PSPS
Public Sector Partnership Services Ltd

Delivering services for South Holland District Council, Boston Borough Council, East Lindsey District Council

Appendix A

Information Security Policy Employee/Members Access

May 2021

Document Control

Version Control

Issue Number	Issue Author	Issue Date	Reason for Issue
1.0	J Wright	Oct-18	Review and 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

Approval Control

Issue Number	Approval Authority	Name	Approval Date	Due for Review
3.1	ELDC/BBC	James Gilbert	May-21	May-24
	PSPS	Lewis Ducket	May-21	May-24
3.2	SHDC	James Gilbert		May-24

Contents

1. Policy Aim

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 staff and 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 of the Organisation's data.

It will also provide employees and Members with clear guidance in the acceptable and appropriate use of the Organisation's ICT equipment and services.

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	Employees/Members

2. Introduction

This is a joint Employee/Members Access Policy. 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.

The Organisation's intentions for publishing this Employee/Members Access Policy is not to impose restrictions that are contrary to the Organisation's established culture of openness, trust and integrity. However, we are committed to protecting the Organisation and its employees and partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

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 confidentiality, integrity and availability (CIA) of their critical client data and their computing resources.

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.

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

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

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.

The procedures accompanying this policy are split into 3 key stages of a Employee'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.

This policy also applies to third party access to Organisation's information systems (e.g. contractors, service providers, voluntary agencies and partners) in addition to the Third Party Access Policy.

This policy applies to Councillors, employees, contractors, consultants, temporaries, and other workers at the Organisation, including all personnel affiliated with third parties (contractors, service providers and partners).

This Employee/Members Access Policy forms part of the Information Security Framework.

Access to the Organisation's Information systems can be revoked if it is found users have not reviewed and accepted the relevant Information Security Framework policies within 1 month of this policy being released for review.

3. Roles and Responsibilities

The following roles are those formally defined within the Policy:

Role	Responsibility
The Organisation's Chief Executive	Supporting Company/Authority compliance with the policy
Senior Management 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 members, and advising on it.
All Staff/Members	Understanding and complying with the policy.

4. Definition

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**:

- Be suitable for their roles
- 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.

5. Officers Policy Statement

Every user must be aware of, and understand, the following policies:

Information Security Framework Overview

Employee Access Policy

ICT Incident Management Procedure

Systems Acquisition, Development and Deployment Policy

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

5.1 Starters & Leavers – Line Manager Responsibility

5.1.1 Prior to Employment

The Organisation must ensure that potential users are recruited in line with the Organisation's Recruitment and Selection Policy for the roles they are considered for and to reduce the risk of theft, fraud or misuse of information or information systems by those users.

5.1.2 Role and Responsibilities

Decisions on the appropriate level of access to information or information systems for a particular user are the responsibility of the appropriate Service Manager.

Line managers are responsible for ensuring that creation of new users, changes in role, and termination of users are notified to the HR/ICT Section as soon as practicabley possible, using an agreed process.

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

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:
- Information Security Framework Overview
- ICT Employee & Member Access Policy
- ICT Incident Management Procedure
- Systems Acquisition, Development and Deployment Policy

Access to the Organisation's Information systems can be revoked if it is found users have not reviewed and accepted the relevant Information Security Framework policies within 1 month of this policy being released for review.

5.1.3 User Screening

Background verification checks must be carried out on all potential employee users, 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.

The basic requirements for Organisation employment must be:

- Minimum of two satisfactory references.
- Completeness and accuracy check of employee's application form.
- Confirmation of claimed academic and professional qualifications.
- Identity check against a passport or equivalent document that contains a photograph.

Users who require access to secured systems, such as Revenue's and Benefits, **must** be cleared to "Baseline Personnel Security Standard". The following requirements **must** be met:

- Minimum of 2 satisfactory references.
- Completeness and accuracy check of employee's application form.
- Confirmation of claimed academic and professional qualifications.
- Identity check against a passport or equivalent document that contains a photograph. Identity must be proven through visibility of:
    - A full 10 year passport.
- Or two from the following list:
    - British driving licence.
    - P45 form.
    - Birth certificate.
    - Proof of residence – i.e. council tax or utility bill.
- Verification of full employment history for the past 3 years.
- Verification of nationality and immigration status.
- Verification of criminal record (unspent convictions only).

DBS checks on the user,for specific roles, must be carried out to an appropriate level as demanded by law.

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

All the above requirements for verification checks must also be applied to technical support and temporary staff that have access to those systems or any copies of the contents of those systems (e.g. backup tapes, printouts, test data-sets).

5.1.4 **Terms and Conditions of Employment**

As part of their contractual obligation employees must agree and sign the terms of their employment contract.

Each employee 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.

5.1.5 **During Employment**

5.1.5.1 During Continued Employment

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.

It is also necessary that user changes 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.

5.1.5.2 Management Responsibilities

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

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

Any changes to user access must be made as soon as practicabley possible, and be clearly communicated to the user.

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

5.1.5.3 Information Security Awareness, Education and Training

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

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

5.1.6 **Job Role Changes & Leavers**

5.1.6.1 Secure Termination of Employment

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 practicabley possible, when no longer required by the user.

5.1.6.2 Termination Responsibilities

Line managers must notify the HR/ICT Section as soon as practicabley possible, of the impending termination or suspension of employment so that their access can be suspended.

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

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

5.1.6.3 Return of Assets

Line Managers must 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.

5.1.6.4 Removal of Access Rights

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

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.

5.2 General Use and Ownership

5.2.1 Information stored on electronic and computing devices remains the sole property of the Organisation. Employees must ensure through legal or technical means that information is protected and should have an understanding of their responsibilities under the statutory legislation.

5.2.2 Employees 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.

5.2.3 Employees 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.

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

5.2.5 Employees have a responsibility to report any suspected or confirmed ICT Security events in accordance with the ICT Incident Management Procedure.

5.2.6 Connecting to cloud based services that hold corporate information should only be conducted from a corporate device, for example MS365

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

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

5.2.9 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.

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

5.2.11 The Organisation retains the right to use a performance/productivity monitoring system to monitor and report on the ICT usage within the Organisation. Use of such a system will undergo required DPIA and DPO approval.

5.3 Security and Information

5.3.1 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.

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

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

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

5.3.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders.

5.3.6 Employees must exercise caution with the transmittal of data and must not transmit by email or any other method, any file which they know to be infected with a virus, malware etc.

5.3.7 Employees must not download data or programs of any nature from unknown sources.

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

5.3.9 Employees must not forward virus warnings other than to the ICT Service Desk.

5.3.10 Employees must report any suspected files to the ICT Service Desk.

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

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

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

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

5.4 Email and Communications

5.4.1 All use of email must be consistent with the Organisation's values and ethos of ethical conduct, safety, compliance with applicable laws and proper business practices.

5.4.2 The Organisation's/individual email accounts 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.

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

5.4.4 All data contained within an email message or an attachment must be secured according to the current company standard.

5.4.5 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.

5.4.6 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.

5.4.7 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.

5.4.8 Organisation employees shall have no expectation of privacy in anything they store, send or receive on the Organisation's email system.

5.4.9 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.

5.4.10 Email must not be considered to 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.

5.4.11 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 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 are being abused by a user, they should contact the ICT Service Desk.

5.4.12 Access to another employee's email is strictly forbidden unless the employee has given their 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 employee's email account must be absolutely necessary and has to be carried out with regard to the rights and freedom of the employee. Managers must only open emails which they believe to be relevant.

5.4.13 It should be noted that email and attachments may need to be disclosed in accordance with the ICT Audit & Forensic Computing Policy.

5.4.14 There may be instances where a user will receive unsolicited mass junk email or spam. It is recommended that users 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.

5.4.15 When away from the Office or otherwise unable to respond to emails for an extended period, users should use the 'Out of Office' function to ensure that the person initiating an email is aware that the email will not be actioned for some time or given an alternative contact point.

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

5.4.17 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.

5.4.18 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.

5.4.19 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.

5.4.20 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.

5.4.21 The Organisation supplies desk and/or mobile phones for business purposes. Devices should be used in accordance with this policy.

5.5 Internet & Social Media

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

5.5.2 At the discretion of an Employees line manager, and provided it does not interfere with their work, the Organisation permits appropriate personal use of the Internet in an Emplotees own time (for example during their lunch-break or before or after work).

5.5.3 When using Organisation resources to access and use the Internet, users must realise they represent the Organisation. Whenever

employees state an affiliation to the Organisation, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the Organisation".

5.5.4 Employees 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. Employees 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.

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

5.5.6 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.

5.5.7 All personal usage must be in accordance with this policy. Employees 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.

5.5.8 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.

5.5.9 Employee access to Social Media for work purposes is with the explicit consent of an Employees line manager and will be reviewed on an individual basis.

5.5.10 Employee access to Social Media for personal use is with explicit consent of their line manager, and provided it does not interfere with their work. Such requests will be reviewed on an individual basis.

5.6 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities by a member of the Senior Management Team.

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

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

Any unacceptable use of ICT systems/services will be subject to the Organisation's Disciplinary Policy.

5.6.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

5.6.1.1 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.

5.6.1.2 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.

5.6.1.3 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.

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

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

5.6.1.6 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.

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

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

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

5.6.1.10 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee 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.

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

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

5.6.1.13 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.

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

5.6.1.15 Providing information about, or lists of, the Organisation's employees to parties outside of the Organisation.

5.6.2 **Email Activities**

The following activities are strictly prohibited, with no exceptions:

5.6.2.1 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).

5.6.2.2 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. Employees who receive any emails with this content from any employee should report the matter immediately.

5.6.2.3 Unauthorised use of email header information.

5.6.2.4 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.

5.6.2.5 Automatically forwarding email to a third party email system. Individual messages which are forwarded by the user must not contain confidential or personal information.

5.6.2.6 Non-work email accounts must not be used to conduct or support official Organisation business. Employees 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. All emails that represent aspects of official business or administrative arrangements are the property of the Organisation and not of any individual employee.

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

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

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

5.6.3 **Cloud Storage**

5.6.3.1 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.

5.6.3.2 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.

5.6.3.3 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 Employee of its arrival, always enquire if unsure.

5.6.3.4 Please do not transfer Official-Sensitive information via Cloud Storage. If an Employee is unsure what type of information is appropriate please contact the ICT Department or the DPO.

5.6.4 **Telephones (Desk phones, Mobiles & Smart devices)**

The following activities are prohibited:

5.6.4.1 The use of Organisation resources by Employees to make private calls, without authorisation. Where authorisation has been obtained, each employee 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 employee. Employees 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.

5.6.4.2 The use of Smart devices (i.e. Smart Phones and Tablets) for personal use without explicit consent. Where the use of Mobile data is concerned, the employee agrees to calculate the usage at the normal tariff for the day and time of use and repay the Organisation. This is in order to be equitable between employees and to ensure that it is the Organisation, and not employees who use the mobile telephone for private purposes, who benefit from contracted data usage that is associated with the Organisation-owned device.

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

5.6.4.4 The use of a supplied device with mobile data capabilities for tethering or as a data hotspot without consent by an appropriate Line Manager.

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

5.6.4.6 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 employee's rest breaks.

5.6.4.7 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

5.6.5 Desk and workstations

5.6.5.1 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.

5.6.6 Internet Access

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

Should an Employee 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.

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

5.6.6.1 Create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.

5.6.6.2 Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files

5.6.6.3 Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.

5.6.6.4 Subscribe to, enter or use online gaming or betting sites.

5.6.6.5 Subscribe to or enter “money making” sites or enter or use “money making” programs. Run a private business.

5.6.6.6 Download any software that does not comply with the System Acquisition, Development and Deployment Policy.

5.6.6.7 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.

5.6.7 Social Media

The use of Social Media by employees, 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.

5.6.7.1 Employees shall not engage in any Social Media that may harm or tarnish the image, reputation and/or goodwill of the Organisation and/or any of its employees.

5.6.7.2 Employees 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.

5.6.7.3 Employees may also not attribute personal statements, opinions or beliefs to the Organisation when engaged in Social Media. If an employee is expressing his or her beliefs and/or opinions, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the Organisation. Employees assume any and all risk associated with Social Media.

5.7 Password Management

5.7.1 Password Creation

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

5.7.1.2 Users must not use the same password for Organisation system access as for other personal access (for example, personal ISP account, internet shopping, bank and so on).

5.7.2 Password Construction Guidelines

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. imgladmypasswordisagoodone
- 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 number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

5.7.3 Protecting Passwords

The following guidelines must be adhered to at all times:

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

5.7.3.2 Do not share passwords with anyone, including assistants, secretaries, managers, co-workers while on planned absence from work.

5.7.3.3 Never use the 'remember password' function.

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

5.7.3.5 Passwords must not be inserted into email messages

5.7.3.6 Passwords must not be revealed over the phone to anyone

5.7.3.7 Never store passwords in a computer system without encryption.

5.7.3.8 Do not use any part of a username within a password.

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

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

5.7.4 Changing Passwords

5.7.4.1 All user-level passwords must be changed at a maximum of every 90 days, or whenever a system prompts a change.

5.7.4.2 Default passwords must also be changed immediately. If an Employee become aware, or suspect, that their password has become known to someone else, they must change it immediately and report their concern to the ICT Service Desk.

5.7.4.3 Users must not reuse the same password within 20 password changes.

5.7.4.4 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 user will be required to change it to be in compliance with the Password Construction Guidelines.

5.7.5 System Administration Standards

All Organisation ICT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users - i.e. no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.
- All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed at least every 90 days.

6. Members Policy Statement

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

Information Security Framework Overview

Employee & Members Access Policy

ICT Incident Management Procedure

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

6.1 New & Departing Members - Member Services Responsibility

6.1.1 General Role and Responsibilities

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

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 user is aware of, and understands, the following Council policies:
- Information Security Framework Overview
- ICT Employee & Member Access Policy
- ICT Incident Management Procedure

Access to the Organisation's Information systems can be revoked if it is found Members have not reviewed and accepted the relevant Information Security Framework policies within 1 month of this policy being released for review.

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 in the course of their Council work, and to reduce the risk of human error. It is the responsibility of all Members to inform ICT should they have any concerns relating to security or permissions.

6.1.1.1 Information Security Awareness, Education and Training

All Members will receive information security awareness training at the beginning of their 4 year term and as deemed necessary during this period.

6.1.2 **Departing Members**

It is to be ensured that access to Organisational information assets is removed as soon as practicabley possible, when no longer required by the Member.

Member Services must notify the HR/ICT Section as soon as practicabley 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.

6.1.2.1 Return of Assets

Unless otherwise agreed, Member Services must ensure that Member return all of the organisation's assets in their possession ceasation of their elective period. This must include any copies of information that is not in the Public domain.

6.2 General Use and Ownership

6.2.1 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 have an understanding of their responsibilities under the statutory legislation.

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

6.2.3 Members 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.

6.2.4 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.

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

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

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

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

6.3 Security and Information

6.3.1 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.

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

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

6.3.4 Members must use extreme caution when opening e-mail attachments received from unknown senders.

6.3.5 Members must exercise caution with the transmittal of data and must not transmit by email or any other method, any file which they know to be infected with a virus, malware etc.

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

6.3.7 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.

6.3.8 Members must not forward virus warnings other than to the ICT Service Desk.

6.3.9 Members must report any suspected files to the ICT Service Desk.

6.3.10 It is 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.

6.4 Email and Communications

6.4.1 All use of email must be consistent with the Organisation's values and ethos of ethical conduct, safety, compliance with applicable laws and proper business practices.

6.4.2 The Organisation's/individual email accounts should be used primarily for Council/Ward purposes; personal communication is permitted on a appropriate basis, but non-Organisation's related commercial uses are prohibited.

6.4.3 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.

6.4.4 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.

6.4.5 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.

6.4.6 Members shall have no expectation of privacy in anything they store, send or receive on the Organisation's email system.

6.4.7 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.

6.4.8 Email must not be considered to 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.

6.4.9 Whilst respecting the privacy of out Members users, the Organisation maintains its legal right, in accordance with current legal and regulatory requirements to monitor and audit the use of email 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.

6.4.10 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 given on the submission of an ICT Service Request submitted by Chief Executive. Access to a Members email account must be absolutely necessary and has to be carried out with regard to the rights and freedom of the Member.

6.4.11 It should be noted that email and attachments may need to be disclosed in accordance with the ICT Audit & Forensic Computing Policy.

6.4.12 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.

6.4.13 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.

6.4.14 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.

6.4.15 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.

6.4.16 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.

6.4.17 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.

6.5 Internet & Social Media

6.5.1 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.

6.5.2 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.

6.5.3 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.

6.6 Unacceptable Use

The following activities are, in general, prohibited.

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.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

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

6.6.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

6.6.1.1 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.

6.6.1.2 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.

6.6.1.3 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.

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

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

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

6.6.1.7 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.

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

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

6.6.2 **Email Activities**

The following activities are strictly prohibited, with no exceptions:

6.6.2.1 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).

6.6.2.2 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.

6.6.2.3 Unauthorised use of email header information.

6.6.2.4 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.

6.6.2.5 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.

6.6.2.6 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.

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

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

6.6.3 **Cloud Storage (Excluding Microsoft 365)**

6.6.3.1 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.

6.6.3.2 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.

6.6.3.3 Please do not transfer Official-Sensitive information via Cloud Storage. If a Member isunsure what type of information is appropriate please contact the ICT Department or the DPO.

6.6.4 **Mobile Data**

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

6.6.4.1 All members should seek to use WiFi as their primary data transition method, where this is not achievable, mobie data may be used.

6.6.4.2 A Organisational data bundle is in use to support the provision of mobile data. This is a shared bundle where high users are offset by lower use users. Beyond this allowed data usage, a per GB price if in place. To ensure the Organisation does not incur significant overuse expense, it reserves the right to monitor and limit the use of Mobile data.

6.6.5 **Internet Access**

Access to the following categories of websites is strictly prohibited and when using the Corporate network, technically controlled:

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

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 deemed illegal, obscene or offensive.

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.

6.6.6 **Social Media**

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.

6.6.6.1 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.

6.6.6.2 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.

6.7 Password Management

6.7.1 Password Creation

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

6.7.1.2 Members must not use the same password for Organisation system access as for other personal access (for example, personal ISP account, internet shopping, bank and so on).

6.7.2 Password Construction Guidelines

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. imgladmypasswordisagoodone
- 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 number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

6.7.3 **Protecting Passwords**

The following guidelines must be adhered to at all times:

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

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

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

6.7.3.4 Passwords must not be inserted into email messages

6.7.3.5 Passwords must not be revealed over the phone to anyone

6.7.3.6 Never store your passwords in a computer system without encryption.

6.7.3.7 Do not use any part of a username within a password.

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

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

6.7.4 **Changing Passwords**

6.7.4.1 All user-level passwords must be changed at a maximum of every 90 days, or whenever a system prompts it to be changed.

6.7.4.2 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.

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

6.7.4.4 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 in compliance with the Password Construction Guidelines.

7 Review

As a standard principle, this policy should be reviewed at least once every two 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.

8 Policy Compliance

If any Officer is found to have breached this policy, they will be subject to the Organisation's disciplinary procedure.

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

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

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

9 Related Policies

Information Security Framework Overview

Audit & Forensic Computing Policy

Data Protection Policy

Breach Management Procedure

ICT Incident Management Procedure

Audit Policy

Password Management Policy

Systems Acquisition and Development Policy

Starters & Leavers Procedure

Code of Conduct

Disciplinary Policy

Local Authority Constitution