media devices must not be stored with the portable computer device.

22.29 Portable computer devices must be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

22.30 The Organisation retains the right to monitor and access use of its data and systems/services to ensure continued compliance with this policy.

22.31 It is also strongly recommended that Members should: be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

22.32 Members are strongly advised not leave equipment where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. Devices should not be left either on or in standby mode, with Bluetooth\wireless devices turned on. Ideally endeavour that the office area of the house is kept separate from the rest of the house.

22.33 Ensure that all ICT equipment is secured whenever it is not in use.

22.34 Members should ensure that access / authentication tokens and personal identification numbers are kept in a separate location to the portable computer device at all times.

23. Access Controls

23.1 It is essential that access to all personal or confidential information is controlled. This can be done through physical controls, such as locking the home office or locking the

computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or User Login controls.

23.2 All data on portable computer devices must, where possible be encrypted. If this is not possible, then all personal or confidential data held on the portable device must be encrypted.

23.3 The approved Virtual Private Network (VPN) software or hardware device must be configured to allow remote users access to Organisation's systems if connecting over Public Networks, such as the Internet. This must use or be used upon an approved client provided by the Organisation.

23.4 Connecting to cloud-based service that hold corporate information should only be conducted from a corporate device; for example, MS 365

23.5 The corporate device acts as MFA for the user's primary tenant, with a separate MFA token or authenticator app for secondary tenants

23.6 Two-factor authentication must be used when accessing the Organisation's network and information systems (including Outlook Web Access) remotely. Such authentication involves the use of "something you have" e.g., a certificate on a laptop or a supplied Remote Access Point and "something you know" e.g., a password.

23.7 Access to the Internet from a laptop, should only be allowed via onward connection through the Organisation's Proxy Servers and not directly to the Internet.

24. Incident Management Procedure

Definition

24.1 This procedure needs to be applied as soon as information systems are suspected to be or are affected by a security event which is likely to lead to an incident resulting in the compromise of service or loss of data.

24.2 The definition of a "security event" is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. ICT Incident management is concerned with intrusion, compromise and misuse of information systems and resources.

24.3 A security event could also be the result of:

- Uncontrolled system changes
- Access violations – e.g. password sharing
- Breaches of physical security
- Non-compliance with policies

Event Reporting

24.4 Security Events and weaknesses need to be reported at the earliest possible stage to the ICT Service Desk. The ICT Team will identify when a series of events or weaknesses have escalated to become an incident. It is vital for the ICT Section to gain as much information as possible from the business users to identify if an incident is occurring.

24.4.1 All events that have the potential to result in the unauthorised disclosure of personal or sensitive data must also be reported in accordance with the Data Protection Policy and associated Breach Management Procedure, to the Organisation's Data Protection Officer (DPO) who may inform the Information Commissioner's Office (ICO).

24.4.2 The DPO and the ICT Security team will validate the impact of the event and offer guidance as required.

Suspicious Activity on ICT equipment

24.5 Security events that relate to equipment, for example a virus infection, could quickly spread and cause data loss across the Organisation. All members must understand and be able to identify that any unexpected or unusual behaviour on their device could potentially be a software malfunction.

24.5.1 If an ICT event is detected members **must**:

- Note the symptoms and any error messages on screen.
- Immediately disconnect from any WI-FI or VPN connections

Violation of Controls/Measures

24.6 Non-equipment related events are also expected to be reported to the ICT Service Desk upon identification, for instance.

- Uncontrolled system changes
- Access violations – e.g. password sharing
- Breaches of physical security
- Non-compliance with policies
- Human errors

Lost or Stolen ICT Equipment

24.7 Any provided ICT equipment that has been misplaced/lost is to be reported to the ICT Service Desk immediately to allow for controls to be put in place to stop data loss/leakage.

24.7.1 Any provided ICT equipment that has been stolen needs to be reported to the ICT Service Desk immediately and then reported to the Police, a crime reference number obtained, and the ICT Service Desk Incident updated.

24.7.2 All events, whether suspected or confirmed should be reported immediately to the ICT Service Desk.

25. Review

25.1 As a standard principle, this policy should be reviewed at least once every three years to ensure that it remains fit for purpose. It may need reviewing more regularly in response to specific legislation changes or changes to best practice guidance.

26. Policy Compliance

26.1 Should any Member be found to have breached this policy; the issue will be reviewed by Senior Management.

26.2 If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

26.3 If a member does not understand the implications of this policy or how it may apply to them, they should seek advice from the ICT Department.

27. Related Policies

Local Authority Constitution

The Seven Principles of Public Life