London Borough of Redbridge

Information Security Policy Framework

Ambitious for Redbridge

Classification: NOT PROTECTIVELY MARKED

Date: December 2017

Version: 5.0

Owner: Information Governance Board

Note:

Be aware that any printed copies of this document may not be the most recent version. So please check on the Intranet to ensure that you are using the current version before relying on the information and policies contained within it.

Version	Date Reviewed	Summary of Changes	Updated by	Approved by	Date Published	Published to
1.0	4.02.09	Final version	Michael Bishop		4.02.09	LBR
2.00	15 January 2013	Revision to reflect IGB ownership and requirements around manual data	Tim Rodgers	Information Governance Board		
3.0	15th January 2014	IGB approved version	Tim Rodgers	Information Governance Board	19th February 2014	
3.1	9th April 2014	Draft for IGB	Tim Rodgers	Information Governance Board	9th May 2014	Intranet
4.0	March 2015	Changes to Information Classification Policy	Antoinette Carter		Draft	
4.0	October 2016	Revamp to update branding and make this a more user oriented document and incorporate a clear information security policy remove less user relevant policies and add the password policy and reference to the BYOD policy to be added later	Lesley Holmes			
4.0	November 2016		Lesley Holmes	Information Governance Board	29/11/2016	Intranet
4.1	January 2017	Minor Changes to wording of Mobile Working	Lesley Holmes	Information Governance Board	17/01/2016	Intranet

		Confidentiality Statement				
5.0	December 2017	Changes to include the new GDPR mandates. Remove all references to GCSx as that has now been retired Other minor additions / deletions	Mary Umoh/ Aysha Mukhtar	Information Governance Board 19/01/2018	07/02/2018	Intranet

This Framework will be reviewed within six months of its initial implementation and at least annually thereafter. The review body will be the Information Governance Board.

NOTE in relation to this framework:

For the Purposes of Approval the framework is presented with all the policies appended. On Publication the policies will be separated and presented individually for ease of access and understanding.

The document control panel shown above will be replicated at the commencement of each of the policies to ensure that the approvals are clearly shown.

The roles and responsibilities and compliance statements will not be repeated within each policy but a statement referring back to the framework will be included.

CONTENTS

1 Information Security Policy Framework

1.1 Purpose

Like the Data Protection Act 1998, the GDPR (GDPR) places an obligation on organisations to comply with the principle of implementing appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. In fact, the GDPR goes further and prescribes (under article 32) how organisations must implement the security of processing of personal data appropriate to the risk.

The overarching Information Security Policy Framework sets out how the Council will protect personal information and manage the risks associated with loss, unauthorised change, or unauthorised disclosure of information. The Framework comprises a series of policies that guide and govern how information is protected, accessed and managed for the purposes that the Council has collected or produced it.

The policies included in this framework are as follows:

- Information Security Policy
- Acceptable Use Policy
- Password Policy
- Information Classification Policy
- Remote Access Policy
- Bring Your Own Device Policy

1.2 Scope

The term 'users' will be used throughout this policy framework to refer to all employees, council members, contractors, third party employees, agency workers, temporary staff, and partner organisation staff. It also includes school-based staff where the Board of Governors has adopted the policy framework.

This policy framework applies to all users who handle information belonging to the Council regardless of their work location i.e. in the office, at home, remote or mobile working.

The policy framework also applies to all equipment issued by, or containing information owned by the Council. It includes computers (including virtual machines as well as physical), laptops, tablets, ipads, smart phones and removable storage media such as CDs, DVDs, memory cards and USB drives. Also included within the scope of this framework is information stored on the Council's servers and IT infrastructure, and that held by third party suppliers of physical and electronic storage services.

It applies to all information stored, transmitted or shared. It therefore includes information held electronically, on paper, or other physical media which is shared electronically, physically, orally or visually e.g. email, on paper, in a photograph, by telephone, presentation and/or video conferencing, etc. (This list is not exhaustive)

1.3 Statement

The information held by the Council is an extremely valuable asset. Good Information Security is essential in protecting this asset from all threats whether internal or external,

accidental or deliberate. This policy framework defines the way in which information must be handled and shared.

This policy framework aims to:

- Ensure information handling practices comply with Council policies and the law;
- Protect the Council's information by preventing misuse, damage or loss; and
- Protect information and systems against unauthorised access.

All physical assets issued to a user remain the property of the Council at all times, and **must** be returned when the user reaches the end of their contractual obligations.

It is the line manager's responsibility to ensure that all physical assets are returned to the Council so that they can be returned to IT to be re-assigned to colleagues in the same department.

1.4 Responsibilities

Responsible	Senior Information Risk Owner (SIRO) The SIRO is responsible for ensuring organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist.
Accountable	The Chief Executive has ultimate accountability and authority for the policy.
Conscience	The Caldicott Guardian is the "conscience" of the Council, providing a focal point for service user and patient information sharing issues and advising on the options for lawful and ethical processing of information as required, within the People Directorate.
The Information Governance Manager	The Information Governance Manager is responsible for ensuring that the Council complies with the Data Protection Act 1998, Freedom of Information Act 2000 and the Environmental Information Regulations 2004, by drafting and disseminating of the Information Governance policies and guidance. The IG Manager shall ensure that Information Governance training and awareness is provided and provide advice to the SIRO, IAO's, and all staff and agency workers on all types of Information Governance and Management issues.
Consulted	Information Governance Board - It is the responsibility of the Information Governance Board to ensure that: • This policy is well publicised, updated and remains relevant; • If users cannot access the intranet, provision is made to distribute the policy and any updates through their appropriate reporting structure; and • Users are able to meet the obligations and responsibilities set

	out in this policy.
Members	Members should understand and apply the policy in their day-to-day activities; • Are aware of any changes to the policy; and • Understand how to report breaches as set out in sections below
Information Risk Management	Information Asset Owners (IAO) are senior individuals (Operational Directors for People and Place and Heads of Service for Resources and Strategy) IAOs are responsible for understanding and addressing risks to personal data/information assets they "own" and provide assurance to the SIRO on the security and use of these assets. Information Asset Managers (IAM) are responsible for supporting the Information Asset owners in the delivery of their role. The information Asset Manager will be responsible for the information assets within a defined scope (usually a service delivery area) and will fulfil the requirements.
Operational	Managers have basic responsibility for the manner in which personal data is used or processed within their department or areas of responsibility and must liaise with the Information Governance Manager in all aspects of data protection. It is a manager's responsibility to have a good working knowledge of Information security and the Data Protection Act and the relevant Codes of Practice. Managers should also ensure that their staff are aware of the Data Protection policy and the act. All Council employees, agency workers, contractors and consultants, staff members of partner organisations (who have been permitted access to the Council's information- Understand and apply the policy in their day-to-day activities; • Are aware of any changes to the policy; and • Understand how to report breaches as set out in sections below.
Communicated	Via the Intranet, staff newsletter, training, briefings

1.5 Monitoring for Compliance

At any time and without prior notice, the Council maintains the right and ability to examine any equipment and systems. These examinations will be used to ensure compliance with internal policies and the law, to support any internal investigations and assist in the management of information assets.

In order to ensure compliance with this policy, the Council employs monitoring software and specifically reserves the right for authorised personnel to analyse this monitoring information.

1.6 Policy Non Compliance

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in an inability to provide necessary services to the public, a huge fine from the Information Commissioners Office, enforcement action taken against the Council or individuals and reputational damage to the Council.

Users found to be in breach of this policy (e.g. recklessly handling personal data) will be subject to the Council's disciplinary procedures. If a criminal offence has been committed, further action will be taken to assist in the prosecution of users involved.

1.7 Policy Awareness

A lack of awareness of a new or updated policy cannot be used to defend liability in the event of an information security breach. This policy takes precedence over any local procedures.

This Policy will be periodically communicated to staff using the MetaCompliance online policy acceptance system, and be available on both the intranet and the Council's website.

1.8 Security Incidents

Users **must** report incidents or any concerns about information security at the earliest opportunity to the service desk through the Information Security Incident Reporting Procedure

If this is not appropriate then breaches should be escalated by:

- Contacting the appropriate Head of Department; or by contacting the Head of HR or Head of Audit under the Council's Whistleblowing Policy.
- Council Members **must** report breaches of information security to the Head of Legal and Constitutional Services

1.9 Authority to Grant Access to Information

If a breach occurs, then the power to authorise accessing information needed to support any investigation has been delegated to the:

- Head of HR for employees;
- Secretary to the Leader of the Council for Members; and
- Head of Legal and Constitutional Services.

1.10 The policies within this framework should be read in conjunction with

- Social Media Policy
- Information Security Incident Reporting Procedure

- Data Protection Policy
- Information Risk Management Policy
- Data Quality Policy
- Guidance on Handling Classified Information
- Remote Working Guidelines
- Secure Email Guidance
- Records Management Policy
- IT Operational Security Policy Framework (where technical security is involved)
- Confidential Waste Procedures

2 Information Security Policy

This Policy forms part of the Information Security Framework and should be read in conjunction with that document. The Framework sets out the overarching roles and responsibilities relating to this policy and the compliance requirements.

2.1 Introduction

Information stored and processed by the council or by third parties working on behalf of the council is a valuable asset. Without adequate levels of protection, confidentiality, integrity and availability of information, the council will not be able to fulfil its obligations including the provision of government services and meeting legal, statutory and contractual requirements.

The council's information is in many forms including:

- Hardcopy documents on paper and sent by fax
- Electronic information stored on computers, remote servers, mobile devices, tapes, microfilm, CDs, external disks and USB portable storage devices
- Verbal information (face to face conversations and over the telephone)

We are committed to preserving the confidentiality, integrity and availability of the information assets within the jurisdiction of the Council for the purposes of:

- sound decision making
- delivering quality services to our customers
- compliance with the law
- meeting the expectations of our customers and citizens
- protecting our reputation as a professional and trustworthy organisation
- safeguarding against fraudulent activity.

This policy is part of a suite of information governance policies. It sets out the council's commitment to information security and provides the guidelines and frameworks for ensuring all forms of information, supporting systems and networks are protected from security threats such as malicious software, unauthorised access, computer misuse, information technology failures, human error and physical security threats.

The Head of IT Operations has overall responsibility for the security of Information Assets within the jurisdiction of the council, but it is the responsibility of **all** employees and agents of the council to comply with this policy.

This policy and all other artefacts related to it will be governed and maintained by the Council's Information Governance Board (IGB). Please see the Terms of Reference for IGB for further information. This can be found on the Information Governance page on the Intranet.

2.2 Purpose

The purpose of this policy is to protect all information assets within the control of the Council from all threats whether internal or external, deliberate or accidental. The policy sets out the controls and requirements that will protect a wide range of information that is generated, shared, maintained and ultimately destroyed or archived.

The purpose of security in an information system or process is to preserve an appropriate level of:

- **Confidentiality:** to prevent unauthorised disclosure of information
- **Integrity**: to prevent the unauthorised amendment or deletion and maintain integrity of information
- **Availability**: to prevent unauthorised withholding of information or resources and ensure information is available as and when legitimately required
- **Resilience**: to ensure that information is accessible when it is needed

2.3 Scope

This policy applies to all information assets held by the council irrespective of their format and covers all locations into which London Borough of Redbridge information is taken and/or accessed from.

The scope of this policy extends to users as defined in the Information Security Policy Framework

2.4 Legal Framework

The council must comply with all relevant statutory UK and European Union legislation, including:

- Human Rights Act 1998
- Data Protection Act 1998 and the successive legislation when replaced
- General Data Protection Regulations 2016 (GDPR 2016)
- Freedom Information Act 2000
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Environmental Information Regulations 2004
- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2012
- Health and Safety at Work Act 1974
- Telecommunications (Lawful Business Practice) Regulations 2000
- Protection of Freedoms Act 2012
- Waste Electrical and Electronic Equipment (WEEE) Directive
- Re-use of Public Sector Information Regulations 2005

The requirement to comply with this legislation extends to everyone who can be held personally accountable for any breaches of information security for which the Council is responsible.

2.5 Home working/Remote/ Mobile working

All home working and remote/mobile working must be carried out in compliance with the Remote Working Guidelines and Remote Access Policy

All users working outside of the Council's office locations **must** sign the mobile working confidentiality agreement prior to being given access to the network using a virtual private network or virtual machine accessed from non LBRC equipment

Line Managers are responsible for ensuring that the Mobile Working Confidentiality Statement has been signed when granting permission for remote working.

As part of the issue of laptops or hybrid tablets IT will ensure that staff have signed the mobile working confidentiality agreement.

2.6 Procurement of services

When procuring services all users must ensure that:

- GDPR and Information Governance requirements are clearly specified within the conditions of contract and service specification for all relevant procured services.
- Privacy by Design and Default is mandated and incorporated across all stages of the life cycle development of the service. This mandates the completion of a Privacy Impact Assessment from the onset for any service provision.
- the council's conditions of contract relating to General Data Protection regulation, freedom of information etc. are included in all relevant procurement information.
- the pre-qualification/evaluation of prospective suppliers includes where appropriate consideration of capability for providing sufficient guarantees with compliance with GDPR.
- due regard is given to GDPR as part of contract monitoring and management.
- the implications of sub-contracting are considered and ensure that the above requirements are passed through the relevant supply chain, with specific considerations for the mandates of the GDPR
- third parties have adequate and demonstrable controls in place with regards to offsite/ remote storage of council information.

2.7 Disposals

Users must ensure compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive and ensure that sensitive data is not accidentally released. The disposal of any IT equipment **must** be carried out by IT.

When disposing of any personal, sensitive and/or confidential information staff must do so in accordance with the council's corporate confidential waste disposal procedures.

If working at home staff must comply with the above disposal methods which ensure secure methods such as cross-cut shredding. If no secure disposals methods are available, sensitive information must be transported to your normal working area for secure disposal.

It is important to keep the waste in a secure place until it can be collected for secure disposal. **Never put sensitive and confidential waste in any normal waste bins.**

2.8 Systems and Software

All information systems which are to be used for storing and processing council information must be formally authorised by IT. This includes cloud based systems that are

accessed via the internet, which must satisfy the cloud security principles published by the National Cyber Security Centre.

Information Asset Owners (IAOs) are responsible for ensuring that Privacy Impact Assessments are completed for all new systems and information handling processes.
They must also ensure that all new systems comply with the Privacy by Design and Default mandate.

User access to systems must be adequately controlled using complex passwords and appropriate access rights. User access rights must be regularly reviewed to ensure they are still appropriate.

Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is strictly forbidden.

User Responsibilities

All persons with IT access (users) **must** undergo the council's Information Security and Data Protection elearning packages.

Users must use a unique username and password for accessing the council's network and information systems.

Users are responsible for keeping their passwords confidential at all times, and must not disclose passwords to anyone, including their line managers. Written down passwords are not permitted Weak passwords must not be used. See the Password Policy for more information about password strength

Users must not attempt to access systems or records within systems which they have not been formally authorised to access.

Users must not bypass, disable or subvert system security controls.

Users shall ensure that unauthorised persons are not able to view council information on portable devices and shall protect access by locking computers when unattended. This Policy also applies to staff accessing council information on their own devices.

Users must ensure they do not leave portable media such as CDs that contains personal or sensitive information in drives.

All users must inform their manager if they detect, suspect or witness an incident which may be a breach of security and notify the IT Service Desk through the Information Security Incident Management Procedure.

All users must be aware that the network is monitored. IT Service Desk will monitor day to day access to ensure adequate protection against security threats, and where necessary, will collect evidence of misuse and unauthorised activity.

Manager's Responsibilities

Managers shall ensure that the Council's elearning packages or briefings for Information Security and Data Protection are part of a new employees' induction.

Managers shall ensure that all users complete refresher training for Information Security and Data Protection on an annual basis in the first quarter of the financial year.

Managers must ensure that when any staff member leaves the Authority, all council equipment (including their ID card) is returned. The IT Service Desk must be informed of all leavers immediately to ensure network access is revoked.

Portable hardware including laptops, mobile devices & tablets

Unauthorised equipment must not be connected to the council's network. The exception being personal devices connecting to the council's 'guest' wireless system.

Equipment taken off site must be locked away and kept out of sight when left unattended. USB ports are restricted and only permit the use of IT approved and encrypted devices. Active scanning will automatically check all media plugged into USB ports to ensure compliance with USB port restrictions.

Equipment left on site overnight e.g. laptops or tablets should be securely stored in a locker or locked cupboard, in accordance with the Clear Desk Standard.

2.9 Information Handling

Building Security

All facilities that hold or process information must have suitable physical security. This includes, but is not limited to:

- **ALL** staff, contractors, agency workers or other persons having access to the Council's information assets must wear their ID badge clearly displayed at all times whilst on Council premises
- Visitors to office facilities must be escorted at all times while in data processing areas See the guidance about notifying visitors on the intranet.
- Visitor reception and pass procedures must be followed
- Computer Data Centres will have controlled access and logs recording access
- IT communications equipment must be enclosed in secure locked cabinets if in general office areas

Users also need to familiarise themselves with the Clear Desk Standards

Storage

Everyone must ensure that information is not put at risk of damage or theft, and is stored securely and access allowed only to those who need it for legitimate purposes and in accordance with the General Data Protection Regulation For example Records must be stored in secure buildings with access controls to the building, specific floors and individual offices.

The location of any stored records must be sited to avoid unauthorised access, damage, theft and interference. Stored records must not be removed or moved to another location

without notification being given to the relevant Information Asset Owner or Records Co-ordinator.

Electronic information needs to be stored on the council network unless alternative storage (e.g. Cloud) is authorised by IT.

Users shall not under any circumstances download or store sensitive Council Information (including sensitive personal and personal data) on any non-Council device or facility (e.g. personal cloud).

Communication

Extra care must be taken when printing sensitive information or sending/receiving faxes. When sending sensitive information a test fax must be sent prior to sending the information or phone the organisation first to let them know what is being sent.

Secure "Follow Me" printing should be used in all cases and printing should only be done where it is necessary.

Voicemail may contain personal and sensitive information and therefore passwords must be kept secure

Records Management

Records are a key resource for the effective operation and accountability of the council. It is also recognised that some records will over time become of historical value and need to be identified and preserved accordingly. The Records Management Policy gives more detail about the Council's approach to records management

Removable media

To prevent data loss, the use of USB devices (e.g. portable hard drives, memory sticks) and removable media (e.g. CDs, DVDs, memory sticks etc.) on the council's PCs **must not** be used to store personal and sensitive information unless there is a business requirement to do so.

Users must only use mobile media to transfer personal and sensitive council information if there is a business requirement to do so and there is no other more secure means available e.g. Egress

Only media purchased through the councils IT service and with a sufficient level of encryption, may be used to temporarily hold and transfer personal and sensitive Council information.

2.10 Information Sharing

Information shall only be shared within the Council and with other organisations in line with the law, where there is a need or obligation to do so, and where possible consent has been given.

Where there is a need to enable service delivery through partnership with external organisations the information sharing will be governed either under the terms of a contract or an information sharing or information access /disclosure agreement.

Users are advised to refer to the Council's Information Sharing guidelines for more information.

2.11 Information Security Incidents

Any loss or risk of loss of sensitive and confidential information, either actual or suspected, must be reported immediately without undue delay (within 48 hours of becoming aware of the incident), to the IT Service Desk using the Information Security Incident Management Procedure. The Information Governance Manager will provide oversight and advice for this process.

2.12 Information Asset Register

An Information Asset Register will be maintained by Information Asset Owners (and managers) of all the Council's major information assets, including those required for the Council to meet its statutory obligations. Oversight and moderation of the Register will be provided by the Information Governance Manager.

The Information Asset Register will define the ownership and classification (according to sensitivity) of each information asset. This process will be carried out in accordance with the Council's agreed Information Classification Policy.

3 Acceptable Use Policy

This Policy forms part of the Information Security Framework and should be read in conjunction with that document. The Framework sets out the overarching roles and responsibilities relating to this policy and the compliance requirements.

3.1 Introduction

This policy has been developed to clearly state the expectations of the Council in respect of all persons using equipment, facilities and information belonging to the Council and its citizen's which is processed using that equipment or facility

This policy covers the use of:

- Equipment (including but not limited to computers, laptops, tablets and smartphones
- Internet
- Email

A separate policy covers the use of social media

3.2 Purpose

The Council has introduced this Acceptable Use Policy to encourage safe data handling, minimise the risk of information security breaches, and meet security requirements relating to the use of the Public Services Network and other compliance standards (E.g. Payment Card Industry Data Security Standard (PCI DSS)).

3.3 Scope

The Council requires that **any user** of Council information **must** agree and adhere to this Acceptable Use Policy before being granted data access. It includes any process, whether electronic, computer or a manual facility used to access information.

The scope of this policy extends to users as defined in the Information Security Policy Framework

3.4 Statement

Failure to adhere to the Acceptable Use Policy will result in appropriate disciplinary action in line with the Council's Disciplinary procedures. The Council requires users to accept that:

- This policy applies no matter your work location i.e. in the office, at home, remote or mobile working.

- You **are** aware that improper use of any Council information can result in either you and/or the Council incurring civil or criminal liability so the Council reserves the right to report any illegal activities to the appropriate authorities.

3.5 Controlling Access

To ensure only authorised users can access the Council information and systems:

- You **must not** use a colleague's user name and password (credentials) to gain access to any information or system.

- You **must not** attempt to access any information or system that you have not been given explicit permission to access.

- You **must not** share your credentials or use them to log another person into the network even if you are asked to by your line manager. (If you are asked to do this then you should report the request via the Council's whistleblowing procedure)

- You **must** notify the loss of your credentials or where a third party gains access to your password, by reporting this to your management structure.

- You **must** notify the IT Service Desk to disable your account as soon as you become aware of any unauthorised access using your credentials.

- You **must** lock your computer screen when away from your desk using the keyboard locking mechanism in order to protect on-screen information.

- A clear desk standard is in place to protect sensitive or protectively marked paper based or digital information e.g. DVDs or USB devices.

In addition, your:

- Personally owned computer equipment **must not** be connected to the Council's data network except where this has been expressly authorised and is compliant with the Bring Your Own Device Policy requirements.

3.6 Information Sharing

Information should only be shared where there is a business need to do so and this should be in accordance with the Information Sharing guidance available on the intranet.

3.7 Conduct

As a user of the Council's information and information systems, you are expected to act in a professional and responsible manner and therefore you **must not**:

- Attempt to make changes to information or information systems where you have no explicit permission or authorisation to do so, or where the change could be construed as fraudulent or illegal. This includes installing or attempting to re-configure any software, or delegating such a change to another user.

- Make statements on your own behalf or on behalf of the Council, by using any of the Council's communication channels, which are or may be defamatory, bring the Council into disrepute or imply that you are acting on behalf of the Council when you have no authority to do so.

- Knowingly carry out action(s) that will degrade or deny access to information to other users that includes installing software not authorised by IT.

- Use Council systems to breach, or attempt to breach, any legislation. These include Protection of the Children Act; the Obscene Publications Act; GDPR; Freedom of

Information Act; Intellectual Property Legislation; Copyright Legislation; and the Computer Misuse Act.

- Place Council information at risk by handling it in an insecure manner within and outside of Council premises.

3.8 Email Usage

Email is an effective business tool for communicating with colleagues and service users, suppliers etc. inside and outside the Council.

Email is not always a secure means of communication. Care must be taken when sending confidential or sensitive emails containing personal data.
All emails sent or received from the Council's systems are the property of the Council.
All messages will be unpacked and scanned for viruses as they arrive or leave the Council.

Users of Council Email **shall**:

- Except for 'Not Protectively Marked' classified emails clearly indicate the sensitivity of their message content in the subject line of all email to indicate to the recipient how you expect them to handle the information
- Except where consent is given by the data subject send confidential, personal or sensitive personal information to external email addresses (e.g. supplier's or provider's, Hotmail, yahoo, gmail, msn) by encrypted email using Egress.
- Use the delegation functionality in email to grant or withdraw access.
- Use the blind copy (BCC) functionality when sending out group emails to external personal email addresses.
- Use "Private" calendar appointments where the subject of meeting indicates confidentiality is of concern
- Treat email as permanent written records which may be read by persons other than the addressee and store these in appropriate network locations in a structured manner according to their retention schedule
- Review their Email mailbox regularly and delete unnecessary messages
- Treat unsolicited Emails from unknown sources with suspicion
- Treat both emails and attachments in the same way, where corporate decisions or advice are being given or discussed.

Users of Council Email **shall not**:

- Send Council information to your own personal email address especially where this includes sensitive personal information of a service user
- Download Council information to non-Council devices or personally controlled cloud storage.
- Set up automatic forwarding of email rules to external email accounts

- Transmit PIN (personal identify numbers) or PAN (personal account numbers) used in credit card transactions via email or any other messaging systems unless appropriately encrypted.
- Send outbound email from generic email accounts set up to receive incoming email only
- Forward "chain" or joke emails to others
- Rename email attachments or password protect attachments to evade malicious software scanning.
- Seek to gain access to another users mailbox without either their consent or the written approval of their line manager

Where you are replying to messages from internet email accounts, take care to remove personal data from the correspondence chain where appropriate. The onus is on the Council to protect data in transit.

3.9 Personal use of Email

Users may use the corporate Email system for personal use, provided such use does not breach the officer's code of conduct and/or the Council's constitution.

Permitted personal use **must not** impact on your day-to-day work.

3.10 Confidentiality

In order to maintain confidentiality

- Do not forward to an external party any information that may compromise the Information Classification Policy, or the rights of a service user or third party in relation to their confidentiality

- Where you have received email inadvertently, notify the sender that you have received the message in error and then delete any copies of misdirected message. If the email contains sensitive or personal information notify the IT service desk that information has been disclosed in error using the Information Security Incident Reporting Procedure

3.11 Monitoring

The Council automatically monitors all Internet usage so you are responsible for all Internet sites accessed under your login as this information is recorded for compliance purposes.

3.12 Standard of Use

You **must**:

- Ensure all Internet access is carried out under your login account only;

- Ensure that Internet access is for the purpose of your contractual obligations and that you do not either misrepresent your level of authority in these regards.

3.13 General Usage Guidance

3.13.1 Removable Media

All removable media **must** be approved before use on the Council's computer systems and network. If you require clarification then contact the IT Service Desk (x.84455). This is to prevent data loss, and to stop the Council's computer systems being infected with malware e.g. viruses and key loggers.

The Council will not be liable for damage to personal items that are connected to its equipment E.g mobile phones being charged through USB ports.

If you are in possession of unencrypted portable media holding personal data, please contact the IT Service Desk to arrange its collection and disposal

3.13.2 Desktop / Laptop computers

Desktop/Laptop computers **must not** be used to store any data, including protectively marked or personal, sensitive data files. Data stored on the hard disk (or C: drive, or 'My Computer' folder) are not backed up, and are at risk of loss, theft, or damage by viruses or other malicious software such as spyware. Files stored on the hard disk or C: drive can also be viewed by anyone using that computer.

You **must not** store any non-work related (i.e. not for Council business) files, personally owned software or pictures on Council owned computers or shared folders.

You **must not** store any non-work related video clips, pictures, graphics such as JPEG files, music files such as MP3 files, games, screen savers or desktop wallpapers on the home drives (H: drive or 'My Documents' folder), laptops or any other storage media such as USB devices issued by the Council.

This includes any similar files that may be downloaded from the Internet or personally owned.

It is Council policy to monitor electronic file storage usage, and to remove any software or files deemed inappropriate or pose a risk to the Councils information systems, break copyright legislation, or are not for work purposes.

3.13.3 Cloud storage

Staff **are not** permitted to host Council data with free cloud storage providers such as . Dropbox, Google Drive, iCloud or other free cloud storage providers.

Should cloud storage be required, a business case including a completed Privacy Impact Assessment should be submitted to the Senior Information Risk Owner (via the Information Governance Manager). For more information please see the Information Risk Management Policy available on the intranet.

3.14 Remote or Mobile Working

Remote or mobile working requires a higher degree of care as the risk to information is greater. ALL users must accept the remote/ mobile working confidentiality statement to show that they have understood the risks.

3.15 Foreign Travel

Users who need to take information abroad for contractual obligations e.g. to be contactable for a major project or incident, **must** obtain permission to do so, including:

- Ensuring there is appropriate equipment insurance cover by contacting the Council's Insurance team (Finance)`;
- Contacting the Information Governance Manager if taking any information outside of the EU or information classified as OFFICIAL or above to the EU.

3.16 Lost or Stolen Assets

If Council information is lost or stolen in the UK or abroad, due to a burglary or street robbery, you **must** report this to IT Service Desk, so that it is logged as lost or stolen.

The Information Governance Manager **must** be notified of losses if data stored on the device is of a personal, sensitive nature i.e. classified as OFFICIAL or higher. Or data has been lost in addition to that stored on the device

3.17 Return of Council Assets

All users, issued with computer equipment **must** return all assets upon termination of their employment, contract or agreement. This includes any removable storage media, laptops, mobile phones, tablets, software, computers, printers and any other computer equipment for home or mobile working.

Managers shall ensure that their staff return all equipment as part of the exit procedures, and notify IT so that their accounts are closed. All equipment shall be returned to IT for reallocation.

4 Password Policy

4.1 Introduction

This Password Policy conforms to the security requirements of the Public Services Network (PSN) Code of Connection. The following points define the password arrangements and provide help and guidance on ensuring good information security.

4.2 Scope

The scope of this policy extends to users as defined in the Information Security Policy Framework

4.3 Password Requirements

- Your password must be a minimum of 8 characters long, containing an upper case letter, a lower case letter and a least one digit and / or special character (e.g. $, *,!).
- Your password **must not** be based on dictionary words, family names, your name or login account, sports teams, telephone numbers or memorable dates, as these are easy to guess and subsequently cracked.
- Do not use the word 'Password' in any form.
- Do not use passwords with consecutive identical digits or lower/uppercase characters e.g. AAA, aaa, or 111.
- Do not use the same password for business as you would for non-business use.
- Do not write down your password with your login name and leave it on display.
- Do not disclose your password to anyone else.
- You will be prompted to change your password every 90 days.
- The new password that you choose must be different from the last 24 passwords that you have used.
- You will be given five opportunities to input your password every time you access the Council's network. On the fifth failed attempt your account will be locked, and can only be unlocked by contacting the IT Service Desk.
- You will be given five opportunities to input your password every time you access the Council's network. On the fifth failed attempt your account will be locked, and can unlocked using the password self service facility or by contacting the IT Service Desk.
- The use of the Password Self Service is mandatory for all staff. This must form part of the induction for new starters.

Should your password become known, change your password immediately using password self-service and contact the IT Service Desk, ext. 84455, to report the incident.

5 Information Classification Policy

This Policy forms part of the Information Security Framework and should be read in conjunction with that document. The Framework sets out the overarching roles and responsibilities relating to this policy and the compliance requirements.

5.1 Purpose

The purpose of this policy is to reduce the risk of an information security breach, or a breach of the GDPR , by setting out appropriate methods of protectively marking and handling Council owned information. This is to ensure public confidence is maintained in the Council's ability to handle their personal information.

The scheme is adopted from the Government Security Classifications Scheme which came into force in 2014

5.2 Scope

The information covered in this policy cover relates to any Council information stored, shared or transmitted via any means and by any user.

The scope of this policy extends to users as defined in the Information Security Policy Framework

5.3 Statement

Information Classification is used to manage the Risk associated with the loss, unauthorised change to, or unauthorised sharing of information. The Council has decided to adopt the Government Security Classification Scheme

Protectively marked information received from other organisations **must** be treated in accordance with those organisations' information handling procedures.

To achieve the aims of this policy:

- All Council information **should** have a Classification and an owner
- All Council Information that is in a document or record **should** be clearly marked with its Classification in its header and or footer

5.4 What is Information Classification?

Information Classification is used to manage the risk associated with the loss of (availability), damage to, (integrity) and inappropriate disclosure (confidentiality) of information.

- **Availability -** is the requirement that information is available when it is needed, and can be accessed by those who require it, to complete a task or provide a contractual service.

- **Integrity -** Integrity is the confidence that information is authentic and complete

- **Confidentiality -** is the requirement that information is only shared with people who need to know.

5.5 The Government Security Classification Scheme

Introduced in April 2014 this is the standard that is being applied to all Government produced documentation. It is not mandatory for Local Authorities to adhere to this standard, however it is prudent to do so as it helps people to understand the level of care that they need to take when dealing with different types of information. It also provides consistency with the marking schemes used by other government and public sector organisations.

The table below gives examples of the different classifications and the types of information that would fall into them.

Not Protectively Marked	May be viewed by anyone, anywhere in the world. E.G. Information that could be put on the website.
Official	Available to Council employees, members, contractors and partners that need access to the information but not to others. It is likely to contain personal information e.g. name and address, telephone number, date of birth.
Official Sensitive **(contains sensitive personal /commercial information)**	Available only to specified Council employees, contractors and partners with appropriate authorisation. E.G. social care case files, tender documentation partner / framework agreements, major tenders.
Secret **(ONLY USED FOR INFORMATION RELATING TO NATIONAL SECURITY)**	Access is controlled and restricted to a small number of people.

5.6 Guidelines

All users who create a new information asset e.g. a report, policy document, procedure, spreadsheet, or database, **must** ensure the information asset is classified in line with the Information Classification policy. This includes electronic and paper records, and information shared orally or visually e.g. presentations.

5.7 Previous Council Scheme

- There is no expectation that information with an existing protective marking will be reclassified. Therefore the existing classification scheme will remain valid in relation to existing documents.

Classification	Explanation	Examples
NOT PROTECTIVELY MARKED	Can be publicly shared.	Policies and procedures Blank templates
PROTECT	**Must not** be shared unless there are reciprocal agreements in place (Impact Level 2, HMG InfoSec Standard); or: • If personal information, i.e. information, which falls under the "Personal Sensitive Data" as, defined by the Data Protection Act 1998 or its successor, **must not** be shared unless reciprocal information sharing agreements are in place (Impact Level 2, HMG InfoSec Standard). • Limited sharing - there may be limited sensitivity in sharing it depending on additional protective marking (IL 1).	List of staff contact details
RESTRICTED	Must not be shared unless there is reciprocal information sharing agreements in place.	Child protection document. Details of a crime prosecution

5.8 Common rules for both schemes

- Only the owner or an appropriately authorised individual can change the information classification.

- Information marked at the RESTRICTED, PROTECT, OFFICIAL, OFFICIAL-SENSITIVE level should be sent through EGRESS When sharing with non-government contacts e.g. *.co.uk, *.com or *.net.

- Information specifically intended for external publication should not be marked.

5.9 Information Asset Management

A Corporate Information Asset register **must** be maintained and appropriate sections must be regularly reviewed by each Service Area.

The register **must** additionally list the owner, the classification of the information and where it is stored.

6 Remote Access Policy

6.1 Purpose

This policy aims to reduce the inherent risk of remote access to the Council's information.

6.2 Scope

This policy applies to all forms of remote access to the Council's network. This includes, but is not limited to, remote access:

- Using Council issued equipment;
- Using personal computing equipment, where permitted;
- Using public computing equipment; and
- By third parties under contractual obligations.

The scope of this policy extends to users as defined in the Information Security Policy Framework

6.3 Statement

An individual remotely accessing the Council's Network **must** be authorised by their Head of Department to do so. All remote access users **must** adhere to the Council's:

- Information Security Policy
- Acceptable Use Policy
- Remote Working Guidelines
- Bring Your Own Device Policy (if applicable)

All individual's accessing the Council's network from a remote location must also accept the Mobile Working Confidentiality Statement (Appendix A) whenever this is presented to them automatically by the Council's policy management system.

6.4 Guidelines

The Council's *"Password Policy"* describes the standard for user set passwords.

Once the remote connection to the Council has been established, any equipment providing or accessing this connection **must not** be left unattended.

Access to the PSN services is not possible from abroad or from an unmanaged device

Due to the indeterminate nature of and security issues associated with, internet connections in foreign counties, you must contact the IT Service Desk to seek advice if there is a need for you to access the corporate network from abroad.

Under the PCI DSS requirements, remote access for third party users must incur via multi factor authentication technology i.e. username and password.

6.5 Laptops to be connected to the network at least once every 30 days

All assigned users of Council owned laptops **must** connect their laptop to the Council network at least once in every 30 day period. This ensures that software is updated to the latest version and virus prevention updates are applied. This in turn ensures that Council information is maintained in a safe and secure state.

Mobile Working confidentiality statement

Name: **Department:**
Address:

I understand that in the course of my duties I may have access to personal and other confidential information relating to residents, clients, colleagues and the Council's partners and contractors. When I am working outside the office environment I understand that I need to take extra care of that information.

I undertake to make sure that any equipment or documentation that I have is secured (preferably in a locked cupboard) when it is in my home and not in use.

I undertake to make sure that any equipment or documentation is not left in my car (or other vehicle, including vehicles belonging to LBR) overnight, and during the day is securely locked in the boot or other secure space where it is concealed.

I undertake to make sure that any information that I have access to, is not exposed to people who do not need to see it, including my family, friends and other visitors to my home. I further undertake to make sure that if I am working in a client's home or a public place that any information that I am using is not exposed to people who do not need to see it.

I undertake to report any breaches of information immediately using the Information Security Incident notification form available on the intranet.

Employee Statement

I also acknowledge that if I breach this confidentiality, I may be liable for formal disciplinary action taken against me. I acknowledge that in addition, I may be subject to criminal prosecution under either the Data Protection Act or Computer Misuse Act or a civil prosecution for damages by the supplier of the information.

Agency Worker / Consultant/ Contractor Statement

I also acknowledge that if I breach this confidentiality, I may be liable for a claim against my professional indemnity and termination of my contract. I acknowledge that in addition, I may be subject to criminal prosecution under either the Data Protection Act or Computer Misuse Act or a civil prosecution for damages by the supplier of the information.

DECLARATION

I, _____

(Name in block capitals)

confirm that I have read the above confidentiality statement, understand it, and agree to abide by it.

Right Click on the X to sign electronically

X

Employee / Agency Worker/ Consultant/ Contra...

X

Manager