Information Security Policy
Acceptable Usage Policy
Officer

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 Officer 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 Councillor requirements into a separate policy. General review of the policy wording including the addition of remote working direction.

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	Officers

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 Officers 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 Officers with clear guidance in the acceptable and appropriate use of the Organisation's ICT equipment and services.

Introduction

2.2 This policy only relates to Officers. Where the term "Officer(s)" is referenced, this refers to an individual that is Officer regardless of employment type, contractor, or any other individual that undertakes work paid or unpaid on behalf of The Organisation.

Where "The Organisation" is referenced, this refers to either Public Sector Partnership Services or its Client Council's South Holland District Council, East Lindsey District Council or Boston Borough Council.

2.2.2 Access policy for Members is detailed in a separate policy.

2.2.3 Access policy for third parties is detailed in a separate policy.

2.3 The Organisation's intention for the publication of this policy is to strike the correct balance between protecting the Organisation, its Councillors, Officers, 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 Officer, 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 3 key stages of an Officer's access to information or information systems used to deliver the Organisation's business:

a) Pre-system access - checks must be made to ensure that the individual is suitable to allow access to information systems, these might include pre-employment checks, DBS check etc.

b) 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.

c) Post system access - When a user's requirement for access to information or information systems ends (i.e., when a user terminates their employment with the Organisation or changes their role so that access is no longer required) - 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
Senior Leadership Team	Ensuring the policy adheres to statutory legislation & guidance and that it is embedded in the workforce and ensuring managers and Team Leaders show compliance with the policy and it is understood.
Managers & Team Leaders	Understanding and complying with the policy, ensuring it is available to team Officers, and advising on it.
All Officers	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.

3.2 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.

3.3 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 Officers must be aware of, and understand, the following policies:

- This policy – ICT Acceptable Usage Policy
- Systems Acquisition, Development and Deployment Policy

In addition, subject specific policies will be applicable where additional ICT requirements are required, for example Removable Media Policy and Artificial Intelligence Policy.

There are several principles in place to support the operational delivery of ICT, such as the Audit & Forensics Principle and Cryptographic Principle, these can be accessed upon request.

5. Starters & Leavers – Line Manager Responsibility

Prior to Employment

5.1 The Organisation must ensure that potential Officers are recruited for roles in line with the Organisation's Recruitment and Selection Policy. Due consideration should be given for the need to reduce the risk of theft, fraud or misuse of information or information systems by those users.

Roles and Responsibilities

5.2 The decision as to an Officers appropriate level of access to information and information systems is the responsibility of the appropriate Service Manager.

5.2.1 Line managers are responsible for ensuring that the creation of new Officer accounts, changes in role, and termination of Officer accounts are notified to both ICT and HR Departments using an agreed process and with at least two weeks' notice,

5.2.2 Applications for access to ICT services must only be submitted by an authorised Officer of staff.

5.2.3 The information security responsibilities of users must be defined and documented and incorporated into induction processes and contracts of employment. As a minimum this will include:

- A statement that every user is aware of, and understands, the following Council policies:
- ICT Acceptable Usage Policy
- Systems Acquisition, Development and Deployment Policy

5.2.4 Access to the Organisation's Information systems will be revoked if it is found that an Officer has not reviewed and accepted the relevant Information Security Framework policies within 1 month of this policy being released for review to an Officer.

User Screening

5.3 In line with HR policy background verification checks must be carried out on all potential Officers, in accordance with all relevant laws, regulations and ethics. The level of such checks must be appropriate to the business requirements, the classification of the information to be accessed, and the risks involved.

5.3.1 Where applicable due to the specific role being undertaken by the Officer additional DBS checks must be carried out to an appropriate level as demanded by law.

5.3.2 Where access is to systems processing payment card data, credit checks on the Officer must be carried out to an appropriate level as required by the Payment Card Industry Data Security Standards (PCI-DSS).

5.3.3 All the above requirements for verification checks must also be applied to any Officer that occupies a position that enables them to have access to systems or data contained linked a system (e.g. backup tapes, printouts, test datasets).

Terms and Conditions of Employment

5.4 Each Officer must sign a confidentiality statement that they understand the nature of the information they access, that they will not use the information for unauthorised purposes

and that they will return or destroy any information or assets when their employment terminates.

During Employment

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

5.5.1 It is also necessary that changes in on Officers in role or business environment are carried out in a systematic manner that ensures the continuing security of the information systems to which they have access. Such changes must be requested via the ICT Service Desk.

Management Responsibilities

5.5.2 Line managers must notify the appropriate function as soon as practicable, of any changes in a user's role or business environment, to ensure that the user's access can be changed as appropriate.

5.5.3 Processes must ensure that access to information systems is extended to include new user requirements and that any access that is no longer needed is removed.

5.5.4 Any changes to user access must be made as soon as practicable and be clearly communicated to the user.

5.5.5 Departmental managers must ensure that staff understand and be aware of information security threats and their responsibilities in applying appropriate Organisation policies.

Information Security Awareness, Education and Training

5.5.6 The organisation is committed to the training of all users on security education, training, and awareness.

5.5.7 All users must undertake appropriate information security awareness training and regular updates in related statute and organisational policies and procedures as appropriate to their role.

5.5.8 It is the role of managers to ensure that their staff are adequately trained and equipped to carry out their role efficiently and securely.

Job Role Changes & Leavers

Secure Termination of Employment

5.6 Termination of employment may be due to resignation, change of role, suspension or the end of a contract or project or many other reasons. The key requirement is that access to Organisational information assets is removed as soon as practicably possible, when no longer required by the user.

Termination Responsibilities

5.6.1 Line managers must notify the HR/ICT Department as soon as practicable, but ideally with at least 2 weeks' notice, of the impending termination or suspension of employment so that their access can be suspended on the day of departure.

5.6.2 The appropriate system owners will then be notified to ensure access for that user is suspended at an appropriate time, considering the nature of the termination.

5.6.3 Responsibilities for notifying changes, performing employment termination or change of employment must be clearly defined and assigned.

Return of Assets

5.6.4 Line Managers have an unequivocal responsibility to ensure that users return all of the organisation's assets in their possession upon termination of their employment, contract, or agreement. This must include any copies of information in any format.

Removal of Access Rights

5.6.5 Processes must be implemented to ensure that all access rights of users of Organisational information systems shall be removed as soon as practicably possible, upon termination or suspension of their employment, contract, or agreement.

5.6.6 Processes and responsibilities must be agreed and implemented to enable emergency suspension of a user's access when that access is considered a risk to the Organisation or its systems.

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. Officers must ensure through legal or technical means that information is protected, and they should understand their responsibilities under the statutory legislation.

6.2 Officers 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 ICT Incident Management Procedure, Data Protection Policy, and the associated Breach Management Procedure.

6.3 Officers 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 Officers have a responsibility to ensure ICT equipment is located 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 Officers 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 Officers have a responsibility to report any suspected or confirmed ICT Security events in accordance with the ICT Incident Management Procedure.

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 Principle

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.

6.10 Information stored on electronic and computing devices remains the sole property of the Organisation. Officers must ensure through legal or technical means that information is protected and should understand their responsibilities under the statutory legislation.

6.11 Officers may access, use or share the Organisation's information only to the extent it is authorised and necessary to fulfil their assigned role duties.

6.12 The Organisation operate a clear desk policy, both home and office locations should be clear of personal, confidential, or any information relating to clients or citizens at the end of each day. Work should be stored in a secure location.

6.13 The Organisation retains the right to use a performance/productivity monitoring system to monitor and report on the ICT usage within the Organisation. Were such a system is used a “Statement of Intent” will be published clearly articulating its controls, intent, and oversight.

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 and may lead to disciplinary action.

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

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

7.4 Officers must 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 Officers must 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. Officers must report any suspected files to the ICT Service Desk.

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

7.7 Officers must not try to circumvent any of the mechanism used to control and monitor software or settings.

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

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

7.10 Officers must report any suspected files to the ICT Service Desk.

7.11 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.

7.12 All computing devices must be secured with an automatic lock set to 10 minutes or less. In addition, Officers are expected to routinely manually lock the screen or log off when the device is unattended, using “Windows Key + L”

7.13 Remote access to the Organisation’s ICT network must be explicitly requested through the ICT Service Desk.

7.14 Partners or 3rd party suppliers must not be given details of how to access the Organisation’s network without permission from the ICT Department.

7.15 Access provision must be made in accordance with the Starters and Leavers procedure.

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/individual email accounts and instant message systems should be used primarily for business-related purposes; personal communication is permitted on a limited 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”, “@sholland.gov.uk” or “@pspsl.co.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 All data contained within an email message, or an attachment must be secured according to the current company standard.

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

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

8.8 The legal status of an email message is similar to 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 considered to 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.

8.9 Using a reasonable amount of the Organisation's resources for appropriate personal emails is acceptable during non-working hours or breaks, but non-work-related email shall be saved in a separate folder from work related email.

8.10 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.

8.11 Whilst respecting the privacy of authorised users, 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 by authorised users to ensure adherence to this Policy. Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the ICT systems. Where a manager suspects that the email facilities and instant message systems are being abused by a user, they should contact the ICT Service Desk.

8.12 Access to another Officers email is strictly forbidden unless the Officer has given their written consent, is the subject of a legitimate ongoing investigation or their email needs to be accessed by their line manager for specific work purposes whilst they are absent. If this is the case, access will be given on the submission of an ICT Service Request submitted by the authorising Officer. Access to an Officer's email account must be necessary and must be carried out with regard to the rights and freedom of the Officer. Managers must only open emails which they believe to be relevant.

.

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

8.14 There may be instances where an Officer will receive unsolicited mass junk email or spam. It is recommended that the Officer 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.

8.15 The Organisation's email service will not process emails in excess of 60 megabytes. Officers 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.

8.16 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.

8.17 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.

8.18 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.

8.19 Care should be taken when addressing all emails, but particularly where they include sensitive or confidential information, to prevent accidental transmission to unintended recipients. Consideration should be given to the ability for emails to be forwarded on without an Officers knowledge or approval. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

The following activities are strictly prohibited, with no exceptions:

a) Sending unsolicited email and instant 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 and instant messaging 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. Officers 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 or instant message systems must not be used to conduct or support official Organisation business. Officers 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.

j) The creation or transmission of material which brings the Organisation into disrepute.

Data Integrity and Sensitivity Concerns

8.20 Officers 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.

8.21 Officers 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.

8.22 Officers 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.

8.23 Officers 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.

8.24 Officer 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.

9. Social Media

9.1 The use of social media by Officers, 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) Officers 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) Officers may also not attribute personal statements, opinions or beliefs to the Organisation when engaged in social media. If an Officer is expressing his or her beliefs and/or opinions, the Officer may not, expressly, or implicitly, represent themselves as a representative of the Organisation. Officers 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 an Officer is very different from using for personal use.

9.4 Officers are personally responsible for the social media content they create, publish and share. Being an Officer 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 Officers 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, Officers should also keep in mind their responsibility in relation to confidential information, copyright, data protection, the pre-election period, and exempt reports. Officers 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 an Officer. As a rule, Officers 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 Officers 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 a representative of The Organisation.
- what you post can affect the reputation of The Organisation
- The Organisation is a corporate decision-making body – you can't, independently, make decisions for The Organisation on social media.
- 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 Officers 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 the relevant Communications Teams.

10. Internet

10.1 Officers accept that the Organisation is not responsible for any personal transactions they enter - 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.

10.4 Access to the corporate Internet provision should only be used to access anything in pursuance of an Officer work including access to and/or provision of information, research, electronic commerce (e.g., purchasing equipment).

10.5 At the discretion of an Officers people manager, and provided it does not interfere with their work, the Organisation permits appropriate personal use of the Internet in an Officers own time (for example during their lunchbreak or before or after work).

10.6 When using Organisation resources to access and use the Internet, users must realise they represent the Organisation. Whenever an Officer states an affiliation to The Organisation, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of The Organisation".

10.7 Officers accept that the Organisation is not responsible for any personal transactions they enter - for example in respect of the quality, delivery or loss of items ordered. Officers 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.

10.8 Officers must ensure that personal goods and services purchased are not delivered to the Organisation's property. Rather, they should be delivered to the Officers home or other personal address.

10.9 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.

10.10 All personal usage must be in accordance with this policy. Officers' computer and any data held on it are the property of the Organisation and may be accessed at any time by the Organisation to ensure compliance with all its statutory, regulatory and internal policy requirements.

10.11 Officers access to social media for personal use is with explicit consent of their people manager and provided it does not interfere with their work. Such requests will be reviewed on an individual basis.

11. Unacceptable Use

11.1 The following activities are, in general, prohibited. Officers may be exempted from these restrictions during their legitimate job responsibilities by an Officer of the Senior Management Team.

a) Under no circumstances is an Officer 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 Disciplinary Policies.

System and Network Activities

11.2 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) Unauthorised storing, loading or execution of software which has not been purchased in accordance with Organisation procurement procedures and in line with the Systems Acquisition and Development Policy.

d) Unauthorised execution of software that has not been the subject of formal virus checking procedures.

e) Accessing data, a server, or an account for any purpose other than conducting corporate business, even if they have authorised access.

f) 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.

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

h) Revealing their account password to others or allowing use of their account by others. This includes family and other household Officers when work is being done at home.

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

j) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the Officer is not an intended recipient or logging into a server or account that the Officer is not expressly authorised to access, 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.

k) Executing any form of network monitoring which will intercept data not intended for the Officer's host, unless this activity is a part of the Officer's normal job/duty.

l) Circumventing user authentication, controls, monitoring or security of any host, network, or account.,

m) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

n) Storing, processing, or printing of data for a purpose which is not related to the business activity of the Organisation.

o) Providing information about, or lists of, the Organisation's Officers to parties outside of the Organisation.

Cloud Storage

11.2.1 Cloud Storage is only to be used to transfer files between agreed parties. Only files that have been added by or for agreed third parties must be transferred, no personal use is permitted.

11.2.2 Cloud Storage is not considered a file storage area, files are not to be retained. Once transfer to or from the third party has concluded the files should be deleted.

11.2.3 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 Officer of its arrival, always enquire if unsure.

11.2.4 Do not transfer Official-Sensitive information via Cloud Storage. If unsure what type of information is appropriate, please contact the ICT Department or the DPO.

Telephones (Desk phones, Mobiles & Smart devices)

11.3 The following activities are prohibited:

a) The use of Organisation resources by an Officer to make private calls, without authorisation. Where authorisation has been obtained, each Officer should keep a record of the private calls they make. Periodic and regular collections should be made. Where an itemised telephone bill is available, the actual cost of each private call per the bill (plus VAT) should be recharged to the relevant Officer. Officers should check the details of the itemised bills against their own records of private calls. Where itemised bills are not available, charges based upon the appropriate tariff should be applied.

b) The use of corporate smart devices (i.e. Smart Phones and Tablets) for personal use without explicit consent. Where the use of mobile data is concerned, the

Officer agrees to calculate the usage at the normal tariff for the day and time of use and repay the Organisation. This is to be equitable between Officer and to ensure that it is the Organisation, and not Officers who use the mobile telephone for private purposes, who benefit from contracted data usage that is associated with the Organisation-owned device.

c) A limit of Mobile data may be imposed by the Organisation.

d) The use of a supplied device with mobile data capabilities for tethering or as a data hotspot without consent by an appropriate People Manager and notification to the ICT Department.

e) The use of a mobile phone or smart device for the sharing of personal or confidential information. Alternative, more secure channels should be used.

f) The use of personal devices to make and receive calls during working hours of service provision is not explicitly prohibited but where possible, these calls should be made during an Officers rest breaks.

g) The use of non-corporate systems for the transition and storage of data pertaining to Organisational operation or containing sensitive/personal data on Mobile devices

Desk and workstations

11.4 The Organisation has a clear desk policy in place. Information should not be left on desk or workstations either within the place of work or at home when unattended and should be removed from view if left unsupervised.

Internet Access

11.6 Access to the following categories of websites is strictly prohibited and technically controlled:

- Illegal
- Pornographic
- Violence
- Hate and discrimination.
- Offensive
- Weapons
- Hacking
- Web chat
- Gambling
- Dating

- Games
- Webmail

11.6.1 Should an Officer require access to a resource which is currently prohibited, access will be reviewed on an individual basis subject to the receipt of a signed business case.

11.6.2 Except where it is strictly and necessarily required for work, for example ICT audit activity or other investigation, Officers must not:

a) Create, download, upload, display, or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
b) Subscribe to, enter, or use peer-to-peer networks or install software that allows sharing of music, video, or image files.
c) Subscribe to, enter, or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
d) Subscribe to, enter, or use online gaming or betting sites.
e) Subscribe to or enter "money making" sites or enter or use "money making" programs. Run a private business.
f) Download any software that does not comply with the System Acquisition, Development and Deployment Policy.
g) Attempt to bypass the Organisation's Proxy system.

The above list gives examples of "*unsuitable*" usage but is 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 Organisation policies.

12 Destroying Information

12.1 The printing of information is discouraged, however where this is a necessity, 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 retain hard copies of information outside of office locations, unless there is a business requirement.

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

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

12.5 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

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

13 Password Management

Password Creation

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

Password Construction Guidelines

13.2 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 Officers, 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

13.3 The following guidelines must be always adhered to:

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 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

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

1.1.1 Default passwords must also be changed immediately. If an Officer 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.

1.1.2 Officers must not reuse the same password within 20 password changes.

13.4.3 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 Officer will be required to change it to be following the Password Construction Guidelines.

14 Anti-Virus Protection

14.1 All ICT equipment will have the latest Anti-Virus signature and Windows Update files when connected to the network. Officers 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.

15 Security Updates

15.1 ICT regularly push security, operating system, and application updates to corporate provided end user devices. It is therefore essential that Officers connect their corporate provided laptops to the corporate network at least once a week to enable their device to obtain the updates. Connections should be maintained for 3 hours.

15.2 Officers must “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.

15.3 Officers must ensure that any Apple based products check and apply updates as soon as they become available.

16 Remote Working

Officer's Responsibility

16.1 It is the responsibility of an Officer to ensure that the following points are always adhered to.

16.2 All Officers must comply with appropriate codes and policies associated with the use of ICT equipment.

16.3 All Officers must comply with the Acceptable Usage Policy – this document.

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

16.5 Officers must ensure that access / authentication tokens and personal identification numbers are kept in a separate location to the portable computer device at all times. All removable media devices and paper documentation must also not be stored with the portable computer device.

16.6 Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g., secure filing cabinets) when not in use. Wastepaper containing personal or confidential information must be shredded to required standards.

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

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

16.9 All Officers 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.

16.10 All Officers have a responsibility to promptly report the theft, loss, or unauthorized access of the Organisation's equipment in accordance with the ICT Incident Management Procedure section of this document and the Data Protection Policy.

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

16.12 Officers will not install any software on to an Organisation owned portable computer device without the prior agreement from ICT.

16.13 Officers will not change the configuration of any Organisation owned portable computer device. Officers will not install any hardware on to or inside any Organisation owned portable computer device, unless authorised by an Officer of the ICT Department.

16.14 Officers will allow the installation and maintenance of Anti-Virus updates immediately.

16.15 Officers will allow the installation of software patches and updates immediately.

16.16 Officers 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.

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

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

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

16.20 Officers must not deliberately remove or deface any asset registration number.

16.21 All requests for upgrades of hardware or software must be approved by an authorised individual. Equipment and software will then be purchased and installed by an Officer of the ICT Department.

16.22 No family members may use the ICT equipment. The ICT equipment is supplied for the Officers sole use in order to undertake their work activities.

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

16.24 Officers 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. ICT will seek approval from Service Managers and the DPO prior to agreeing this action.

16.25 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 Officers must co-operate fully with any such audit.

16.26 Removable media devices must not be stored with the portable computer device.

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

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

16.29 Officers 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.

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

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

16.32 It is the responsibility of the Organisation's Officers 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.

16.33 All ICT equipment (including portable computer devices) supplied to users to facilitate remote working is the property of the Organisation. It must be returned upon the request.

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

16.35 Remote or home working should be in line with the Organisation's Flexible or Agile Working Policy and in agreement with the manager.

16.36 Agreement should be reached between the manager and colleague as to:

- how the colleague will record their time worked (for example, maintain a timesheet for submission to their manager weekly)
- the frequency of contact required between them – on the phone and in person.

- the nature of the contact – management visits, 121's, Team meeting participation etc.
- how often the colleague will be required to attend the office (ideally this should be at least weekly)
- arrangements for attendance at team meetings, staff briefings, etc.

16.37 All homeworking arrangements are subject to being removed or amended due to business need or in circumstances where the colleague is not performing to the required standard, without the colleagues' prior consent.

17 Remote Working Access Controls

17.1 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.

17.2 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.

17.3 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.

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

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

17.6 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.

17.7 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.

18 Incident Management Procedure

18.1 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.

18.2 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.

18.3 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

18.4 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 Department to gain as much information as possible from the business users to identify if an incident is occurring.

18.4.1 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).

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

Suspicious Activity on ICT equipment

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

18.5.1 If an ICT event is detected users **must**:

- Note the symptoms and any error messages on screen.
- Disconnect the workstation from the network if an infection is suspected (with assistance from ICT Support Staff).
- Not use any removable media (for example USB memory sticks) that may also have been infected.

Violation of Controls/Measures

18.6 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

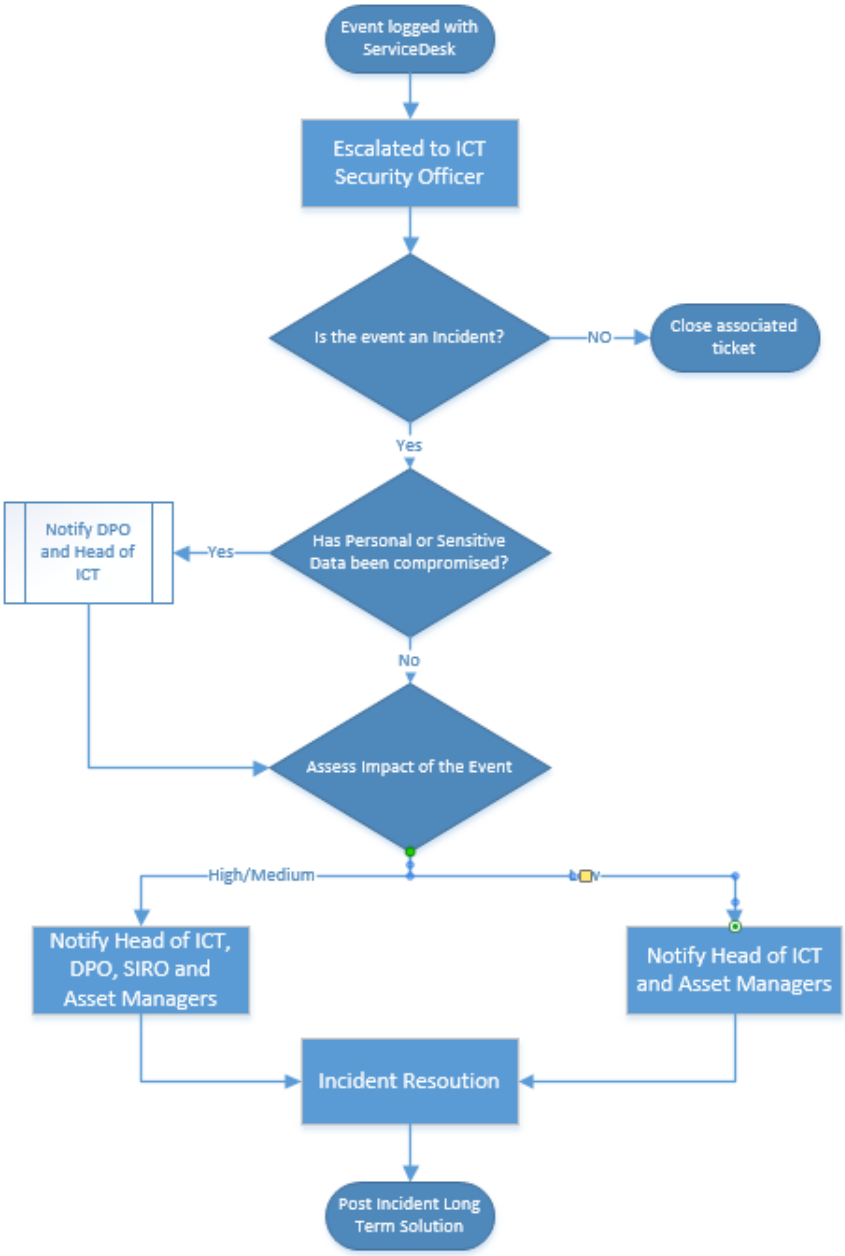
Lost or Stolen ICT Equipment

18.7 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.

18.7.1 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.

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

19 Security Event Process Flow



20. Review

20.1 As general guidance, 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.

21. Policy Compliance

21.1 Should any Officer be found to have breached this policy; the issue will be reviewed by Senior Management and Disciplinary Policies may be enacted.

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

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

22. Related Policies & Principles

Audit & Forensic Computing Principle

Data Protection Policy

Audit & Forensic Computing Principle

Systems Acquisition and Development Policy

Starters & Leavers Procedure

Code of Conduct

Disciplinary Policy

Local Authority Constitution

The Seven Principles of Public Life