Ealing Council

Information Security and Data Management Policy

Classification: Unclassified
Date created: November 2018
Date reviewed: July 2023
Version: 1.8
Author: Lorraine Cox, corporate information governance manager
Owner: Kevin Griffin, chief information security officer

Date	Change description	Author	Version
November 2018	Amendments to Acceptable Use	Lorraine Cox	1.1.1
February 2020	Review	Lorraine Cox	1.2
September 2020	Amendments	Kevin Griffin	1.3
November 2020	Amendments due to Brexit	Kevin Griffin	1.4
January 2021	Amendments for working abroad	Kevin Griffin	1.5
November 2022	Amendments for PCI/DSS offsite, amendments for Working Abroad	Kevin Griffin	1.6
May 2023	Amendments for local login	Kevin Griffin	1.7
July 2023	General review	Kevin Griffin	1.8

Review and approval

Name	Title or role	Date of Issue	Version
Emily Hill	Strategic director for resources	May 2023	1.7
Edward Axe	Director – ICT (CIO) and property services	May 2023	1.8
Peter Greenham	Head of ICT	May 2023	1.8
Lorraine Cox	Corporate information governance manager	May 2023	1.8
Kevin Griffin	Chief information security officer	May 2023	1.8

Contents

1. Policy introduction

This is a policy that covers the obligations of any user of Ealing's infrastructure, data or buildings. This policy is updated periodically, staff and all users of the network and associated services need to keep abreast of any changes.

1.1 Policy breaches

Failure to adhere to this policy will be considered a serious disciplinary offence and will be dealt with in accordance with the appropriate council disciplinary procedures. This could lead to a termination of employment for employees, termination of a contract in the case of service providers or consultants and termination of placement in the case of student placements.

Additionally, individuals may be subject to civil or criminal prosecution.

1.2 Policy compliance

To ensure compliance with this policy ad hoc reviews will be undertaken at regular intervals by ICT and data management.

1.3 Policy review

This policy will be reviewed at least annually. It will be amended in response to changes in operational and legal requirements. Every effort will be made to ensure individual users are made aware of changes when they occur, but staff have an obligation to ensure they have read and comply with the latest version. A copy will be maintained on the ICT SharePoint site.

2. Glossary and definitions

Knowledge of these definitions is important to an understanding of this policy.

User – means council officers, councillors, agency workers, consultants, and any other persons processing data on behalf of Ealing Council.

Personal data - means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing - means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special categories of data - is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data subject - means an identified or identifiable natural person.

Controller - means the natural or legal person, public authority, agency or other body

which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal Data Breach - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Information Commissioners Office (ICO) - the ICO is the UK's independent body set up to uphold information rights.

Data Protection Officer (DPO) - a statutory requirement for public authorities. The DPO is tasked with monitoring compliance with the UK GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.

Electronic communications - any transfer of signals, writings, images, sounds, data or intelligence that is, created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems.

Electronic communication systems and facilities - telecommunications equipment and systems used as a means of sending, receiving and displaying communications electronically through connected computer systems.

Electronic communication records - the content of electronic communications.

Encryption - to convert data from its original form to a form that can only be read by someone that can reverse the encryption. The purpose of encryption is to prevent unauthorized reading of the data.

WAP - the open international standard for applications that use wireless communication. Its principal application is to enable access to the internet from a mobile phone or PDA.

3. Roles and responsibilities

Chief executive

The chief executive has overall responsibility for all matters of security within the council. This responsibility is delegated to the following:

Strategic leadership team – is responsible for ensuring that:

- mechanisms are in place to comply with all legislative and regulatory requirements in respect of information and data security
- they endorse this and all supporting Information and data management policies
- their endorsement is communicated to all users of the council's information and data assets

Director – ICT (CIO) and property services – is responsible for:

- identifying and managing all security risks to business activities performed under their management. They must ensure that the appropriate corporate information and data management and security policies, standards,

procedures, guidelines and mechanisms are complied with in the performance of those activities. The responsibility for all matters of security is delegated to the Director – ICT (CIO) and property services

- the physical and environmental security of the council's property portfolio where information, data and information systems reside

The CIO or CISO - chairs the Corporate Data Governance Board and is responsible for:

- providing regular update reports to the Strategic leadership team and the
- ensuring that the corporate board and cabinet approve all corporate information and data management policies
- developing a consolidated Information and Data Management and ICT Strategy that actively promotes compliance with the International Security Standard ISO 27001
- an Information and Data Management Policy Framework is developed to support ISO 27001
- the development, production and communication of standards, procedures and guidelines to support the implementation of this and all supporting information and data management policies
- the on-going review of the effectiveness of this and all supporting information and Data Management policies
- the implementation of the appropriate technical and operational controls to protect the services, technical platforms and communications infrastructure that transport information ensuring alignment with the approved consolidated Information and Data Management and ICT Strategy and ISO 27001 Information Security standard
- advising information and data owners on the appropriate technical and operational solutions defined within the approved consolidated Information and Data Management and ICT Strategy

The chief information security officer or senior information risk owner (CISO/SIRO) is responsible for:

- ensuring all information risks are recognised and managed in the organisation through its information risk policy and assessment process
- the cyber security and monitoring of security alerts and monitoring of activity on the council's devices and network
- advising information and data owners on the appropriate technical and operational solutions defined within the approved consolidated Information and Data Management and ICT Strategy
- monitoring day-to-day compliance with this and all supporting information and Data Management policies

The director human resources and organisational development is responsible for:

- ensuring there are adequate procedures and processes in place to relating to information security
- incorporating the appropriate confidentiality agreements in contracts and terms and conditions of employment on receipt of specific requests and justifiable by departments. The corporate Code of Conduct applies to

everyone employed by the council, covers general standards of behaviour relating to people, including confidentiality, finance, contracts for work, political activity, and safety at work

- working in partnership with the ICT (CIO) and property services department, develop and deploy training to the council's workforce with regard to information security competencies
- working in collaboration with the ICT (CIO) and property services department support training initiatives on information security, data protection and freedom of information. Ensuring that that all staff have access to training in order to increase their awareness of their obligations and responsibilities with respect to standards, guidelines and procedures
- encourage management to ensure relevant security responsibilities are defined in all role profiles and that they encourage their staff to attend and complete relevant training as required

The Caldicott Guardian is responsible for:

- protecting the confidentiality information, complying with the 7 principles of the Caldicott Report and enabling appropriate information-sharing

All Personnel including but not limited to employees, councillors, MP's, NHS, Emergency Services, 3rd sector, contractors, consultants or business partners:

- must observe and comply with this policy and all supporting information security policies and the standards, procedures, guidelines and mechanisms put in place to implement these policies
- are to play an active role in protecting the information assets of the council
- must not access or operate these assets without authority and must report security breaches or exposures that have come to their attention, in line with those policies and documented procedures
- must ensure the security of their own passwords and reporting any potential compromise to the security of their user accounts

Corporate Data Governance Board (CDGB) is accountable to the Corporate Board and membership comprises a senior manager from each directorate.

The purpose of the Corporate Data Governance Board (CDGB) is to provide leadership and specialist support to ensure that the council complies with its legal responsibilities in relation to data governance, and to consider and explore potential new initiatives, opportunities and best practice in the data governance field with a view to determining whether or not they will be appropriate for implementation.

The council's CIO together with the Corporate Data Governance Board (CDGB) is responsible for reviewing and ratifying changes to this document.

4. Relevant legislations

4.1 Computer Misuse Act 1990

This Act makes it an offence for an unauthorised person to access knowingly a program or data or for a person to modify knowingly the contents of a computer. The Police and Justice Act 2006 have increased the penalties under this act.

4.2 General Data Protection Regulation (UK GDPR) and Data Protection Act 2018

Governs how personal data should be processed, by laying down 8 principles of good data handling practice. The Act gives living Individuals the right to confidentiality and security for their information and also the right to access it.

4.3 Human Rights Act 1998

There may be human rights implications to consider when investigating misuse. Inspecting or monitoring electronic communications may infringe the employee's right to respect for his or her private life (Article 8), particularly if s/he has a reasonable expectation of privacy, if the employer has given no warning that it may undertake monitoring.

4.4 Freedom of Information Act 2000

Promotes the individual's right of access to general information held by public authorities.

4.5 Common Law Duty of Confidentiality

Unless there is a statutory requirement or a public interest justification, confidential information should only be used for those purposes that the provider of the information has been informed about and has consented to, either implicitly or explicitly.

4.6 Waste Electrical and Electronic Equipment (WEEE) Directive

Promotes the 'eco-friendly' disposal of electrical goods as well as goods containing electrical components.

4.7 The Privacy and Electronic Communications (EC Directive) Regulations 2003

Defines the rules on electronic marketing.

4.8 The Public Interest Disclosures Act 1998

Known as the "the Whistle Blowers Act" protects employees who make a "Protected Disclosure".

4.9 Protection of Children Act 1978; Criminal Justice Act 1988

These Acts make it a criminal offence to distribute or possess scanned, digital or computer- generated facsimile photographs of a child under 16 that are indecent.

4.10 Sex Discrimination Act 1975, Race Relations Act 1976 and Harassment Act 1997

These Acts outlaw sex and race-based discrimination. Harassment and discrimination are unlawful, whether or not the use of work-based communications

facilities has played a role. The employer could be liable, unless it has taken steps to reduce the risk of such e-mails being distributed.

4.11 Obscene Publications Act 1959

This Act makes it a criminal offence to send material to another person which is likely to 'deprave or corrupt' the recipient (those likely to read, see or hear it). There are tighter provisions relating to the handling of child pornography, under the Criminal Justice Act 1988 and the Protection of Children Act 1978.

4.12 Defamation Act 1996

This Act exists to protect the reputation and good standing of an individual. Defamation is a false statement made by one individual about another. This statement attempts to discredit that person's character, reputation or credit worthiness. In order to be defamatory, such a statement must be communicated to at least one other person. If such a statement is spoken, then it is described as slander. However, if it is written, broadcast or shown in a film it is described as libel.

4.13 Copyright, Design and Patents Act 1988

This Act applies to digital and electronic publications as much as it does to books and other forms of writing. Where permission has not been granted, individuals and the Council could be liable to civil proceedings by the author. Also, see **Copyright, etc. and Trademarks (Offences and Enforcement) Act 2002** which increased the penalties.

4.14 Regulation of Investigatory Powers Act 2000 (RIPA)

This Act regulates the interception of communications by public or private telecommunication systems. The **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** - these regulations temper the requirements of RIPA and allow certain monitoring in the course of legitimate business practice. Therefore e-mail (and telephone) monitoring are allowed without consent for the following reasons:

- quality control monitoring
- combating crime
- combating unauthorised use of the system (for instance, investigating suspected misuse of e-mail or internet)
- determining whether the communication is business-related (this allows an employer to inspect the inbox of an employee who is absent from work, in order to check whether any business-related e-mails have come in)

All policies and their implementation will comply with the above acts as well as any relevant employment legislation and occupational health and safety regulations

5. Information security

5.1 Introduction

As the custodian of a large volume of information and data assets that includes highly sensitive and personal information, the council has a fundamental “duty of care” to protect them from unauthorised or accidental disclosure, unauthorised modification, loss, release, or damage. The main objective of information and data security is to protect information and data assets from hazards and threats, as failure to do so could result in a loss of:

- **confidentiality** – the accidental or unauthorised disclosure of information and data
- **integrity** – unauthorised modification or destruction of information and data
- **availability** – the continuity of business processes and their recoverability in the event of a major disruption

The loss of confidentiality, integrity and availability, may in turn have an adverse impact on the efficiency of the council's operations and ultimately, its reputation. Legislation, such as The UK General Data Protection Regulation and Data Protection Act 2018 and The Freedom of Information Act 2000, are also key drivers in the protection of information and data assets, which places an obligation on the council to strike a balance between the perspectives of access and openness against their confidentiality, privacy and security.

The council's strategy to ensure the safe and secure management and handling of these extremely important assets is standards based. The council aligns itself to International Standard ISO 27001 for Information Security. The development of this policy supports ISO 27001; the purpose of this high-level Information and Data Security Policy is to:

- provide management direction and support for information and data security across the council
- provide a robust, standards-based framework for securing the information and data assets owned, leased or hired by the council
- meet legislative and regulatory requirements
- clearly define the requirements for the use of information and data assets, ensuring that information assets are processed, handled and managed securely and that accountability is evident
- identify the essential safeguards and controls that need to be put in place and provide adequate resources to minimise the risk of a security breach
- ensure the continuity of the council and its services to its customers and business partners
- ensure that the principles of information and data security are consistently and effectively applied during the planning and development of council activities
- inform all people and businesses who have access to council information and data assets of their responsibilities and obligations with respect to security and safe keeping of them

5.2 Scope

This policy applies to all users of council information, data, information systems and the council's property portfolio (its physical buildings), including service providers and consultants and encompasses data, information, software, systems, paper documents and personnel (see Appendix B).

5.3 Policy statement

The council aligns itself to an ISO 27001 information and data security management framework that incorporates policies, procedures and processes to include organisational, technical and operational safeguards in order to preserve the

confidentiality, integrity and availability of its information and data assets.

The following measures have been implemented to support this policy.

Organisational security

- a consolidated information and data and ICT strategy has been developed which promotes the implementation of a standards-based approach to information and data security – ISO 27001 Information security management
- an independent review of the implementation of this policy will be undertaken periodically

Asset management

- to enable appropriate management and control, all information and data assets are inventoried, allocated an owner, classified and labelled
- to identify the threats associated with the information and data assets, the probability and impact of security failures are assessed to enable selection of the appropriate control measure

Personal security

- to reduce the risk of misuse, fraud, abuse, theft or human error by those employed by the council, over time, any additional, to this policy, security responsibilities are defined within all role profiles
- to minimise the likelihood of employing staff who may pose a risk to the security of confidential information and data and key information systems, appropriate screening and enhanced vetting procedures are undertaken in accordance with Ealing's employment policies
- appropriate security awareness and training is provided to all new starters as part of their induction. Training is also available to existing staff and users of all information and data assets and information systems
- procedures are in place to ensure the prompt removal of access rights and the return of information and data assets, information and data systems and access to buildings when an employee leaves the organisation
- staff must not share their passwords with anyone
- staff must not log in and allow anyone else to use their account
- staff must always ensure their computer is locked or log out when they are away from their desk and always log out at the end of their working day

Physical and environmental security

- appropriate physical and environmental controls have been implemented to prevent unauthorised access or damage to, loss or theft of, interference or interruption to the council's information assets
- information systems that process critical, sensitive or high availability information are located within secure areas

Use of council devices and processing data outside the UK and Northern Ireland

While the technologies ICT have successfully delivered give us massive flexibility as an organisation as to where and how we can work, this needs to be managed in line with all council policies and procedures. As of August 2021, there is not a council

policy in place to consider short term or permanent requests to work abroad covering health and safety and other HR considerations. The council's current employment contract states that our place of employment must be within reasonable travelling distance of the borough. The Guidance Note below however sets put the council's approach.

Guidance note

- the default position of the council is that staff must not work outside of the UK and NI
- IT systems and devices will no longer work, by default, outside of the UK and NI because of recent restrictions put in place to protect the council from cyber-attack by parties based overseas
- in very exceptional circumstances access may be given to work outside the UK and NI for a short period of time, no longer than 21 days. However, this exception will only be enabled if permission is sought and agreed prior to leaving the UK. Request for access is via the ICT portal
- permission must be provided from the Service Director, Director of ICT and Property Services and the Director of HR before requesting access via the ICT Portal for access enablement. Any request for access enablement without this permission will be refused
- if permission is granted to work outside the UK and NI, you should only use trusted Wi-Fi at a single address. Public Wi-Fi connections, such as in a café, is not permitted. Any equipment breakages or loss outside of the UK and NI will be charged to the department concerned

The following policy statements also apply.

- while it may be legally permissible to use any Ealing Council device **within** the European Economic Area (EEA), you must first be enabled by ICT before using any Ealing Council device inside of the EEA. The same approach described in the Guidance Note above applies
- no Ealing Council device should be used **outside** of the European Economic Area (EEA) under any circumstance. Access to the council's network will be revoked if a device is discovered being used outside of the EEA
- no Ealing Council data should be processed or stored outside of the European Economic Area (EEA) under any circumstance. Access to the council's network will be revoked if a data is discovered being processed or stored outside of the EEA

Use of cloud storage

- the use of cloud storage in Ealing Council is permitted by using Microsoft One Drive or council SharePoint sites only
- if you wish to share folders and files using online facilities, you should use Microsoft OneDrive
- it is not permitted to use any other service such as Drop Box for uploading or sharing council information without the express permission of the CISO/SIRO or CIO

Communications and operations management

- to ensure the correct and secure operation of information and data

processing systems and entry into the council's physical buildings, all procedures and processes are fully documented, reviewed and updated on an annual basis

- third-party service delivery is managed and monitored to ensure that information and data security controls are maintained
- the appropriate processes and procedures have been implemented to minimise the risk of systems failure in accordance with corporate policies
- controls have been implemented to protect the council's information and data and the infrastructure which they reside within from threats and will maintain the security council's network in accordance with this policy and operational procedures
- the handling, storage and exchange of information and the media it is held on are governed by its classification in accordance with this policy
- information and data involved in electronic commerce or that is published electronically, are governed by this Policy
- information processing activities are logged and monitored with regular reviews being undertaken in accordance with the ICT operational procedures

Access control

- access to information and data assets are managed in accordance with this policy
- guidelines that support good security practises in the selection of passwords and the use of information assets have been developed and circulated to all users
- controls have been implemented to manage and control remote access to the council's information and data assets in accordance with this policy)

Information systems acquisitions, development and maintenance

- all infrastructure, applications or services must be procured and implemented via ICT. Any infrastructure, applications or services procured outside of this process will not be allowed to be accessed on the corporate network or devices
- security requirements and controls are required to be detailed within the specifications for new information and data processing applications or enhancements to existing applications
- all applications implemented have controls governing the input, processing and output of information and data to ensure its accuracy, integrity, confidentiality, completeness and availability and importantly, its quality
- in accordance with legislative requirements the use and control of application software is governed by this policy
- procedures and controls govern the development, maintenance and support of application system software
- appropriate measures are taken to reduce the risk of exploitation of technical vulnerabilities

Information security incident management

- information security incidents, events and weaknesses are investigated and responded to in line with the corporate Information and Data Management operational procedures and this policy
- procedures and processes are documented to ensure a consistent approach is applied to the investigation of all incidents, events and weaknesses reported or discovered

Business continuity management

- a business continuity management framework is maintained in accordance with the corporate Business Continuity Management Policy. All business processes will be risk assessed to identify any threats and the possible impact they could have on the provision of services. Plans will be drawn up that detail how operations will be maintained or restored should those failures occur. Testing of plans will be undertaken on a regular basis

Compliance

- appropriate measures have been implemented that support the council's compliance with statutory and regulatory requirements relevant to information and data security
- adherence to procedures, processes and standards that support the implementation of the security polices will be reviewed periodically. Failure to comply will be considered a security breach which will be subject to an investigation and possible further action being taken
- security policies will be reviewed annually. They will be amended in response to changes in legal and operational requirements to ensure the controls remain relevant and effective
- exemption to any security policy will be stated within the policy itself, where an operational function thinks there is a justifiable reason. Policy exemptions must be requested from the council's CIO

6. Data protection

6.1 Introduction

The London borough of Ealing is committed to ensuring the privacy of the individual is respected and that all personal data that is processed by the organisation is dealt with in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other related legislation.

The UK GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data and to the free movement of personal data; it protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

All council officers and councillors need to ensure that personal data is protected and kept safe at all times. If personal data is taken from one location to another it must be done so as a necessity and not as a convenience and it must be done so in the safest possible way. We must ensure electronic equipment is fully password protected and encrypted and kept secure at all times. Files, diaries, notepads or computer equipment (that has not been screen locked) must never be left unattended.

Any queries about your data protection obligations or the rights of individuals and members of the public in relation to information about themselves should be directed to the corporate information governance team.

6.2 Purpose

The council needs to collect and use personal data about individuals, residents, customers, employees (present, past and prospective), suppliers, contractors and other businesses, in order to meet its statutory obligations and provide its services. No matter how personal data is collected or held, either manually or electronically, it must be handled and processed properly to ensure that the council meets its legal obligations.

The UK GDPR places obligations on organisations, such as the council, which process [1] personal data [2], and protects the rights and freedoms of the individuals who are subjects of that data.

The purpose of this policy is to:

- explain the council's commitment to the lawful and fair treatment of personal data and its intent to comply with the principles of UK GDPR
- ensure that all employees, elected members [3] and partners [4] are made aware of their responsibilities under UK GDPR
- ensure that all employees, elected councillors and partners are aware of the rights of data subjects [5] and ensure that those rights are protected

6.3 Scope

This policy applies to all council officers, councillors, agency workers, consultants, and other person processing data on behalf of Ealing Council", and any references shall be taken as applying to all of those people."

6.4 The council's commitment

The council, through the appropriate application of managerial and operational controls, will:

- only process personal data fairly and lawfully and in accordance with all required conditions
- specify the purpose(s) for which personal data is being used; (this is defined in the council's Privacy Notice)
- only collect the personal data that is necessary to fulfil the operational needs of any service provided or to comply with legislative or organisational requirements
- take steps to ensure the quality and integrity of personal data used
- put in place the appropriate measures to ensure that personal data is only retained for as long as it is needed for the purpose(s) it was obtained for, or to meet legal requirement
- ensure that the rights of every individual who provides the council with personal data are respected
- provide the appropriate technical and organisational security measures that will safeguard personal data against unauthorised or unlawful processing, accidental loss, destruction or damage
- ensure that personal data is not transferred outside the European

Economic Area without the appropriate safeguards

- Appoint a Data Protection Officer (DPO) who will be an independent expert in data protection to assist and advise the council in meeting its legal obligations

In addition to the above the council will endeavour, through the distribution of guidance material and training, to ensure that:

- all processing of personal data undertaken by the council is notified to the Information Commissioner's Office
- all employees managing and handling personal data are aware of and understand their responsibilities under UK GDPR and related legislation
- every individual managing and handling personal data are appropriately trained to do so
- every individual understands the purpose(s) for which they are processing personal data and also under what circumstances further processing may take place
- every individual managing and handling personal data understand the rights of the data subject
- the DPO is appointed by the council to have overall responsibility for the monitoring of data protection legislation and compliance within the council
- there is a representative within each department/service to provide a communications network to ensure compliance with UK GDPR and related legislation

6.5 The responsibilities of persons processing personal data

You are personally responsible and accountable for ensuring compliance with the principles of the UK GDPR and that your use and handling of personal data is in accordance with the purpose(s) the council have notified to the Information Commissioner. Adherence to the UK GDPR, Data Protection Act 2018 (DPA) and related legislation forms part of council's Code of Conduct and contract of employment.

Any council officers, councillors, agency workers, consultants, and other person processing data on behalf of Ealing Council who fails to carry out their duty in compliance with any of the data protection laws will be subject to disciplinary action and could also be subject to criminal prosecution.

---

1 Processing in relation to data includes obtaining, recording, holding, using or disclosing,

2 Personal data is data that relates to an identifiable living individual.

3 Elected members need to understand in what capacity they are acting under the provisions of the Act

4 A partner includes contractors, consultants, agency staff, service providers etc.

5 A data subject is an individual to whom the data relates.

Reporting a data breach

Data breaches can include loss or unintentional disclosure of personal data relating to an individual. This can be, but is not limited to, a loss of paper records containing personal data, unavailability of systems, information sent to the wrong recipient either by post or email, and a lost mobile device.

If you become aware that they or another person has caused, or may have caused, an unintentional disclosure of personal data is responsible for reporting it at soon as reasonably practicable to their line manager. This should usually be within a few minutes of discovery of the breach but should in any event be no later than the same working day.

If your line manager is not available, the breach should be reported to the Data Protection team at dataprotection@ealing.co.uk and details of the incident should be provided so that the council's data management breach process can be initiated accordingly.

The UK GDPR requires that, in the case of a breach, the council shall notify the breach to the Information Commissioner (ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of it.

New purposes of processing

All managers must ensure that any additional or new purpose for which they are processing personal data is notified to the corporate information governance manager, who will amend the council's notification as appropriate.

6.6 Individual rights

The UK GDPR gives rights to individuals in respect of personal data processed about them by the council. These rights apply to all individuals, whether they are employees, elected members, or members of the public. The UK GDPR – Chapter III confers the following rights on data subjects:

- the right of access to personal data
- the right to rectification
- the right to erasure (right to be forgotten)
- the right to restriction of processing
- obligation regarding rectification or erasure of personal data or restriction of processing
- the right to data portability
- the right to object
- the right not to be subject to automated decision-making, including profiling

6.7 Right of access

Subject to a limited number of exemptions, an individual has the right to be supplied with a copy of their personal data. This is called the subject access right and is the right that individuals are most likely to make use of. Requests can be received either in writing or verbally and the council has 30 calendar days in which to comply with a valid request.

You should be able to recognise a request when received and be aware of the procedure for handling such requests (see the Intranet). If you are instructed to

prepare a file in accordance with Article 15 of UK GDPR, you should be suitably trained and respond within the statutory time period.

6.8 The Information Commissioner's Office (ICO)

The powers of the ICO include:

- serve information notices requiring organisations to provide the ICO with specific information within a certain time period
- issue an assessment notice to permit the ICO to carry out an assessment of whether the controller or processor has complied with or is complying with the data protection legislation
- serve an enforcement notice requiring organisations to take (or refrain from taking) specific steps in order to ensure they comply with the law
- prosecute those who commit criminal offences under the DPA
- conduct audits to assess whether organisations processing, or personal data follows good practice
- report to Parliament on data protection issues of concern
- issue monetary penalties to organisations who fail to comply with the DPA

Appeals from notices are heard by the Information Tribunal, an independent body set up specifically to hear cases concerning enforcement notices or decision notices issued by the ICO.

6.9 Criminal offences

The DPA creates a number of criminal offences. Failure to comply with the requirements of the DPA could result in you being held personally liable under the DPA for your actions.

The Computer Misuse Act 1990 makes it an offence for an unauthorised person to access knowingly a program or data or for such a person to modify knowingly the contents of a computer.

The DPA also provides for separate personal liability of individual council officers or councillors where their consent, connivance or neglect has been instrumental in an offence committed by the corporate body.

You should be aware that a breach of the DPA could lead to you being the subject of a criminal prosecution and, if found guilty, you could be liable to pay a fine.

6.10 The data protection principles

There are six data protection principles that must be adhered to. The following is a summary:

1. personal data shall be processed fairly and lawfully and in a transparent manner in relation to the date subject
2. personal data collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
4. personal data shall be accurate and where necessary kept up to date;
5. personal data shall be kept in a form which permits identification of data subjects for no longer that is necessary

6. personal data shall be processed in a manner that ensures 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

The accountability principle requires the data controller shall be responsible for and be able to demonstrate compliance with the six principles above.

7. Access control and user account management

7.1 Introduction

Effective security controls in relation to access to data are an essential component of the effective risk management of the council's data resource. Access controls protect information by managing access at all entry and exit points, both logical and physical. These measures ensure that only authorised users, as determined by the council, have access to specific information, systems and facilities.

User accounts offer a way of managing access, providing user accountability and tracking their use of information, information systems and resources. User accounts can take various forms from a system login to an ID swipe card.

Therefore, the application of access controls, the management of user accounts and the monitoring of their use plays an extremely important part in the overall security of information resources.

7.2 Purpose

The purpose of this policy is to define the access controls and monitoring required by the council to fulfil its obligations.

Scope

This policy applies to all information resources, systems or facilities (existing or new) where access controls are assessed to be required. It covers the management of all accounts whether administered corporately or departmentally. It does not cover the authentication method used to ensure the identity of that user.

7.3 Statement of principles

Access controls

- access controls will be established for all major information, information systems and facilities based on their classification and security risk assessment to ensure that the appropriate level of security is implemented
- logical access controls will be implemented in accordance with this policy and the Information Security Policy. Physical access controls will be implemented in line with this policy and the Physical and Environmental Security Policy
- access to the network, information systems and servers will be achieved by the use individual user accounts (UIDS) that will require an appropriate authentication method as outlined in the Password and Authentication Policy
- access to information systems and facilities will be governed by a formally defined authorisation process covering the creation, modification, maintenance, re-enabling and deletion of accounts

- users will only be granted access to information and information systems and facilities on a “need-to-know” basis. Users will only be granted the minimum access and privileges required to perform their duties
- procedures will be implemented to ensure that access to data or information is not dependant on any one individual. Privileges granted by groups will be implemented in order to facilitate this function
- each assigned account will uniquely identify the user and must conform to the council’s naming standard (making use of the users name/surname) or an appropriate coding structure. Accounts must not give any indication of the user’s access rights. Security of systems administration accounts and passwords will be the responsibility of the technical owner of that system and must adhere to the council policies unless this is not technically possible
- a notice warning user about accessing information without authorisation will be displayed before users can gain access to any information system or facility; It should not identify any information about the information system or any other internal matters
- the council has in place appropriate systems in place to monitor the activity of users on the network and applications
- anytime it is deemed necessary, ICT reserve the right to access any machine holding council data and to take any appropriate action
- all members of staff should attend the council office at least once a month to ensure their surface is patched completely up to date, with the latest software and security patches.
- a review period, determined by the information “owner”, will be established to re-assess the access controls implemented for information, information systems and facilities; a record of the review must be maintained
- user accounts will be reviewed on a regular basis to ensure access and account privileges remain applicable to the job function or role or employment status of the user. A record of the review must be maintained
- all employees have a legal duty to keep all personal data confidential and to comply with the data protection provisions contained within the Code of Conduct for Employees
- access to information systems and facilities will be revoked for users who do not need access to perform their duties in order to ensure the confidentiality, integrity and availability of information to other users

7.4 Account management

- accounts will only be created and maintained for users that need access to information, systems and facilities to perform their official duties on behalf of the council
- user accounts will only be authorised to the capabilities appropriate to the user’s role requirements, responsibilities or specific needs to carry out a function for which they are employed. Users will only be assigned the access privileges needed to carry out their job function
- all accounts created or modified must have a documented request and the appropriate authorisation. A record must be maintained of all authorisations including the access rights and privileges granted

- procedures will be established to ensure user's access rights and privileges are adjusted in a timely manner whenever there is a change in a user's status;
- user accounts will not be activated until the authorisation process has been correctly completed. Users must not have access to information systems until all activities relating to the commencement or resumption of employment have been completed i.e. acknowledgement of Acceptable Use Policy
- generic or shared accounts will not be permitted. The only exception will apply to email accounts required by services where CIO or CISO/SIRO has granted approval
- upon notification of termination, transfer, resignation, suspension or retirement from employment received from the relevant authoritative source(s) the user account will be disabled/deactivated. Disabled accounts will be deleted after the period specified in the Access Control Standard
- each user account must be unique, only connected with the user to whom it was originally assigned. Reuse of user IDs is not permittedAll user accounts will as a minimum force the use of a password
- all default passwords for accounts must be constructed in accordance with the council's Password and Authentication Policy. All default passwords must be immediately changed by the user immediately after logging into the system if not prompted automatically to do so
- user accounts with system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by the user

7.5 Event logging, monitoring and reporting

Auditing will be implemented on all information systems to track access and record events in line with this policy.

7.6 Exceptions

Exceptions to this policy will only be granted if compliance:

- would adversely affect the ability of the service to accomplish a mission critical function
- would have an adverse impact on the service provided or supported by the information, system or resource
- cannot be achieved due the incapability of the information system or resource. A procedure for requests for exception to this policy will be produced and implemented

8. Password and authentication

8.1 Introduction

An authentication method provides a way of ensuring that the person accessing an account is the person who has been assigned the account and authorised to access the information, system or facilities.

Generally, there are three methods that can be used to authenticate a user,

consisting of something:

- you know – password, Personal Identification Number (PIN)
- you have – a token, Smartcard Personal ID card (PID)
- you are – fingerprint, iris scan, voice

A combination of these factors may be needed to ensure adequate protection, depending on the sensitivity/confidentiality of the information resource.

Therefore, the implementation of strong authentication methods (passwords, tokens, smart cards, biometrics, or other recognized forms of authentication) in conjunction with the management of user accounts is essential in the overall security of information, system and facilities.

8.2 Purpose

The purpose of this policy is to define the appropriate authentication methods needed to protect the council's information, systems and facilities from unauthorised access.

8.3 Scope

This policy applies to all information, systems or facilities (existing or proposed) where access controls requiring an authentication method are assessed to be necessary.

8.4 Statement of principles

All information, systems and facilities assessed to require access to be controlled, will be configured with appropriate controls as described in this policy

8.5 Password or PIN

To maximise the effectiveness and security of passwords the following standards will be adhered to by all information systems/applications:

- a minimum password length of 8 characters will be enforced
- a mix of upper and lower-case alpha, and numeric will be enforced

All passwords must be stored in an encrypted form; passwords must never be stored in clear text or any easily reversible form.

Default passwords for privileged accounts will be changed before the information systems or facility is implemented.

All information systems or applications will force a password change on the users first use of the system.

All information systems or applications will set passwords to expire at a pre-defined interval (currently 60 days). A warning will be issued before the expiration time. Only five "grace" logins will be allowed. If the user fails to change their password before the expiration date or during one of the grace logins the account will be locked. This applies to all user and system-level accounts.

All information systems/applications will allow passwords to be changed anytime before the expiry date has been reached.

All information systems/applications will prevent the re-use of passwords utilised by the user in the last 180 days.

All information systems will be set to lock out an account after six failed attempts to login. Where an account has been locked, it can only be unlocked or reset by the relevant system administrator in line with set corporate procedures.

Passwords will be "masked" on the display screen when they are entered to prevent

unauthorised observation. The ability to “cut and paste” within the password entry field will be disabled to prevent unauthorised recovery.

The resetting of passwords will be governed by formally documented procedures.

All users will be educated in the selection and use of passwords through issuing of guidance and an awareness campaign.

8.6 Multi-factor authentication and tokens

Multi-factor authentication (MFA) will be implemented where it has been assessed that an additional level of protection is required for information, systems or facilities.

Access to Office 365 including Outlook webmail will require MFA. All new user accounts will have MFA configured.

Tokens will be used for all client VPN services and Citrix contractor access.

Secure Envoy is the token management system that is to be used to manage the lifecycle of the tokens. A charge will be made to departments using this facility to cover license and subscription costs.

8.7 Personal identification cards (PIDs) and photographic identity in authentication systems

All PIDs will incorporate the photograph of the bearer, their first and last name and job title. The issuing PIDs will be governed by a formal authorisation process.

Personnel who forget their PIDs will be issued with a temporary PID for that day, upon proof of their status/identity. PIDs will only be valid on the day of issue.

PIDs will only be issued for the required period of time consistent with the duration of person’s employment. Where there is no expiry date PID’s will be renewed no later than two years from the date they were first issued.

Upon suspension or termination of an employment contact or contractual services the PIDs must be retrieved and deactivated.

PIDs must not be loaned to any other person.

A photograph of all staff using will be linked to their Active Directory account for the purposes of identification.

This is obligatory for all staff and contractors working for the organisation as mandated by the council’s senior leadership team.

This photograph will be synchronised to Office 365 and be able to be viewed by all staff within the council. The photograph, by default, will not be available external to the council.

8.8 Event logging monitoring and reporting

Auditing of password strength will be undertaken periodically.

Monitoring and reporting of activities and events will be implemented for all information systems and facilities.

8.9 Exceptions

Exceptions to this policy will only be granted if:

- compliance would have an adverse impact on the service provided or supported by the information, system or facility
- compliance cannot be achieved due the technical incapability of the information system or facility

In either case a risk assessment will be undertaken by the CISO/SIRO – leading to a recommendation for approval to the CIO.

9. Acceptable use

9.1 Introduction

Electronic communication plays an essential role in the conduct of the council's business, with the council's workforce making extensive use of the electronic communication systems and facilities both within the organisation and externally with other organisations and customers.

The council values every authorised user's ability to communicate with colleagues, clients, customers and business partners and has invested substantially in information and communications technology (ICT) that will enable them to work more efficiently and effectively.

An electronic address, number or account identifies, not only the user but also the council as a business organisation and as such, any activity engaged in by the user will also reflect on the council.

9.2 Purpose

This policy defines the conditions under which these systems and facilities may be used and the standards of behaviour expected of all users. It will also:

- ensure that the council's electronic communication systems and facilities are used for purposes appropriate to the council's business
- inform users of the applicable laws and policies and ensure compliance with those laws and policies
- avert disruption to and misuse of the council's electronic communications systems and facilities
- establish rules on privacy, confidentiality, and security in electronic communications

9.3 Scope

This policy applies to all:

- electronic communication systems and services owned, leased or managed by the council or provided by the council via contracts and other agreements. This includes but is not limited to:
    - internet and intranet
    - email
    - telephones (landline and mobiles (including smart devices)
    - laptops, tablets, surfaces and other mobile devices
    - voicemails
    - videophone and video conferencing

- faxes, scanners, printers and photocopiers (including multi-function devices)
- users granted authorised access to and any uses made of the council's electronic communication systems and facilities whether the user is office based or working remotely (Mobile and home working)
- electronic communication records created or received by users of those systems and services including the content of attachments and transactional information

To support this policy and to assist users in their use of the electronic communication systems and facilities stated above, good practice guidelines have been produced.

9.4 Provision and use

All users granted access to the council's communication systems and facilities are reminded that these services are provided primarily to support the provision of the council's business and services.

The council is a legal entity and as such, all correspondence including emails is considered to be legally binding. Users are responsible for the content of all text, audio and images that they transmit using any of the council's communication systems. The council reserves the right to withdraw the use of these facilities at any time.

9.5 Confidentiality and security

All users of the council's communication systems and services will from time to time be involved in the processing of confidential business information and personal data as part of the service function.

Breaches of confidentiality and privacy may occur as a result of inappropriate handling of personal data, the unintentional transmission to an 3rd parties or its unauthorised interception by unknown entities. In order to protect the confidentiality and privacy of data during transmission all users must comply with the law of confidentiality, the UK GDPR and Data Protection Act 2018 and the council Information Security and Data Protection policies.

Confidential and personal information should never be transmitted without the appropriate level of protection; consideration should be given to the nature of the content or the method of communication prior to transmission.

Any communications sent or received by means of the Public Services Network (PSN) may be intercepted or monitored. Misuse may result in disciplinary or legal action.

9.6 Statement of principles

9.6.1 Acceptable use

Use of the council's electronic communications systems and services are subject to the following conditions:

- electronic communications systems, services and facilities are provided to support the legitimate business needs and administrative requirements of the council
- electronic communications pertaining to the administrative business of the council are considered public records, whether or not the council owns the

electronic communication systems, services or facilities used to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, print, or record them, and are subject to the council's Records Management policy

- information and personal data relating to our customers and some of our business operations are confidential. All such information must only be used for the purpose(s) intended and not disclosed to any unauthorised third party (this may sometimes include other employees of the council). Confidential information and personal data should never be transmitted without appropriate protection; **Consideration must be given to the nature of the content, or the method of communication used and the appropriate standards of security must be exercised, such as encryption or a secure connection;**
- reasonable use may be made of electronic communication systems and services for **incidental personal purposes** provided that:
    - the systems are not used for private business or other commercial purposes, including the private sale or purchase of goods and services
    - use of the systems do not interfere with the normal performance of your duties and there is no breach of the prohibitions identified in this policy
- any abuse of the systems, services and facilities is reported immediately once users become aware of any taking place
- it does not violate other council policies, procedures or guidelines
- we reserve the right to automatically recharge for any costs incurred by you for your personal use
- you must report any loss of any council provided device at the earliest possibility to your manager and ICT (CIO) and property services
- employees are forbidden from transmitting council related information to their personal email address

9.6.2 Unacceptable use

Electronic communication systems and services **will not** be used to:

- take part in or aid and abet any criminal action including (but not limited to) offences under the following acts:
    - UK GDPR and Data Protection Act 2018
    - Human Rights Act 1998
    - Computer Misuse Act 1990
    - Copyright, Design and Patents Act 1998
    - the Obscene Publications Acts1959
    - Equal Opportunities law
    - Protection from Harassment Act 1997
- transmit, download, retrieve or store any messages, attachments, images or pages that contain offensive, libellous, defamatory or obscene material

including but not limited to, pornographic, racist, terrorist, anarchic, insulting and sexist material

- download store or transmit messages, images or pages that are intended to harass, intimidate, persecute, terrorise or bully other users relating to but not limited to gender, age, race, sexual orientation, religion, disability or other similar issues (including ‘jokes’)
- introduce or transmit pirated or unauthorised commercial software or deliberately spread computer viruses, worms or Trojan horses or programmes that create trap doors or sustain high volume network traffic that substantially hinders others in their use of the network, deliberately corrupt, modify or erase data or programmes intentionally interfering with the normal operation of the council's network; use the facilities in such a manner that would inhibit, distract or have a detrimental effect on council services
- introduce copyright material without the owner's permission onto the council's network
- transmit or upload personal, sensitive personal or confidential information without the appropriate safeguards, such as encryption
- overload or disable the system, services or facilities or attempt to disable or circumvent any security mechanisms intended to protect the privacy or security of the system, service or facility or any associated information, records or messages
- employ a *false identity or hide* the identity of the sender or tampering with the communications of others
- abuse the services and computer facilities in such a way that wastes resources (including employee time), denial of service, global mailings etc. not taking appropriate care in terms of limiting file sizes and maintaining archives of messages sent and received, this refers to the size that will have a detrimental impact on the performance of the network
- access, receive or transmit electronic communications to participate in or circulate inappropriate or non-business related material to others including (but not limited to) chain letters, business opportunities, jokes, electronic greeting cards, executable files, Items for sale, entertainment software, gambling or betting, financial markets, sport scores, social networking or any other bulletins that are not business related
- operate a business or participate in any pursuit geared to personal gain for themselves or an acquaintance or enter into any contractual arrangement using a council electronic identity or address as any part of a personal contract with a third party
- promote personal views that are detrimental to the council or commonly regarded public decency or participate in discussions that are politically sensitive or controversial or give advice of information that they know to be contrary to the council's policies and interests
- Microsoft Teams should not be used for the storage or sharing of personal identifiable data

Exceptions to the above will apply to employees who, as part of their job function, have to access material that may contravene the prohibited uses listed in this policy.

All such employees will need authorisation from their line managers in order to access such material.

9.7 Monitoring

An audit trail of system access, data use and other sources of staff data, such as web logs, vehicle logs, door access logs etc, shall be maintained and reviewed on a regular basis. Ealing Council will put in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy or code of conduct. The council logs all electronic activity and has an ability to monitor and analyse data for the following reasons.

- establishing the existence of facts
- investigating or detecting unauthorised use of the system
- preventing or detecting crime
- ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- in the interests of national security
- ascertaining compliance with regulatory or self-regulatory practices or procedures
- ensuring the effective operation of the system

Access to the 'raw' logs is restricted to the administrators of each system. In addition, Ealing Council collects logs to a central reporting and analysis service in support of and for the execution of the above reasons. Access to the centralised log reporting and analysis service is limited to the CIO, CISO and the council's cyber security provider. Access is specifically not given to the ICT teams, system administrators or other Ealing staff.

A non-exhaustive list of the types of data that may be collected and used is below.

- ICT authentication services (including login and logout times)
- ICT database and application access and activity logs
- all web traffic logs
- firewall and security appliance logs
- telephone, including mobile, logs
- collaboration and instant messaging software including but not limited to, Teams, Skype for Business, WhatsApp (on council devices), text messages etc
- any council data held in a cloud service.
- door access logs
- council provided vehicle movement logs and video

The council may use its monitoring of its logs and business communications to:

- provide evidence of business transactions
- ensure the accessibility of business records
- establish the existence of any facts

- ensure that the council's business procedures, policies and contracts with staff are adhered to; (this may include the verification of attendance and timesheets)
- comply with legal obligations
- track all council assets, including but not limited to vehicles, desktops, surfaces, laptops, phones, PDA/tablets, SIM cards, memory sticks, printers, scanners, and their use
- observe standards of service, staff performance and for staff training
- prevent and/or detect unauthorised use, abuse or any criminal activities taking place using the council's communication systems and services
- maintain the effective operation of the council communication systems

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act and any other applicable law. Investigation of an individuals account for audit or HR purposes is only by prior authorisation of the director of ICT and property services (CIO) and the director of HR.

The council does not actively monitor the content of electronic data as a matter of course, because it is recognised that it may constitute a breach of an individual's human rights. However, if misuse is suspected which contravenes this policy or the council deems it to represent a threat to the security of council systems, the council reserves the right to inspect the content of any data/messages without authorisation from or notification to the user or sender and/or the recipient, in line with the Lawful Business Practice Regulations and the Information Commissioner's Employment Practices Code Part 3.

10. Card payments PCI DSS

10.1 Introduction

Card payments made to Ealing Council adhere to the Payment Card Industry Data Security Standards (PCI DSS). These are standards defined to ensure that payments are secure and controlled. They are designed to reduce card fraud. Ealing Council ensures that the infrastructure used for card payments is secure and that payment standards are adhered to.

10.2 Infrastructure penetration testing

Regular scheduled infrastructure internal and external penetration tests are undertaken. These ensure that the infrastructure is secure and robust and that vulnerabilities are identified and addressed. The payment card merchants receive updates from Ealing Council to verify compliance on a scheduled basis.

10.3 Card payments

Card payments are taken by Ealing Council staff and card details are securely managed. Ealing Council use a hosted payment application which is approved by the industry standards council.

10.3.1 General requirements

All payment agents are required to adhere to the following requirements set out by PCI DSS:-

- only take card payments in a secure environment - this is an area whereby payment card details are not exposed to anyone else or any third party and that card payment information cannot be viewed or overheard by anyone else or any third party
- use equipment and software provided by the council and use login credentials assigned
- only record payment card details using Ealing Council applications or certified PIN entry devices
- do not record any payment card details on any other media including writing down on paper

10.3.2 Card payments taken in home working environment

Processing of card payments in the home environment is allowed subject to all the requirements in section 10.3.1 being met along with the additional controls:

- multi factor authentication will prompt for the additional token every 24 hours.
- the member of staff must ensure that their desk is clear of all paper and other devices not specifically associated with their work
- the member of staff can only access the payments systems during normal working hours
- the member of staff ensures that they lock their computer every time they leave their desk
- the member of staff shuts down their computer at the end of each workday
- the member of staff attends the council office once a month to ensure their surface is patched completely up to date with the latest security patches
- the member of staff will stop call recording during the time of the card payment
- all staff must have satisfactorily completed the yearly data protection training

11. Mobile computing and remote working

11.1 Introduction

The purpose of this document is to provide direction to staff on remote and mobile computing in order to ensure that this use complies with security standards. Specifically, the objectives of the policy are:

- to ensure that council meets its legal obligations
- to promote safe and secure use of mobile equipment in support of council operations
- to provide a secure working practice for staff working remotely
- to ensure that the security of computer systems and the information they hold is not compromised in any way
- to prevent the council’s reputation from being damaged by the

inappropriate or improper use of its information resources

11.2 Scope

Within the work environment a considerable effort in terms of money, technical knowledge and working time is expended to ensure that we maintain an appropriate level of security around information that belongs to the council or is held by the council on behalf of the public or partner organisations. Much of this information is sensitive and contains personal details of individuals or confidential commercial information.

The Sixth Principle of the Data Protection Act 2018 states that “Personal data shall be processed in a manner that ensures 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. This provision applies to information that is managed by the council within the workplace, and very importantly, also applies to information that is taken away from the workplace. As the use of mobile computing resources grows it is vital that the data held on these devices is not compromised by poor security practices. Mobile devices by their nature are vulnerable to being mislaid as well as being attractive to a potential criminal. It is important therefore that all users of mobile equipment such as laptops, tablet PC’s, handheld devices, memory sticks and mobile phones are aware of the inherent risks associated with their use and measures that can be taken to protect the policy focuses on two key areas; the use of a remote access route to the Ealing environment that does not result in data leaving the security of the Ealing network and where the use of mobile device is unavoidable, ensuring that data contained on them is encrypted to an appropriate standard.

Both solutions involve added cost for the user but this has to be considered in the light of the benefits that remote working brings and the penalty that arises from a loss of sensitive data, which not only carries risk to the individuals involved, but also can result in monetary penalties from the Information Commissioners Office.

11.3 Policy statement

Home, remote and off-site working must be authorised and controlled by business management and suitable arrangements must be in place for the environment used to be safe and secure.

Within the workplace, a number of security measures are taken to protect council information, many of which are legal requirements of the Data Protection Act. It is not acceptable to bypass these by removing information on unprotected devices or by email, and then to store it on personal devices for work at home or on the move.

In circumstances where a mobile solution is required only devices approved and supplied by the corporate ICT and data security manager are approved for connection to the Ealing network for the purpose of extracting or manipulating data, and these devices must be encrypted to AES256 standard. The Removable Media Policy (A10.1) must be followed in all cases.

Access to the Ealing mail system (Outlook Web Access) is permitted from any device but information must not be extracted from the mail system and downloaded onto anything other than an Ealing supplied laptop, surface, or other device. Storing such information, especially if it is sensitive in nature, on a personal computer even if this is well protected is a breach of policy.

All personnel using mobile computing equipment or working offsite are required to comply with this policy. Failure to do so may result in withdrawal of facilities and/or

disciplinary action.

11.4 Mobile computing

This section applies to all mobile computer devices including, but not limited to laptops, tablets, surfaces, mobile telephones.

Only Ealing supplied devices are authorised to connect to the Ealing network. These devices should be asset tagged and securely marked before release.

All devices supplied by Ealing are protected by encryption software. Users must ensure that they use strong passwords (alpha, upper and lower-case, and numeric characters, no recognisable words, and at least 8 digits long) and that these passwords are kept secret.

It is forbidden to load any software onto an Ealing Council device. All software must be loaded by ICT.

For Ealing supplied devices, users must connect regularly to the Ealing network by physical connection where it will be automatically updated on connection. Any Ealing supplied software must never be de-activated.

11.5 Reporting security incidents

Users should report any security incident involving personal data or information loss (such as a stolen or lost device including but not limited to surface or phone etc) to their line manager and log an incident, via the portal on itsupport.ealing.gov.uk, as soon as practicable, providing details of the equipment and the data or information that is at risk. Ealing is obliged to report incidents of data loss to the Information Commissioner.

12. Electronic communications

12.1 Introduction

Electronic communication plays an essential role in the conduct of the council's business, with the council's workforce making extensive use of the electronic communication systems and facilities both within the organisation and externally with other organisations and customers.

The council values every authorised user's ability to communicate with colleagues, clients, customers and business partners and has invested substantially in information and communications technology (ICT) that will enable them to work more efficiently and effectively.

An electronic address, number or account identifies not only the user but also the council as a business organisation and as such any activity engaged in by the user will also reflect on the council.

12.2 Purpose

This section of the policy defines the conditions under which these systems and facilities may be used and the standards of behaviour expected of all users. It will also:

- ensure that the council's electronic communication systems and facilities are used for purposes appropriate to the council's business
- inform users of the applicable laws and policies and ensure compliance

with those laws and policies

- avert disruption to and misuse of the council's electronic communications systems and facilities
- establish rules on privacy, confidentiality, and security in electronic communications

12.3 Scope

This policy applies to all:

- electronic communication systems and services owned, leased or managed by the council or provided by the council via contracts and other agreements. This includes but is not limited to:
    - Internet, intranet, webchat
    - email
    - telephones (landline, mobiles and SMART phones)
    - laptops, tablets and personal digital assistants (PDAs)
    - voicemails
    - videophone and video conferencing
    - faxes, scanners, printers and photocopiers (including multi-function devices)
    - social media
- users granted authorised access to any of the council's electronic communication systems and facilities whether the user is office based or working remotely (mobile and home working)
- electronic communication records created or received by users of those systems and services including the content of attachments and transactional information

To support this policy and to assist users in their use of the electronic communication systems and facilities stated above, good practice guidelines have been produced.

12.4 Provision and use

All users granted access to the council's communication systems and facilities are reminded that these services are provided primarily to support the provision of the council's business and services.

The council is a legal entity and as such, all correspondence including emails is considered to be legally binding, providing that the person is authorised to make a commitment on behalf of the council. Users are responsible for the content of all text, audio and images that they transmit using any of the council's communication systems. The council reserves the right to withdraw the use of these facilities at any time.

13. Removable media

This policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

This policy aims to ensure that the use of removable media devices is controlled to:

- avoid contravention of any legislation, policy or good practice requirements
- maintain high standards of care in ensuring the security of information
- avoid risk to the Ealing network through the introduction of viruses or malicious code

Ealing Council will ensure that the use of removable media devices to store and transfer information is limited to situations where a clear business case exists for their use.

13.1 Purpose

Removable media devices such as laptops and memory sticks must be encrypted to AES256 and use a minimum twelve-character password containing upper and lower case, special characters and numeric.

13.2 Scope

This policy applies to all councillors, committees, departments, partners, employees of the council, contractual third parties and agents of the council who have access to Ealing Council information, information systems or IT equipment and who intend to store any information on removable media devices.

13.3 Definition

This policy should be adhered to at all times, but specifically whenever any user intends to store information on removable media.

Removable media devices include, but are not restricted to the following:

- laptops
- CDs
- DVDs
- optical disks
- Blu-ray devices
- External Hard Drives
- USB memory sticks (also known as pen drives or flash drives)
- media card readers
- embedded microchips (including smart cards and mobile phone SIM cards)
- MP3 players
- digital cameras
- backup cassettes
- audio tapes (including dictaphones and answering machines)

13.4 Risks

Ealing Council recognises that there are risks associated with users accessing and handling information in order to conduct official council business. Information is used throughout the council and sometimes shared with external organisations and applicants. Securing confidential or sensitive data is of paramount importance – particularly in relation to the council's need to protect data in line with the requirements of the Data Protection Act 2018. Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the council. It is therefore essential for the continued operation of the council that the confidentiality,integrity and availability of all information recording systems are maintained at a level that is appropriate to the council's needs.

This policy aims to mitigate the following risks:

- unintended disclosure of information as a consequence of loss, theft or careless use of removable media devices
- contamination of council networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another
- potential sanctions against the council or individuals imposed by the Information
- Commissioner's Office as a result of information loss or misuse
- potential legal action against the council or individuals as a result of information loss or misuse
- damage to reputation of the council as a result of information loss or misuse

13.5 Applying the policy

13.6 Restricted access to removable media

It is Ealing Council policy to restrict the use of all removable media devices. The use of removable media devices will only be approved if safer alternatives for the transport of information, such as secure email, cannot be used. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

For Ealing staff wanting to work from a remote location (such as from home) using your supplied surface device is preferred. This permits access to the same applications and files as are available in an Ealing office. Any files updated through this route remain on the Ealing network and are therefore secure.

Requests for access to, and use of, removable media devices must be made to the information and data management department by email to DataProtection@ealing.gov.uk

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

13.7 Procurement of removable media

All removable media devices and any associated equipment and software must be approved by ICT for use on the network. Non-council owned removable media devices must not be used to store any information used to conduct official council business, and must not be used with any council owned or leased IT equipment.

13.8 Security of data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data that is frequently backed up. Therefore, removable media should not be the only place where data obtained for council purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whilst in their care or under their control.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption must be applied to the information files unless there is no risk to the council, other organisations or individuals from the data being lost whilst in transit or storage.

By default, all emails transmitted via Office365 are encrypted during transit.

For laptops and memory sticks whole disk encryption is mandatory. Products ordered from the Service Ealing catalogue are configured to provide this facility.

13.9 Incident management

It is the duty of all users to immediately report any actual or suspected breaches of information security to the compliance team through the ICT portal. The compliance team will be responsible for handling the incident.

13.10 Third party access to council information

No third party (external contractors, partners, agents, the public or non-employee parties) may transfer data to or from the council's network, information stores or IT equipment without explicit agreement from the CIO or CISO/SIRO.

Should third parties be allowed access to council information then all the considerations of this policy apply to their storing and transferring of the data.

13.11 Preventing information security incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the ICT Portal should removable media be damaged to arrange for safe disposal of the device and its replacement.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the council, other organisations or individuals from the data being lost whilst in transit or storage.

13.12 Disposing of removable media devices

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within the council or for personal use, must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to - ICT for secure disposal.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact ICT.

13.13 User responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- any removable media device used in connection with council equipment or the network or to hold information used to conduct official council business must be approved by ICT
- all data stored on removable media devices must be encrypted
- virus and malware checking software must be used when the removable media device is connected to a machine
- only data that is authorised and necessary to be transferred should be saved on to the removable media device - data that has been deleted can still be retrieved
- removable media devices must not be used for archiving or storing records as an alternative to other storage equipment
- special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss

For advice or assistance on how to securely use removable media devices, please contact the compliance team through the ICT Portal.

14. Bring your own device (BYOD)

14.1 Introduction

Mobile electronic devices have seen a rise in popularity e.g., smartphones, tablet computers. There is increasing pressure to allow employees to use these in the workplace in order to carry out their duties and a growing demand for individuals to use their own devices to access and store corporate information, as well as their own.

Bring your own device (BYOD) is a phrase that was initially conceived to describe corporate initiatives to allow staff to use their privately owned IT devices (PCs, laptops, tablets and smartphones) to carry out business activities.

This policy should be read in conjunction with the Acceptable Use Policy at section 9.0.

14.2 Purpose

The Data Protection Act 2018 (DPA) – sixth principle states that: -

“appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data”

As data controller, Ealing Council must remain in control of the data that we are responsible for regardless of who the owner is of the device is that is used to carry out the processing.

The purpose of this policy is to put in place appropriate security measures to prevent the data that Ealing Council holds being accidently or deliberately compromised in circumstances where employees are using their own devices to carry out business activities.

It is also to ensure that employees who use their own devices to connect to our own IT systems are fully aware and understand their responsibilities.

14.3 Risks

By its very nature, the user is responsible for owning, maintaining and supporting the device.

We will have no control over, or knowledge of, the applications installed on the device. This could include hacking tools, viruses and other types of applications that we have gone to great lengths to prohibit on other devices. This will almost certainly introduce unmanaged (for instance not secure, patched or supported) applications.

The user is also responsible for:

- unintended disclosure of information as a consequence of loss, theft or careless use of removable media devices
- contamination of council networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another
- potential sanctions against the council or individuals imposed by the Information
- Commissioner's Office as a result of information loss or misuse
- potential legal action against the council or individuals as a result of information loss or misuse
- damage to reputation of the council as a result of information loss or misuse

14.4 Implementation

- by using the BYOD service each user accepts the consenting to our remote wiping of their data and device
- these devices will not be able to connect to the corporate network and connectivity will be at the user's cost
- each authorised BYOD will have a Mobile Device Manager installed. This will:
    - enforce a PIN to access the device and encrypt the hard disk
    - ensure that the device is locked if an incorrect password is entered too many times
    - directly manage access to email/calendar entries that has been synchronised to the device and allow us to delete this remotely
    - provide the facility to locate the device remotely
    - give us the ability to remotely wipe the entire device
- if possible, there should be clear separation between the personal data that is processed on behalf of the data controller and that of the device owner's own use for example different apps for business or personal use.

- staff should report the loss or theft of a device immediately to the ICT department
- when a member of staff leaves the employment of the council all council data must be deleted from the device

14.5 Disclaimers

- whilst IT will take every precaution to prevent the employee's personal data from being lost in the event it must remotely wipe a device, it is the user's responsibility to take additional precautions, such as backing up email, contacts etc
- Ealing Council reserves the right to disconnect devices or disable services without notification
- lost or stolen devices must be reported to Ealing Council within 24 hours. Employees are responsible for notifying their mobile provider immediately if they lose their device
- the employee is expected to use their device in an ethical manner at all times and adhere to this Information Security and Data Management Policy
- the user assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware and/or other software or hardware failures, or programming errors that render the device unusable
- failure to adhere to this policy will be considered a serious disciplinary offence and will be dealt with in accordance with the appropriate council disciplinary procedures. This could lead to a termination of employment for employees, termination of a contract in the case of service providers or consultants and expulsion in the case of a student placements