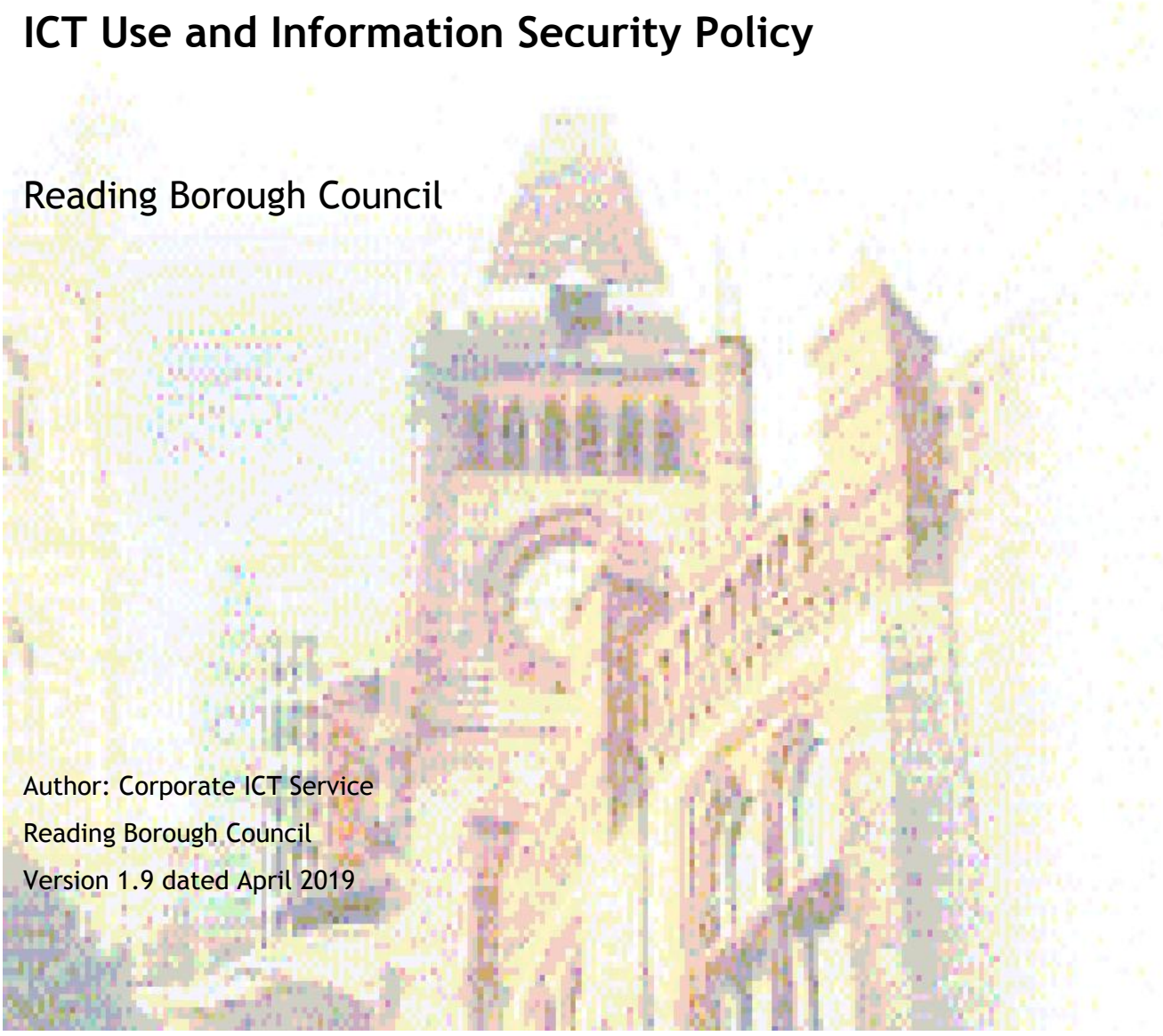
ICT Use and Information Security Policy

Reading Borough Council



Author: Corporate ICT Service

Reading Borough Council

Version 1.9 dated April 2019

Purpose

This policy addresses the information security risks of Reading Borough Council and use of Council owned Information and Communications Technology (ICT).

Document control

Version	Date	Author	Comments
1.0	23rd Dec 2011	Mike Ibbitson	Full review, minor corrections and incorporation of later comments.
1.1	23rd Dec 2012	Mike Ibbitson	Reviewed
1.2	3rd Sept 2013	John Barnfield	Councillor Policy Introduction
1.3	12th Sept 2013	John Barnfield	Calendar Adjustment for Councillors
1.4	14th Oct 2013	John Barnfield	Monitoring and Non-EU Usage, Mobile Phone (reinstated)
1.5	17th Nov 2014	John Barnfield	PCI DSS Regulation Section & Commitment Statement Added GCSX Personal Commitment Statement Added Electronic Media Personal Commitment Statement. NFI Fraud Initiative Policy BYOD & BPSS Checks Pwd Length to 9 Characters
1.6	23rd Aug 2016	John Barnfield	Caldicott role, Cyber Crime / Fraud, Mobile Apps, Information Asset Owners
1.7	5th October 2016	John Barnfield	Lost equipment update & Skype Messenger & Signature format
1.8	18th May 2017	John Barnfield	Minor updates to Glossary, and Gcsx email handling para 111.
1.9	1st Apr 2019	John Barnfield	Updated for GDPR, Data Retention, Closedown desktops, GCSX email, Signatures, File sharing sites, Transparency Monitoring, Data Retention, smartphones, PCI, Cyber Security, Printing.

Distribution

Releasing and issuing of this document is restricted to Reading Borough Council.

Maintenance

Following approval any required changes to this Policy shall be raised and notified to the Corporate ICT Service (CICTS) specifying the reason for and details of the changes.

Document references

Document title	Date	Published by
Data Protection Act 2018 (GDPR)	2018	UK Public General Act
Computer Misuse Act 1990	1990 c.18	UK Public General Act
Freedom Of Information Act 2000	2000 c.36	UK Public General Act
Environmental Information Regulations 2004	2004 No.3391	UK Statutory Instruments
Human Rights Act 1998	1998 c.42	UK Public General Act
Regulation of Investigatory Powers Act 2000	2000 c.23	UK Public General Act
Whistleblowing Policy	July 2000	Reading Borough Council
Procedure for Dealing with Requests for Information	June 2007	Reading Borough Council
Grievance and Disputes procedure	September 2006	Reading Borough Council
The Code of Conduct	Nov 2017	Reading Borough Council
Customer Care Handbook	November 2009	Reading Borough Council
Records Management Policy	May 2005	Reading Borough Council
RIPA (Regulation of Investigatory Powers Act) guidance	n/a	Reading Borough Council
Data protection policies, including subject access request procedures	n/a	Reading Borough Council
Information sharing policies	Various	Reading Borough Council
Document retention schedules	2018	Reading Borough Council
Equality and diversity procedures	n/a	Reading Borough Council
Joiners & Leavers process	n/a	Reading Borough Council

Document title	Date	Published by
ICT Security Policy Statement	Apr 2019	Reading Borough Council
ICT Information Risk Management Document Marking Policy	Apr 2019	Reading Borough Council
ICT Standards Expected of Third Parties Policy	Apr 2019	Reading Borough Council
ICT Camera and Video Usage Policy	Apr 2019	Reading Borough Council
ICT Huddle Acceptable Use Policy	Apr 2019	Reading Borough Council
ICT Removable Electronic Media Policy	Apr 2019	Reading Borough Council
ICT GCSX (PSN) Personal Commitment Policy	Apr 2019	Reading Borough Council
ICT PCI DSS Personal Commitment Policy	Apr 2019	Reading Borough Council
ICT Controls for Storage & Carriage of Hardcopy Documentation (Guidelines)	Apr 2019	Reading Borough Council
ICT Email Monitoring Policy	Apr 2019	Reading Borough Council
ICT Internet Monitoring Policy	Apr 2019	Reading Borough Council
PCI DSS	Dec 2004	Payment Card Industry Security Standards Council
NFI Fraud Initiative	Aug 2014	Audit Commission

Glossary of terms

Term	Definition
BPSS	Baseline Personnel Security Check.
BYOD	Bring Your Own (Personal) Device.
CYOD	Choose Your Own (Council Supplied) Device.
EAS/Mailmeter	E-mail Archiving System.
GCF	Government Convergence Framework. The GSi Convergence Framework (GCF) supports the continuing provision of GCSX, GSE, GSI, GSX and XGSi networks and services and migration to the Public Services Network (PSN). The Government Secure Intranet (GSI) is a UK government secure wide area network. Its main purpose is to enable connected organisations to communicate electronically and securely at a range of protective marking levels.
GCSX (PSN Code of Connection)	Government Connect Secure Extranet – secure, private, Wide Area Network. PSN being the Public Service Network Code of Connection standard the Council must adhere to.
ICT	Information and Communications Technology.
IM&T Security Officer	Information Management and Telecommunications.
ISO27001/2013	Standard for Information Security Management Systems.
NETConsent	Software that allows for electronic acceptance of policies at logon.
NFI	National Fraud Initiative.
PC	Personal Computer.
PCI DSS	Payment Credit Card Industry Data Security Standard.
PSN	Public Services Network.
RBC	Reading Borough Council.
SIRO	Senior Information Risk Officer (Head of Legal).
VPN token	Virtual Private Network token.
GDPR	General Data Protection Regulation changes to Data Protection Act enforced from May 2018.
Caldicott Guardian	A safeguarding role introduced nationally to ensure Local Authorities Social Services apply sensible Information Governance and processes to protect and

	safeguard clients.
NCSC	The National Cyber Security Centre.
Cyber Security Essentials (Plus)	Standards for Cyber Security set by NCSC.
NCSC Cloud Security Principles	Security principles set by NCSC for secure Cloud delivery.
ISO 27002	An Information Security Standard published by the International Standardisation Organisation.
ISO20000 (ITIL)	An ICT delivery Standard (IT Infrastructure Library - ITIL) published by International Standardisation Organisation.
CSA	Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to "promote the use of best practices for providing security assurance within Cloud computing and to provide education on the uses of Cloud Computing to help secure all other forms of computing.
CSA STAR	CSA STAR Certification is a unique new scheme developed to address specific issues relating to cloud security as an enhancement to ISO 27001.
CSA CCM 3	CSA Cloud Controls Matrix
GDPR	European General Data Protection Regulations – a major revision to the Data Protection Act which introduces new obligations and fine structures up to E20m and which came into effect May 2018. Led to revision of the UK Data Protection Act 2018.
Secure Email Blueprint	A new standard for secure Public Sector email delivery that will replace GCSX email by 31.03.2019. Using a combination of DMARC, DKIM, SPF, TLS standards to deliver email securely and stops external parties "spoofing" Council email. Sending email within the Public Sector will be secure by the use of TLS encryption.

Contents

1. Executive Summary

1 This policy sets out the Council's rules and procedures relating to information security and all employees & councillors responsibilities with regard to information security. Information security and governance is of great importance to the Council to protect vulnerable citizens, ensure compliance with legislation and demonstrate that the Council understands and applies proportionate guidance and process to recording, storing, processing, exchanging and deleting information. Should this not be achieved the Council's operations and customers can be put at risk (including the safety of individuals, loss of financial information, breach of commercial confidentiality and subsequent financial penalties from the regulator, the Information Commissioner with fines of up to E10m for technical breaches and E20m now possible for bad information breaches following the GDPR revision of the Data Protection Act in May 2018.

2 This policy provides detailed guidelines on all aspects of information security and associated ICT equipment use. It also provides guidance for all employees relevant to their role in the organisation (see Appendices). A summary of these guidelines should not be regarded as sufficient knowledge but the principles which run through these guidelines are simple and can be summarised as follows:

- All staff and councillors should consider the sensitivity of the information they handle (with personal and sensitive information about vulnerable people being the most important) especially in context with compliance with the Data Protection Act GDPR revision that introduced new categories of Sensitive Personal Data from May 2018 (e.g. IP addresses, Biometric data etc);
- All staff and councillors will protect that information in proportion to that sensitivity by applying this policy and ensuring that information, whatever it's format, should be secured by physical means (such as locking paperwork away) or by using approved electronic means (such as only using Council IT encrypted laptop and smartphone equipment);
- All staff and councillors will be responsible for the protection of their login and passwords and will not share these;

- All staff and councillors will ensure changes to shared information are updated as soon as possible into the **primary record location or system** and not kept at home or personal storage not accessible to others;
- All services will publish clear guidelines for the public to be clear and transparent as to what information will be collected from them and the channels used to collect this so as to protect members of the public from fraudulent social engineering and email spoofing attacks;
- All staff and councillors will conduct their business operations in a sensible low risk manner aware of the continuing Cyber Security threat (be careful when opening emails and documents from external sources or visiting Internet sites);
- Managers and Group Leaders must ensure this policy is applied within their areas of work and should also lead by example to all employees / councillors.

3 This policy is compulsory. Any breach of the policy may result in disciplinary action being taken under the Council's Disciplinary Procedure for staff, and action progressed for councillors in accordance with the Member Code of Conduct as set out in the Constitution of the Council. If something sensitive is accessed by accident this should be reported to the appropriate Line Manager or Councillor Services as is appropriate at the earliest opportunity.

4 Any breaches of security (non-compliance with this Policy) must be reported in accordance with the Councils Security Incident process by logging a Security Incident Call with the ICT Service Desk (Ext 72861) - see Appendix 4. This is to safeguard the Council and limit potential damage from information loss and to ensure appropriate notification of all relevant persons/organisations. Any data breaches must be reported and handled in accordance with the Council's Breach Management Policy.

2. Purpose

5 The purpose of this policy is to protect from all threats, whether internal or external, deliberate or accidental, the information assets of Reading Borough

Council and in doing so assist the Council in planning and delivering high quality, safe services to all customers and ensuring compliance with legislation.

3. Introduction

6 This policy sets out the Council's rules and procedures relating to information security and all staff's responsibilities with regard to information security. The implementation of strict guidelines is a matter of great importance.

7 **SUCH GUIDELINES MUST BE RECOGNISED BY STAFF AND COUNCILLORS AT ALL LEVELS (INCLUDING STAFF OF ARMS LENGTH COMPANIES WHOLLY OWNDED BY THE COUNCIL) WHO MUST ENSURE THEY ARE APPLIED AT ALL TIMES. ANY BREACH OF THIS POLICY MAY RESULT IN DISCIPLINARY ACTION BEING TAKEN UNDER THE COUNCIL'S/ARMS LENGTH COMPANY'S DISCIPLINARY PROCEDURE OR MEMBER CODE OF CONDUCT (IN THE CASE OF COUNCILLORS), AND COULD FOR STAFF, IN THE CASE OF GROSS MISCONDUCT, RESULT IN DISMISSAL FROM EMPLOYMENT.**

8 They must also be supported by Staff Management and Group Leaders who must take responsibility for their implementation and continued adherence.

9 Any breaches of security (non-compliance with this Policy), however minor, must be reported to Northgate Service Desk (Ext 72861), line managers, the Council's Solicitor Head of Legal (Senior Information Risk Owner), and the ICT Manager in Corporate ICT Services, in accordance with the Councils Security Incident Management Policy and in the case of Data Incidents to the Council's Data Protection Manager using the Information Security Incident Reporting form (see Appendix 4) to record the incident at the earliest opportunity. Referrals may be also made to the Head of Internal Audit and the Head of Human Resources for further investigation.

4. Policy Statement

10 It is the policy of the Council to ensure that all information systems operated by the Council are secure systems, which must aspire to comply with the requirements of

the Data Protection Act & GDPR Revision, the Computer Misuse Act and, at the level of principles, aspire to the International Standard for Information Security ISO27001/2013. It is also the aim of the Council that all their staff and councillors must be fully aware of the need to maintain secure systems and they must fully understand their responsibilities as outlined in this policy document. Refer to the separate ICT Security Policy Statement for the full Council Policy Statement detail.

11 All employees and councillors are responsible for ensuring that they understand and abide by these procedures and their contents. All persons are expected to behave and act professionally at all times, and are responsible for their actions including the actions of anyone logged in as them. Failure by any employee of the Council (or any arms-length company of the Council) to abide by the contents of this document will be viewed as a serious matter and may result in disciplinary action. Failure by any councillor of the Council to abide by the contents of this document could result in action being taken in accordance with the Member Code of Conduct. CICTS will hold the Security Officer role as defined within standard ISO27001/2013 (formerly BS7799) although responsibilities may be delegated. This role will operate in conjunction with the Council's Senior Information Risk Officer (SIRO). The implementation of this policy is important to maintain and demonstrate the integrity and security of the Council's dealings with our customers, partners and other members of the community.

12 The Council's ICT Systems are treated as business systems and are monitored accordingly for security compliance.

Any concessions for personal use are only granted on the basis of reasonable behaviour and usage that does not interfere with working, noting the concession can be withdrawn at any time, and should not be taken as a guarantee such facilities will always be available and any activities are always undertaken at the individuals own risk. Any personal activity must never expose the Council to any Consequential Liability, Financial liability, Network risk, or reputation loss within the community. Namely, the Workplace **must not** be considered an extension of any home personal IT environment.

It is the policy of the Council to ensure:

- The Councils ICT Infrastructure is protected from external threats and malware
- A risk based approach is taken to Information Management.
- Information is protected against unauthorised access.
- Confidentiality of information is maintained.
- Information is not disclosed to unauthorised persons through deliberate or negligent action.
- Integrity of information through protection from unauthorised modification.
- Availability of information to authorised users when needed.
- Regulatory and legislative requirements will be met (see goals, specific policies and conditions).
- Contingency plans will be produced and tested as far as is practicable to ensure business continuity is maintained.
- Information security training will be given to all staff and councillors.
- All breaches of information security and suspected weaknesses are reported, investigated and appropriate action is taken.
- Use of Cloud based systems comply with Data Protection requirements (including any post Brexit data hosting compliance requirements).
- Access to the Council's network from non-EU (higher risk) countries will only happen following appropriate risk assessment and sanctioning.
- Council staff are appropriately briefed on the threats posed by Cyber threats and the action to take e.g. Social Engineering, Phishing, bogus telephone callers, bogus visitors, bogus signature harvesting, Malware, Viruses, and Ransomware.
- Staff are aware of the need to show ID when in council's buildings and to challenge those not displaying appropriate ID or visitors passes, or inform security immediately.

13 It should be noted that the Council policy on information and information technology security is evolving alongside technology and further guidance will be added where and when necessary.

14 Where this policy touches upon these areas it is written as if these exist but there are footnotes which make this clear and link existing practice to the policy. This policy itself will evolve over time and will be part of the Council's Information Security Management System (ISMS) as defined within ISO27001/2013.

15 The Information Security policy, together with the following documents, comprise the key policy and process elements of the ISMS:

- ICT Security Policy Statement
- Information Sharing Code of Practice(s)
- Document Retention Schedule
- Information Asset Ownership Register
- ICT Information Risk Management Document Marking Policy
- ICT Standards Expected of Third Parties
- ICT Camera & Video Usage Policy
- ICT Huddle Acceptable Use Policy
- ICT Removable Electronic Media Usage policy
- ICT GCSX (PSN) Personal Commitment Policy
- ICT PCI DSS Personal Commitment Policy
- ICT Security Golden Rules (for Staff and Councillors)
- ICT Controls for Storage & Carriage of Hardcopy Documentation
- ICT Email Monitoring Policy
- ICT Internet Monitoring Policy
- Incident Reporting
- Data Protection Policy Application

- Freedom of Information Policy

The consequences of breaching the rules detailed here is reflected in the Disciplinary Policy for Staff and the Member Code of Conduct for Councillors.

5. Applicability & Monitoring

15 All employees, temporary staff, **visitors** and workers, and councillors who have involvement with information assets covered by the scope of this policy, will be responsible for implementing this policy and shall have the support of the Council who have approved this policy. Where services are provided to the Council by outside organisations then the contracting officer shall ensure that the provisions of this policy are known to, and accepted by that organisation as part of that contract.

16 Councillors now fall within the scope of this policy.

The Council has provided ICT Systems for Council business use and therefore there are no automatic rights of personal use or individual privacy. However the Council does acknowledge that there are some occasions in a modern electronic age where an employee may require reasonable access to personal e-mail and restricted appropriate internet sites where this contributes to their productivity as part of a work life balance.

18 The Council is ultimately responsible for all business communications, but subject to that will, so far as possible and appropriate, respect your privacy and autonomy while working. However in return the Council expects employees to follow instructions for conducting business and personal use at the Council's discretion as directed within this document and employees **must not** see the Council's ICT working environment as an extension of their own private home environment.

19 The Council will monitor your business communications for reasons that includes:

- Providing evidence of business transactions
- Ensuring the Council's business procedures, policies and contracts with staff are adhered to
- Complying with any legal obligations
- Monitoring standards of service, staff performance and for staff training
- Preventing or detecting inappropriate unauthorised use of Council's ICT Infrastructure and systems

- Maintaining the effective operation of the Council's ICT systems.

6. Goals Of This Policy

20 To manage risks to an acceptable level through the design, implementation and maintenance of a formal Information Security Management System.

21 To comply with legislation, examples of which include;

- Data Protection Act 2018
- Computer Misuse Act 1990
- Freedom Of Information Act 2000
- Environmental Information Regulations 2004
- Human Rights Act 1998
- Regulation Of Investigatory Powers Act 2000

22 To comply with statutory and non-statutory guidance as issued from time to time by Government (e.g. PSN Code of Compliance).

7. Responsibilities

23 The Council accepts and endorses this policy (in accordance with the Councils ICT Security Policy Statement).

24 The Corporate Management Team will approve detailed policies and procedures for Information Security and agree implementation arrangements.

25 CICTS and the Councils Senior Risk Information Officer (SRIO) will be responsible for the creation and review of this policy and underpinning Information Security Management System. The Council's Caldicott Guardian will ensure compliance with Information Governance from a Social Services perspective.

17 The Information Security Manager (or person whose role encompasses this function) facilitates the implementation of this policy through the appropriate standards,

committees and procedures supported by the Council's SIRO and Data Protection Manager functions.

27 All employees, temporary staff, visitors and any workers acting on behalf of the Council, Councillors and anyone with access to RBC equipment or data, must follow all and any procedures in place, which are designed to maintain the Information Security Policy.

28 All such personnel have a responsibility for reporting security incidents and any identified security weaknesses (including loss of equipment) to the Northgate Service Desk 0118 9372861.

29 The Council will update employees on Information Security matters by briefings, workshops and other means as necessary.

30 Any deliberate act to jeopardise the security of information that is the property of the Council or their clients may be subject to disciplinary and/or legal action, as appropriate.

8. Guidelines

8.1 General

31 Security is not just a matter of restricting unauthorised access to data; it is also a question of ensuring that the confidentiality, integrity and availability of the data is kept. This applies to IT systems as well as data held on paper files. Information will be treated as an asset and managed as such.

8.2 Network Security

32 Under no circumstances is any non-Reading Borough Council owned equipment to be connected or installed to the Council data network (computer network), communications facilities or any Council owned computer without the written consent of the ICT Manager. The Council does provide some publicly available wireless networks these networks do not require the use of RBC equipment to allow connection and are secure and physically separate from the Council's business network.

At all times PSN Services will be protected by appropriate Boundary / Gateway controls between Non-PSN and PSN Services so as to fully protect the PSN Network to the standards required by the PSN code of connection.

33 Remote access to the Council's network is granted from within the E.U. If remote access is required from other countries this must be preceded by a risk assessment and specific permission of the ICT Manager. Under no circumstances must remote direct network access be attempted from high risk countries such as China or Russia.

8.3 Physical Security

34 Access to data held on the Council's information systems can be minimised by restricting physical access to the Council's buildings. Where information is kept in offices, access to buildings must be restricted. Such restrictions include making sure security doors are closed properly and that entry codes are kept secure and changed regularly. Doors and windows must be secured at lunch times and overnight and at all times when the office is left unattended.

35 All Council staff must wear ID at all times on council premises. Visitors to Council buildings must be accompanied at all times and signed in and out of the premises on arrival and departure, displaying appropriate Visitor passes. Incidents or concerns regarding physical security should be reported to the facilities management team or manager based on that site.

9. Computer Security

9.1 Equipment

36 All members of staff and councillors are responsible for any equipment issued to them as part of their job. They must report any loss to their Manager and the Northgate Service desk (0118 9372861) as a matter of urgency. Unless there are exceptional circumstances, the Service is liable for the cost of equipment replacement.

9.2 Data Storage

37 All members of staff and councillors are responsible for data entered onto Council computers. The very nature of many types of Council information makes protection of that information of prime importance. All staff have legal responsibilities under the Data Protection Act and the Computer Misuse Act to ensure that unauthorised access to data is not allowed and also that data is accurate and kept up to date. Such restrictions apply not only to people outside the Council but also apply to those in the Council whose work does not necessitate access to the data. All staff and councillors must abide by the rules of the Data Protection Act and the Computer Misuse Act. Specific attention is drawn to caution handling personal or

38 **INFORMATION STORAGE ON C:\ (LOCAL HARD) DRIVE OF DESKTOP COMPUTERS OR LAPTOPS IS ONLY PERMISSABLE WHEN PROTECTED BY FULL DISK ENCRYPTION.**

39 This is because the C:\ is not backed up and does not have the physical security access protection of servers if the PC/Laptop is stolen or lost. Also, if the PC/laptop is to be repaired or replaced, the unit is swapped and the data will be lost. All information related to Council business is to be stored on the personal network drive (the H:\ drive) or on Council shared drives (usually the S:\ drive on the network). This is a secure storage area which is regularly backed up and is therefore resilient to failure. The only exceptional use of the C:\ drive is to temporarily store files during a working session. If this is the case the files should be deleted at the end of that work session.

40 The following types of file should only be stored if they relate to explicit business needs and in any event should be stored sparingly as some file types are often very large and consume a high proportion of the shared drives. Please note, this is not an exhaustive list of file types that are considered potentially unsuitable for storage – it is the initial list which will be reviewed as necessary.

File Type	Description
.AVI	Movie Files
.MPG	Movie Files
.MPEG	Movie Files
.MP3	Sound Files
.MP4	Sound Files

.M4A	ITunes Files
.MOV	Movie Files
.EXE	Executable files[1]
.SCR	Screen Savers

9.2 File Storage and Naming Conventions

41 All documents and files must be given clear and descriptive titles that will help others to understand what is contained within them. All documents should have a date and version number clearly included. This information will help manage and dispose of information responsibly.

42 Individuals working on projects must also ensure that they adhere to any document standards specified by the project's configuration librarian.

43 Information which is no longer required (in line with the directorate's document retention schedule) should be promptly disposed of by deletion or destruction. Unless an audit record of versions is explicitly required previous versions of documents should be destroyed when the new version is created.

9.3 Screen Locking

44 **Computers must not be left unattended when logged on (CTRL ALT DEL - Select Screen Lock).** Whenever staff or councillors move away from a workstation they should ensure that they have logged off or locked the workstation. As an extra precaution computers will be automatically screen locked after ten minutes. When leaving a place of work staff should ensure they have logged off and closed down the workstation correctly.

45 Further guidelines apply to mobile and home workers in respect of portable equipment – see section 11.

9.4 Memory Sticks & Removable Media

46 Staff and Councillors will comply with the Personal Commitment Statement Policy for the use of removable electronic media at all times. The only memory sticks which are currently allowed to be used on Council computers are those which are

[1] No member of staff should be installing software on PCs

supplied as fully encrypted by the Council's ICT Partner via the ICT Service Desk or by the Corporate ICT Service.

47 Memory sticks are tagged as assets and must be treated as such.

48 Any loss must be treated as a security incident.

49 **NO COUNCIL DATA IS TO BE TRANSFERRED TO A HOME PC / LAPTOP FOR WORKING AT HOME.**

50 If you need to work on Council information at home or at a remote location, the Council secure VPN system is only to be used from a Council-issued computer, unless in exceptional or temporary circumstances with the prior consent of a Head of Service. Council laptop devices connecting across Open Public Wifi Access, or Public Wifi where the SID and Password Key are on open display must be protected by additional security (e.g. TLS, IPSEC VPN) to protect the traffic.

9.5 Mobile Telephones, Smart Phones & Tablets, & Faxes

51 The rules of data storage and care of device security apply equally to mobile telephones, Blackberry devices, Smart phones & Tablets, which should not have business related stored data held on them unless fully protected by Mobile Data Management Tool (MDM) and should be kept secure at all times. Wherever possible devices must be protected with a password to a minimum standard as detailed in this document. In the event of loss this should be reported to the Northgate ServiceDesk (0118 9372861) and Corporate ICT Services (0118 9373911).

52 The Council does not operate a Bring Your Own Device Scheme (i.e. use of personal devices). Staff and Councillors should not attempt to use private equipment on the council's main network or Hermes secure wireless network. Choose your own device (CYOD) from a selection of Council secure and supported devices is allowed and are protected by Mobile Device Management Systems.

53 Council issued mobile phones, PDAs and other mobile technology must be authorised by managers in accordance with business need and arranged within the corporate contracts. Employees should always be issued with the standard kit offered within the contract unless there is a justified business need for an upgrade.

54 All staff and councillors must be aware of heightened risks associated with mobile technology, in particular information security risks, risk of theft and possible risk to personal safety. Consider these risks when using mobile technology in Council Offices, outside in public places, and use appropriate caution and safeguards to minimise those risks.

55 Staff and Councillors issued with mobile phones, Smartphones, Tablets or other Personal Digital equipment are responsible for its safekeeping and security

56 Security lock and pin protection must be used where available to protect the device and any stored data. This should not be disclosed to anyone else, and you should not leave the device unattended especially in public areas.

57 Staff and Councillors should record the security IMEI number of their mobile device to allow the mobile network operator to bar the service in the event of loss.

58 Asset details of Council purchase mobile devices must be recorded with personnel to allow tracking and recovery upon employees leaving the Council.

59 Contracts must only be taken out with the Council's approved mobile phone operator. Permission must be sought from the Head of ICT for use of any other mobile operator.

60 Always check with CICTs for any returned mobile devices awaiting reallocation before entering into a new mobile device contract.

61 Broken/faulty mobile devices under warranty should be returned to point of purchase for waranty replacement.

62 Damaged or out of warranty mobile devices must be disposed of in consultation with CICTS for recycling or appropriate electrical item disposal in accordance with the Council's "Green" policies.

63 When taking work-related photos or video using Council mobile devices, care must be taken not to include members of the Public/Staff/Children without prior permission. Consideration must be given to:

- Obtaining permission of subject/s and recording this
- Minimising time images remain on unsecure devices and memory cards and thereafter ensuring secure storage and restricting access on a role based need basis
- Ensuring separate secure storage of memory cards and electrical devices minimising any threat of theft
- Set local policies for transport of cameras or video devices to minimise theft of the device in the field
- Avoiding further sharing of information without the specific permission of the data subject. Use book in/ book out to record location, who, when and why information shared and ensure unltimate retrieval. Ensure all third parties are aware of the Council's security requirements in handling such data
- If information has to be moved use encrypted electronic media to do so
- Logging and recording detail of all such information for disclosure if required under Data Protection Subject Access Requests and performing searches as and when required to do so
- Managing the ultimate destruction of all such material under defined retention policies which must have been set

64 Council-issued Mobile phones, Tablets, Smartphones and PDA's are provided for work-related purposes. If they are used for private purposes the Council must be reimbursed for personal call charges including VAT (as this is payable on personal calls). Only corporately approved mobile apps should be downloaded to Mobile phones and Tablets.

65 Staff and Councillors should not respond to unsolicited commercial text / voice-mail messages as this could introduce viruses onto your Council mobile phone.

66 Staff and Councillors must not send inappropriate content from a Council mobile device, or download chargeable ringtones, wall paper, or screen savers to the device.

67 Personal mobile devices should also not be inappropriately used in the workplace. All effort must be made to avoid wasting in-hours working time, disrupting colleagues in their work, and have due regard to maintining work performance at all times. Phones should be set to discrete settings or turned to silent/vibrate mode wherever possible. Similarly texting personal messanges should not disrupt an employee's work performance or distract others.

68 Phones, blackberries and other personal mobile devices should be turned to silent or vibrate when taken to meetings. All care must be exercised so as not to distract the purpose of the meeting. If in exceptional circumstances this cannot be avoided then the Chair of the Meeting should be warned of possible interruption to allow appropriate planning as in the main your full attention is reasonably expected by attending the meeting.

69 Employees must not use a hand-held phone whilst driving; this is illegal under current UK law and is dangerous. Employees must park their car and switch off the engine before using a hand-held. To avoid damage, injury and distraction hand-held mobile phones must also be secured properly when used in a car.

70 Personal mobile devices must not be connected to the Council network or other Council equipment with the exception of Council laptops or netbooks where the personal mobile just provides internet connectivity.

71 No inappropriate photographs, images or jokes received on a Council mobile device should ever be forwarded on. Material of this nature received, gathered or sent genuinely and necessarily in the course of work duties is exempted.

72 Mobile phones and other mobile devices must not be used to harass any persons.

73 Business data/confidential information can only be stored on a mobile device where further security measures protect the data – e.g. encryption and remote wiping.

74 Email with confidential personal information must not be sent from mobile devices unless the device has appropriate security measures (e.g. encryption). Special care should be taken in the operation of Faxes, (as there is no control over documents printed out at the other end) and their usage should be avoided if practically possible. Council mobile devices connecting across Open Public Wifi Access, or Public Wifi where the SID and Password Key are on open display must be protected by additional security (e.g. TLS, IPSEC VPN) to protect the traffic.

9.6 Passwords

75 Most systems within the Council require a log in name and password for access. All staff are given access rights and privileges to the various systems in accordance with the area in which they are working and the type of data they are required to use. All staff will have a log-in for one or more of the network servers in addition to any other systems they use. Councillors will not be given access to Council Application Systems.

76 In all cases any passwords given to you personally are for your use only. Keep Passwords safe and you are responsible for your actions and anyone logged in as you. Passwords should not be written down in an insecure location or given to others to use under **any** circumstances. This includes your manager or Group Leader. If your manager or Group Leader needs access to your computer, for example if you are off sick, they must contact the ICT Service Desk to request managerial access to your computer. You should also register a "Safeword" to assist with Password reset if your manager is not available to authorise (contact the ServiceDesk Ext 72861 for advice).

77 Passwords must be a minimum of 9 characters[2] and should be a combination of upper and lower case characters with a minimum of one number. Ideally it should also contain random characters such as #@?!$& etc. Passwords must include at least three different character types, or they will not be accepted.

78 Do not use family or pet names and if at all possible try not to use proper words. This makes the accidental discovery of a password more difficult. Avoid the use of personal passwords used in your private home environment.

[2] This is the minimum standard required under GCSX CoCo requirements for connection Government secure extranet.

79 Your password must be changed if you feel it has been compromised. You should not choose a password that you have previously used.

80 If you suspect someone else may have detected your password, or you suspect someone else is using it you must change your password immediately and report this as a security incident.

9.7 Backups

81 The Council's ICT Partner team will ensure that all RBC controlled servers and the files contained thereon are backed up on a daily basis. It is the responsibility of individual users to back up any systems which do not deposit their data centrally: they should seek advice from the Corporate ICT Service if this applies. All backups must be kept up to date and must be checked on a regular basis to ensure that it is possible to recover the data on them.

9.8 Network Shared Drives

82 It is the policy of the Council to keep all of its data in a secure manner and to only allow authorised access to files to those who require the data as part of their normal duties. The Corporate ICT Service will grant access to individual data areas as requested in writing by the "owners" of that area. Additionally, managers and supervisors will have access to their staff's individual working areas if required. Group Leaders may request similar access for councillors working areas if required within their own political groups.

83 It is expected that users will make all files of general interest available (normally read only) on a suitable location on the server(s), or on the intranet. Each user is assigned their individual storage area, known as your Home or H:/ drive. Only you have access to the files in this area unless you specifically ask the ICT Service Desk to grant access to others.

9.9 Viruses

84 It is the responsibility of all staff to protect the Council's computer systems from viruses. All files received on disc from outside the Council (including those used at home on home PCs) and any received via electronic mail must be checked for

viruses before being used on Council equipment. Please contact the ICT Service Desk for assistance (ext 72861).

85 If you receive any e-mails that you are unsure of or you do not recognise the sender then do not open them. If you are unsure seek information from the ICT Service Desk.

86 If a virus is suspected, the ICT Service Desk should be informed immediately. The workstation should not be used until given permission from the ICT Service Desk and a sign stating this should be placed on the workstation to warn other users. Any disks, CD ROMS, and USB memory sticks that have been used on the suspected infected workstation should be gathered together and not used.

87 The intentional introduction/sending or downloading of files or attachments which contain viruses, or which are meant to compromise the Council's systems, is a serious breach of this Policy and may result in disciplinary action which could result in dismissal and prosecution under the Computer Misuse Act.

9.10 Network Accounts

88 The Council's ICT Partner Service Desk is responsible for the creation and setup of New User Accounts (network logins) and also for e-mail accounts. Individual departments and system owners are often responsible for allocating access rights to staff wishing to access their line of business applications and systems. Councillor Services will act on behalf of Councillors in respect to councillor accounts.

89 Any access to internal systems via dial-in connections is prohibited. All requests for external 3rd Party network connections will be processed by the Council's ICT Partner and will be strictly governed by relevant standards and approval process.

9.11 Printing

90 Printing should be in black and white unless there is a clear business need to print in colour. Defaults on printers to print black and white should not be changed.

91 For Security reasons, printing is not allowed from home other than by approved exception. Users are always responsible for secure management of their printed output to control appropriate circulation and secure disposal.

92 Users are responsible for checking all printed letters are checked and sent to the correct locations (i.e. envelope addressing matches letter contents).

93 Staff should consider the use of the Central Print room for larger volume prints to safeguard the expected life of office printers and so as not to disrupt other office users trying to print.

10. Clear Desk

94 The safest approach to information security is the use of a “clear desk” approach. This is strongly recommended for all users. All manual files and paper records should be locked away before leaving the office. Where this is not possible or where offices employ “open” shelving for the storage of files and documents, offices must be locked when left unattended.

95 Confidential waste shall be disposed of securely. Confidential waste shall be shredded or placed in the appropriate containers for secure disposal.

96 All confidential information shall be held securely in locked containers, lockers, drawers and filing cabinets to prevent unauthorised access

11. E-mail & Internet Use

97 The Internet is a useful tool that enables individuals to access a range of information and services in support of their business roles. This policy sets out the expectations for all Council users.

11.1 Scope

98 This policy applies to all individuals who are provided with access to the Internet whether from an office or from an RBC-provided home or mobile broadband connection and from any device. Access is made available to: RBC employees, temporary workers, and inward secondees, councillors and also those consultants and contractors who are primarily based on RBC premises.

11.2 Provision

99 The Internet is provided primarily for business use. Reasonable personal use (quota time is usually set at one hour per day) will be permitted provided that it does not interfere with the individual's delivery of their duties or breach any requirements of this policy.

11.3 Downloading of Information Resources

100 Individuals may download information including PDFs and Microsoft Office files from the Internet. To reduce the likelihood of a virus infection, individuals must take care to ensure that the files are from a trustworthy source.

101 Graphical, audio and video files may be downloaded and stored on RBC's network for business use only. Individuals with personal needs for accessing such files must use their own personal equipment and Internet connections to do so.

102 Individuals requiring any new software, including any plug-ins, must make a formal request to the ICT Service Desk (Ext 72861). Software must not be downloaded and/or installed onto Council ICT equipment unless it has been approved by the Corporate ICT Service and can be validated that it is licensed for current use.

103 Individuals are reminded that copyright laws apply to the Internet and care must be taken should there be a need to re-use any information (including images) in any Council work. If there is any doubt, individuals must liaise with RBC's Legal Services department.

11.4 Uploading Data / Information to the Internet

104 Any user or councillor who carries out this function must be sure that the information being uploaded is suitable to upload, and not confidential or personal. Do not post anything on the Internet that could be seen to represent the Council unless you are authorised to do so. If information is confidential or person-specific, advice must be sought from the ICT Service Desk to ensure security controls are in place. Care must be taken when using cloud based services to ensure data is European Economic Area hosted and in accordance with Data Protection Act requirements.

11.5 Prohibited Activities

105 Individuals are explicitly prohibited from using RBC's Internet connection to undertake the following activities:

- Accessing gambling sites (excluding the National Lottery)
- Share dealing
- Auctions and sales of goods except where authorised
- Accessing firearms sites
- Conducting private/freelance business
- Looking at pornographic or offensive images/material
- Accessing sites that promote hatred on the basis of race, religion, sex, sexuality, or other factor that is protected by law is otherwise prohibited under RBC's diversity and equality procedures
- Accessing militant or extremist resources
- Using it to attempt to gain unauthorised access to private networks (i.e. hacking)
- Any activity which is contrary to the Council's Code of Conduct or brings the Council into disrepute
- Any other unlawful or illegal activity

11.6 Internet Filtering and Blocking

106 So that the Internet is used efficiently, safely and primarily in connection with Council business the Council uses Internet filtering software. This software monitors Internet use and bars or limits access to various categories of websites. An individual attempting to access some sites will see a standard web page that explains that access has been blocked or restricted (blocked until an option from a menu is selected). For virtually all sites there is an option to either confirm it is being used for business purposes or to use browsing quota time to continue to access the site. Quota time is usually set at one hour per day but this may vary or change in the future. Individuals who encounter a commonly used business site which is blocked and have genuine business reasons for accessing that site frequently may contact the ICT Service Desk (Ext 72861) and request the site is on an approved list of websites.

11.7 Internet Chat Facilities and Social Networking

107 Individuals may access and use approved chat rooms, discussion group's bulletin boards and social networking sites, but must not post comments that identify or indicate such views to be those of the Council unless authorised to do so by the Head of Communications. Social Media is now a common channel customers expect to communicate over. When using Social Media for Business Purposes you are asked at all times to give proper consideration to the fact that you are making statements on behalf of the Council, that you should have the appropriate knowledge, authority and clearance to make such statements, and have considered your options for statement retraction should this ever prove to be necessary. Please ensure any accounts entered into are properly recorded within your service area and are therefore transferable to other staff in the event that you leave the authority. If you want to use the Council concession that allows for reasonable access to Social Media for occasional private means, you do so knowing the Council's systems are monitored and reported on as business systems and if you are unhappy to accept this then you should make your own separate arrangements for such access (e.g. personal private smartphone). Any personal social media access should not incur any reputational or financial liability for the Council.

11.8 Monitoring and Misuse

108 RBC's web filtering and monitoring software both limits what individuals may access and logs those sites that individuals access or attempt to access. If a line manager or Group Leader is concerned that an individual is misusing their access to the Internet they should contact the ICT Manager or HR Business Partner and make a request for the individual's usage to be investigated. There are further specific separate transparency policies dealing with the monitoring and role based access relating to staff and councillor email and internet use so staff and councillors can be clear on what is held, for how long, who can access this information. Please refer to these policy documents for further detailed clarification.

11.9 E-mail

109 All individuals granted an e-mail account must adhere to the policy contained in Appendix 2 of this document in the use of e-mail and calendar functions. The use of private web based email is a concession for work/life balance and the council does not guarantee availability of this service, retains the right to remove in the event of abuse, and the council must not ever be put at risk from its operation. In particular circulation of inappropriate content (e.g. pornographic material, racist material, malicious, discriminatory, racist, rude or otherwise offensive, copyright non-work related MP3 and DVD files for which the Council will be held liable).

110 Key technical staff controlling the PSN technical architecture should undergo a Baseline Personnel Security standard check (CRB/DBS is accepted too). All PSN users will adhere to a code of conduct as per the ICT (PSN) Personal Commitment Policy (refer to separate Policy document). All Service Managers will ensure delete user requests are submitted to remove accounts promptly after staff leave.

111 Any Personal Identifiable Data sent via e-mail must be sent in an encrypted format which meets the Council standards. All staff have access to Global Certs secure email to facilitate compliance with this requirement.

112 Following adoption of the Secure Email Blueprint standard (DMARC/DKIM/SPF/TLS) both @reading.gov.uk and @brighterfuturesforchildren.org email domains transmit and receive e-mail securely to email domains within the Public Sector.

113 Email sent outside the Public Sector should not be considered secure. Staff should take care to ensure email addresses are selected/typed correctly to avoid miscommunication.

114 Any email with sensitive data or attachments please use Global Certs Secure Email when sending externally outside of the Public Sector to protect the contents.

115 Sensitive email should be appropriately document marked (e.g. OFFICIAL, OFFICIAL-SENSITIVE), when sending internally or to other Public Sector Organisations who recognise the Government Document Marking Standard. It is option to use

document marking outside of the Public Sector as the recipient is not likely to understanding the scheme unless explained.

116 Employees, workers and councillors understand that the RBC e-mail account must only be used for work-related purposes and not for personal use. The RBC e-mail account stores e-mails, which can be retrieved and viewed by other officers of the Council, including where appropriate approval has been given for disciplinary investigations. Please be careful clicking on links or attachments received in emails from external sources.

117 Auto-forwarding of Council emails, i.e. without intervention, to personal accounts is not permitted. Auto-forwarding of Council e-mails to known business partners will be controlled by the Head of ICT, and is on an exception-basis only.

12. Mobile Workers and Home Workers

118 Any portable device, such as a laptop, Blackberry, Smart Phone or Tablet must be kept in a secure location when not in use. When using equipment on the move, or outside of office hours, reasonable care should be taken to secure it. Equipment should only be left unattended when necessary and if necessary additional steps should be taken such as locking the laptop in a secure, non visible place. Laptops should not be taken into pubs or other busy social areas or where it may be difficult for the user to keep hold of the equipment at all times, and care should be taken to avoid being overlooked whilst using Council equipment in any public area.

119 Any portable computing equipment must not be left unattended during the normal working day unless it is on Council premises where there is good physical security at entrances to the building. Even in these circumstances, users of portable equipment must give consideration to whether an additional security such as a locking device secured to the desk is necessary. Outside of normal office hours and when the building is closed, all portable computing equipment left on office premises should be secured by a device lock or kept in a locked cupboard or similar storage.

120 Portable computer equipment containing personal files shall only be removed from the Council's premises where absolutely necessary. If personal data is used off site then, wherever possible, the equipment shall be returned to the Council's premises immediately after use. Where it is absolutely necessary for sensitive personal data to be processed and stored away from Council premises individuals should inform and record this step with their line manager / Group Leader.

121 Where manual files are processed outside of the Council's property they should be kept with the individual completing this work wherever possible. When left unattended they should be in a locked container and out of view. Any computer equipment or manual files that are travelling with an employee should be locked in the boot of the car or kept with the individual at all times when travelling by public transport. Under no circumstances should any computer equipment or manual files be left unattended one a train or bus or left in a vehicle overnight.

122 Broken or obsolete equipment must be securely disposed of in accordance with Data Protection Act and WEEE requirements. Please contact the Councils Managed Service Partner or CICTS.

12.1 Virtual Private Network (VPN) Tokens

123 Any member of staff or councillor who has been authorised to use a VPN token/VPN software Token will be allowed, by default, to connect their Council-owned computer to the Council network remotely. This is comparably as secure as connecting directly to the network in a Council office using the local area network.

124 To ensure protection of this connection mechanism and value for money, users who do not use their tokens will be challenged to ensure they are still required. All token users have signed for their token and agreed to specific terms of use for their VPN connection.

125 Services must not just exchange VPN Tokens between staff. All changes must be properly registered with the Councils Managed Services Partner. Please Contact CICTS for further information if required.

12.2 Incident Reporting

126 Any breaches of security (defined as non-compliance with this policy), however minor, must be reported to the individual's line manager or Group Leader, the Council's Monitoring Officer and the ICT Manager, using the Council 's reporting form and process to record the incident at the earliest opportunity. A security incident may also by lodged by calling the Councils Managed Services ServiceDesk on Ext 72861 or 0118 9372861 if ringing externally. Staff and Councillors should note the Council has obligations for onwards reporting of security incidents as part of the Public Services Network (PSN) Code of Compliance standard.

127 Loss of **any** piece of ICT equipment (computer, laptop, blackberry, mobile phone, Smart phone, Tablet, USB storage device, VPN token etc), is classed as a security incident and should be reported as outlined above.

13. Management of User Accounts - Leavers

128 Line managers are responsible for ensuring that a Leaver Form is completed and handed to the ICT Service Desk on the day of leaving for all staff who leave the organisation to ensure that their IT account is closed immediately after their departure. Prior to the account being closed, line managers are to ensure that the users work related information, e-mails and data is transferred, if required, to the respective working directory for future access on the system or is deleted. This will ensure that the appropriate security is maintained on leavers' information and data. Councillor Services will perform this function on behalf of councillors in consultation with Group Leaders.

129 All Council owned ICT equipment must be handed back with the leaver's form or fully notified to the ICT Service Desk in the case of items which are too large to easily be handed in. All ICT equipment within its reasonable life will be utilised by the organisation. If the equipment is not to be re-used, it should be returned to Northgate for secure disposal.

130 Failure to comply with the requirements of this policy in relation to ICT equipment is regarded as a serious breach of this policy as it means that ICT equipment can go missing unnoticed, is incorrectly assigned to an individual and can mean parts of

the Council have a lot of ICT equipment when others have little or that new items are purchased unnecessarily.

14. The User's Responsibilities

131 Each individual must ensure that as far as is possible no unauthorised person has access to any data held by the Council. Each person must ensure that any physical security measures are properly used. If you think a security breach has occurred please report this immediately to your Manager and the Northgate Service Desk.

132 Individuals must not deliberately or negligently corrupt, damage or destroy data, software or hardware belonging to the Council. This includes the spreading of viruses or other similar computer programmes. Staff & Councillors will ensure they reload their computers on a regular basis to ensure patches applied are activated to protect their device.

133 Individuals will be given access passwords to certain computer systems. These must not be disclosed to other members of staff or councillors. They should not be written down and they should be changed regularly.

134 Staff shall not purchase, load or download software packages onto their PCs (this includes customised toolbars, screensavers, wall paper or other desktop customisation (unless an exception has been agreed with CICTS). This must only be carried out by ICT staff. On no account must games software be loaded on staff desktops.

135 Staff are permitted to store a small number of personal documents or files on their personal network drives (which do not impact onto the Council operations or back-up capability). Any staff found to be storing large numbers of personal files, especially large files such as photographs or videos may be asked to remove them or in some circumstances be the subject of disciplinary action.

136 Any files received on any media, brought or sent into the Council or files received by electronic mail must be virus checked before being loaded onto a Council PC. This includes any media which have been used on machines at home or otherwise

not on the Council's Premises. For assistance with this, please contact the ICT Service Desk.

137 Never leave your computer unattended when it is logged on. Whenever you move away from your workstation ensure you log off or lock your workstation (locking can be achieved by simultaneously pressing the Control, Alt and Delete keys once and selecting "Lock Computer"). If you are not able to lock your workstation you must ensure that a screensaver is set to a time of not more than ten minutes and is password protected. When travelling lock equipment in the boot of your car.

138 If you cease to be employed by the Council, you must return all paper and computer files, including those on portable media such as CD ROMs, plus all software and hardware to your manager.

139 All staff and councillors are responsible for printed material printed by or given to them. Sensitive documents should be controlled appropriately and securely shredded when finished with (confidential waste).

140 A security checklist covering these responsibilities is given in the Leavers Form. All staff will be provided with a copy as a reminder of their responsibilities and a confirmation of compliance.

15. Managers / Group Leaders Responsibilities

141 All managers & Group Leaders must give their full backing to all the guidelines and procedures as set out and agreed in this document.

142 Certain managers, where they have responsibility for individual systems, must maintain records of users of that system and control their access to it by the granting of access privileges, passwords etc. They must:

- check the user has authorisation to use the service (including that the user has a valid CRB check where this is relevant).
- check the level of access is the minimum level appropriate for the business purpose and is consistent with this security policy.
- maintain a formal record of all registered users.
- immediately remove access rights of users who have left their department or the Council.
- periodically check for and remove redundant users' accounts from the system.
- ensure redundant user accounts are not re-issued to new users.
- ensure Information Asset Owners are appointed for all significant information assets
- ensure appropriate Risk Assessments and Privacy Impact Assessments are undertaken with regard to process changes for Information Assets.

143 The granting of user access to the Council network can only be carried out by the ICT Service Desk. For some line of business systems, the manager is responsible for granting access. In these cases, the manager must ensure they fulfil the above, and keep a record of access granted.

144 Line managers must make the ICT Service Desk aware of all new staff (requiring access to any ICT equipment) so that log-in rights and access privileges can be set as appropriate. This is part of the Council's joiner's process.

145 Where staff or councillors do not have sufficient knowledge to be able to use systems efficiently and securely their managers must ensure that appropriate training is arranged before allowing them access to the Council's computer systems. Advice to managers in making this assessment can be obtained from the ICT Service Desk.

146 Managers must also take responsibility to ensure:

- all staff receive a briefing on this policy as part of their induction programme within two weeks of joining the Council.
- all staff are aware of the strict confidentiality of the information to which they will have access.
- staff use the information in an appropriate manner at all times.
- All staff understand their information governance roles and responsibilities.
- Information Asset Owners have been appointed to safeguard information assets and Privacy Impact Assessments and Risk assessments undertaken so as to ensure compliant and appropriate processes are maintained on-going.

147 A more detailed explanation of these responsibilities is given in Appendix 1. All staff must be provided with a copy as a reminder of their responsibilities.

16. Controls – Adherence to Policies

148 It is up to all managers of staff, information asset owners and Group Leaders of councillors in the Council to ensure that individuals adhere to these procedures. The ICT staff will be responsible for monitoring systems under their control for signs of:

- Illegal or unauthorised software having been loaded.
- Password misuse.
- Unauthorised access to systems.
- Inappropriate data usage and leakage.
- Bad security practices.
- Inappropriate personal private email quota usage.

- Inappropriate mobile phone/tablet/laptop usage for private use.

149 Spot checks will also be made to ensure that where data is not held and backed up centrally, adequate backups are being made.

150 The Council's internal audit staff will regularly review the Council's performance in implementing this policy.

17. PCI-DSS Compliance (Applicable to staff handling Card Payments)

151 Credit card data stored, processed or transmitted by Reading Borough Council must be protected and security controls must conform to the Payment Card Industry Data Security Standard (PCI DSS). Staff involved must also conform to the responsibilities as set out in the separate ICT PCI DSS Personal Commitment Policy.

152 Sensitive credit card data is defined as the Primary Account Number (PAN), Card Validation Code (CVC, CVV2, CVC2), and any form of magnetic stripe data from the card (Track 1, Track 2).

153 It is the responsibility of the Council to publish and disseminate PCI DSS policy and instructions to all relevant users (including staff, vendors, contractors and business partners), and to ensure this section is reviewed and updated against changing PCI DSS regulation updates as issued from time to time, or when there have been significant risk changes to the operational business environment to ensure continued compliance with PCI DSS regulations.

154 **Protect Sensitive Data:**

Sensitive and/or confidential data (e.g., Cardholder Data) must be protected when stored and when it is in transit over public (or untrusted) networks. Strong industry standard encryption methodologies must be used to protect data stored on hard drives, removable media, backups, etc. The following policies ensure proper encryption of stored data and data in transit over open, public networks.

155 **Protection Methods:**

Protection methods such as encryption, truncation, masking, and hashing are critical components of sensitive data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable. Credit card data has many sensitive components, including the Primary Account Number (PAN), magnetic stripe authentication data (Track1, Track2), Card Verification Code (CVC), and the Personal Identification Number (PIN), etc. The following policies address the treatment of sensitive credit card data. See the document published by the Payment Card Industry Security Standards Council entitled "PCI-DSS Requirements and Security Assessment Procedures v1.2" p. 4 for definitions of cardholder data types.

156 **Storage of Sensitive Credit Card Authentication Data:**

- Never store sensitive cardholder data such as the authentication data (Track, CVC, PIN) after an authorization event has taken place (even if encrypted). (PCI-DSS Requirement 3.2)
- Never store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere) in any database, log file, debug file, etc. after any type of card authorization event. (PCI-DSS Requirement 3.2.1)
- Never store the credit Card Validation Code (CVC) data (3 or 4 digit number located on the back or front of the customer's plastic card) in any database, log file, debug file, etc. after any type of card authorization event. (PCI-DSS Requirement 3.2.2)
- Never store the cardholders Personal Identification Number (PIN) data (includes actual PIN number or Encrypted PIN block obtained during a debit card transaction from the PIN Entry Device) in any database, log file, debug file, etc. after any type of card authorization event. (PCI-DSS Requirement 3.2.3)

157 **Mask Credit Card Numbers in Displays Wherever Possible:**

- Credit card PAN data will be masked or truncated when displaying card numbers on any media (exceptions may be made for those users who have a valid business need to see full PAN data). (PCI-DSS Requirement 3.3)

158 **Encrypt Transmissions of Sensitive Data Over Public Networks:**

- Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Improperly configured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to sensitive data environments.

159 **Transmission of Card Data via End User Messaging Technologies:**

- Prohibit the transmission of unencrypted cardholder data via end-user messaging technologies (e.g., Smartphones recording, e-mail, instant messaging, etc.). (PCI-DSS Requirement 4.2)

160 **Implement Strong Access Control Measures:**

Access to system components and software within the sensitive data environment (cardholder data network) must be controlled and restricted to those with a business need for that access. This is achieved through the use of active access control systems, strong controls on user and password management, and restricting physical access to critical or sensitive components and software to individuals with a "need to know".

161 **Limit Access to Data on a "Need to Know" Basis:**

Systems and processes must be in place to limit access to critical data and systems based on an individuals need to know and according to job responsibilities.

"Need to know" is when access rights are granted to the least amount of data and privileges needed to perform a job.

162 **Restrict Access to Systems in Cardholder Data Environment:**

- Access to cardholder data and systems handling cardholder data must be restricted by a business "need to know". (PCI-DSS Requirement 7.1)
- Automated role based access control systems must be in place on all systems in the cardholder data network. User ID's must limit users rights to only those necessary for their job classification and function. (PCI-DSS Requirement 7.1.2)

163 **Restrict Access to Sensitive Data and System Components:**

Any physical access to data or systems that house sensitive data (cardholder data) provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. The use of personal Smartphone devices that could record or photograph cardholder data should be controlled where payments are taken.

164 **Securing Hard Copy Materials:**

- Services will have local procedures required for protecting paper and hard copy materials (which includes paper receipts, mail, reports, and faxes) containing cardholder data within all facility locations. (PCI-DSS Requirement 9.6)

165 **Secure Media Containing Sensitive Data:**

- Services will have local specific procedures required for controlling the internal or external distribution of any kind of media containing cardholder data. Maintain strict control over the storage and accessibility of both hardcopy and electronic media that contains cardholder data. (PCI-DSS Requirement 9.7, 9.9)
- All forms of media containing cardholder data is required to be classified as sensitive and must be labeled so as to be identified as confidential data. (PCI-DSS Requirement 9.7.1). Mark as OFFICIAL-SENSITIVE.
- All media containing sensitive cardholder data sent outside the facility must be transferred by secured courier or other delivery method that can be accurately tracked. Log all transfers of media containing cardholder data. Logs must show management approval, and tracking information. Retain media transfer logs. (PCI-DSS Requirement 9.7.2). Mark as OFFICIAL-SENSITIVE.
- Management approval is required prior to moving any and all media containing cardholder information out of a secured area (especially when media is distributed to individuals). (PCI-DSS Requirement 9.8)
- Periodic inventory of stored media containing cardholder data must be performed and documentation must be retained showing these inventories were performed. (PCI-DSS Requirement 9.9)

166 **Media Destruction Policies**:

- Media containing cardholder data must destroyed when it is no longer needed for business or legal reasons. (PCI-DSS Requirement 9.10)
- Services will have documented specific procedures that will be used to destroy any hard copy materials containing cardholder data beyond reconstruction. Technologies such as shredding, incineration, pulping, etc must be used to destroy media. (PCI-DSS Requirement 9.10.1). No materials containing cardholder data will enter the public domain in an uncontrolled way.

167 **Security Policy Dissemination With Regard to PCI DSS:**

A strong security policy sets the security tone for the Council and informs employees and vendors what is expected of them. All employees and vendors should be aware of the sensitivity of PCI DSS data and their responsibilities for protecting it.

Note: "employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site.

- Services will ensure circulation of this policy advice to all relevant parties and will ensure such parties understand their obligations for PCI-DSS.

168 **Publish, Distribute, and Update the PCI DSS Policy & Security Policies:**

- The Council requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners). (PCI-DSS Requirement 12.1)
- The Council's information security policy will be reviewed at least annually to keep it up to date with changes in the industry and with any changes in the cardholder network environment. (PCI-DSS Requirement 12.1.3)

169 **Employee Facing Technologies:**

- Services will ensure for all critical employee-facing technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) that all PCI-DSS users have received appropriate guidance and instruction

so as to remain compliant with PCI-DSS Regulations. (PCI-DSS Requirement 12.3).

- No PCI-DSS data must be transmitted in unsecure ways, or without proper informed management knowledge and approval.
- Usage of employee facing technologies (see above) requires explicit approval by authorized parties. i.e. SIRO/CICTS Management(PCI-DSS Requirement 12.3.1)
- A list of all devices and personnel with access to these technologies must be kept by Services and Accountancy. (PCI-DSS Requirement 12.3.3)
- Explicitly define all acceptable use of employee facing technologies. (PCI-DSS Requirement 12.3.5)

170 **Assign Information Security Responsibilities & Train Employees:**

- Services will ensure the information security responsibilities of both employees and contractors relating to PCI-DSS will be adequately disseminated to all parties and relevant staff trained (PCI-DSS Requirement 12.4)

Establish, document, and distribute security policies	IT Technology & Services Manager / SIRO
Monitor, analyze, and distribute security alerts and information	IT Technology & Services Manager / SIRO
Establish, document, and distribute security incident response and escalation policies	IT Technology & Services Manager / SIRO
Administration of user accounts on systems in the cardholder data network	Service Managers Policed by Internal Audit
Monitor and control all access to cardholder data	Service Managers

171 Responsibilities of information security for PCIDSS are formally assigned to a specific individual(s), position, or team. (PCI-DSS Requirement 12.5)

- This obligation for the Council will be shared by the SIRO/Accountancy/CICTS.

172 Responsibility of distributing the updated information security policies and procedures must be formally assigned to a specific individual(s), position, or team. (PCI-DSS Requirement 12.5.1)

- This obligation for the Council will be undertaken by CICTS.

173 Responsibility to monitor, analyze, and distribute security alerts and information. (PCI-DSS Requirement 12.5.2)

- This obligation for the Council will be undertaken by CICTS and Accountancy.

174 Generate detailed documentation security incident response and escalation procedures and formally assign the responsibility of creating and distributing these procedures to a specific individual(s), position, or team. (PCI-DSS Requirement 12.5.3)

- This obligation for the Council will be undertaken by CICTS and Legal.

175 Responsibility to administer users in the cardholder data network. Includes all additions, deletions and modifications to user access. (PCI-DSS Requirement 12.5.4)

- This obligation for the Council will be undertaken by Services & Accountancy.

176 Responsibility to monitor and control all access to sensitive cardholder data. (PCI-DSS Requirement 12.5.5)

- This obligation for the Council will be undertaken by Services & Accountancy.

177 A formal security awareness program must exist and participation is required for all employees working within the cardholder data environment. (PCI-DSS Requirement 12.6.1)

- This obligation for the Council will be undertaken by CICTS & Accountancy.

178 **Policies for Sharing Data with Service Providers:**

If cardholder data is shared with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), the following policies and procedures must be followed:

- Services must maintain a documented list of any service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network. (PCI-DSS Requirement 12.8.1)-*
- Any written agreement with a service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network, must include an acknowledgement of the service providers responsibility for securing all cardholder data they receive from the Council. (PCI-DSS Requirement 12.8.2)
- Prior to engaging with a service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network, Services will conduct due diligence and follow an established process to ensure that the security of cardholder data within the service providers network has been addressed. (PCI-DSS Requirement 12.8.3)
- Services will have an ongoing program to monitor the PCI DSS compliance status of any service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network. (PCI-DSS Requirement 12.8.4)

18. National Fraud Initiative Worker Compliance (Applicable to Staff using the NFI Service).

179 **User Accounts and Clearance:**
All staff using the NFI Service will undergone appropriate pre-employment screening checks to ensure that the threat to the system or the information is mitigated as far as possible. This includes any subcontractors, 3rd parties or temporary staff that will be using the system on behalf of the organisation.

180 It is recommended that the following standard (or equivalent) is adhered to: HMG Baseline Personnel Security Standard (BPSS) which covers:

An identity check;
Nationality and immigration status check (including an entitlement to undertake the work in question);
Employment history check (past 3 years including a reasonable account of any significant period of time spent abroad); and
Criminal record check (unspent convictions only).
(A BPSS check can be arranged via HR.)

181 The Audit Commission will be notified, via nfiqueries@audit-commission.gsi.gov.uk, if there are any deviations from the recommended standard.

182 Only authorised staff will access the NFI system.

183 Audit and Fraud Investigation Managers will ensure that when an NFI user leaves the Organisation, their NFI account is removed immediately.

184 Restrictions to information sharing:
Information sharing is to be strictly limited to authorised individuals who need to know it for the purposes of their necessary business duties. Staff must not share their account with or disclose their password to anyone.

185 Staff must not deliberately misuse the NFI system or attempt to use any facilities for which they do not have any authorisation.

186 Staff must abide by the Code of Data Matching Practice and supporting documentation including the current NFI Guidelines and any associated guidance notes.

187 All staff users will note the Audit Commission reserves the right to monitor and log all traffic on the NFI system and infrastructure.

188 System Security Policy:

Incident Management and Reporting.

All incidents that have a direct impact or may have an indirect impact on the NFI system must be reported to the Audit Commission NFI team immediately on nfiqueries@audit-commission.gsi.gov.uk.

Examples of incidents include (but are not limited to):

Unauthorised access to the NFI system;
Virus outbreaks that may impact the NFI system or data;
Inadvertent release of information to an unauthorised entity;
Corruption of data or unexpected access to data, or;
Deliberate or accidental sharing of NFI account's or passwords.

189 End Point System Security:

The Council's Fraud Investigation Team and Internal Audit are responsible for the security of all information viewed or extracted from the NFI system and is responsible for ensuring appropriate security controls are implemented to protect that information. The Audit Commission is only responsible for the security of the information when it resides on the NFI system and is not responsible for the security of any end-point systems that view, extract or upload the information on the portal.

190 The Audit Commission will maintain the accreditation of the NFI system so that it provides appropriate security measures to handle information up to a level of Impact Level 3 aggregating to Impact Level 5 covering information with a protective marking of OFFICIAL. OFFICIAL-SENSITIVE where the caveat is used to cover sensitive personal information can also be processed by the system.

191 The Organisation shall ensure that procedures and system security controls are in place relating to information disclosed for data matching that reflect the provisions in the Code, the Data Protection Act 1998 and any applicable HMG Standards. These procedures and controls should:

Make accidental compromise of, damage to or loss of the information unlikely during storage, handling, use, processing, transmission or transport;
Deter deliberate compromise or opportunist attack;
Dispose of or destroy information in a manner to make reconstruction unlikely; and
Make access to the NFI system and its data by unauthorised personnel unlikely.

192 Staff must only transfer data to the Audit Commission data systems by secure data transfer through the online portal or, if approved by the Audit Commission, the PSN network.

193 The Organisation will ensure that NFI data exported from the NFI environment is stored on an appropriately secured system.

194 Information loaded into NFI:

Internal Audit and the Fraud Investigation Team will ensure that:
all data loaded into the NFI is as accurate as possible and where possible that it has been scanned for malware prior to upload;

Data is password protected in line with the NFI policy;
Data does not exceed an impact level of 3 for confidentiality (in line with HMG IA Standard No.1&2: Business Impact Level tables) or protective marking of OFFICIAL (including OFFICIAL-SENSITIVE); and
The Audit Commission are informed immediately if the impact level for any of the Organisation's information rises above this level.

195 Threat Levels:

If the threat levels posed to the Organisation's information increase or if the Organisation is informed of a particular threat to their information within the NFI system, the Audit Commission must be informed immediately, via nfiqueries@audit-commission.gsi.gov.uk.

19. Use of Skype and other presence messenger services

196 Currently Skype is only allowed on a bookable laptop requested via the Northgate ServiceDesk (Ext 72861). This laptop has to connect over the Council's GUEST Wifi network. This will be relaxed for Skype for Business/Teams upon the roll-out of Microsoft Office 365 and will then be allowable across the corporate network.

197 All Staff and Councillors are expected to behave in a responsible and professional manner whenever using Skype and other presence messenger services. This includes the sharing of any inappropriate material (video content, jokes, images, non-work related documents, non-work related documents or any content you do not have permission or work related need to be sharing, emoticons etc).

198 As these services consume bandwidth on the Network these services should be restricted to work related purposes only.

199 You should register your RBC Email for the business account reference for Skype.

200 Please ensure appropriate consideration is given to your location and the Potential disruption when used in open plan offices. We would recommend purchasing separate headsets for this reason when using these types of services to avoid office disruption.

201 Please give consideration to who and what can be seen in the operation of the camera for the session. Where possible limit this to a neutral enviornment not involving others or any sensitive information displayed on wall boards etc.

202 If operating in a public place please becareful from a Security perspective of what people can oversee and hear being discussed. Confidential discussions should only take place in a private setting.

203 Please ensure any Skype of Messenger services are operated in accordance with PCI DSS and Data Protection requirements. This specifically means you should not give control of the screen to any third party when operating PCI DSS processes, or allow control that may access Sensitive protected data.

204 As with all electronic contact channels you should be aware of potential Social Engineering and Phishing attacks so challenge yourself you know a contact source is genuine and who they say they are before revealing information.

205 As video does consume network bandwidth it may be necessary in areas of poor network coverage to run as voice only.

206 As this service is only allowed on a business use basis, please be aware the Council reserves the right to inspect any associated log files as part of any investigation.

20. Appendix 1 – Security Responsibilities

Computer User's Security Responsibilities

207 If you use a Council computer system then you have the following responsibilities.

208 **Under no circumstances is any non-Council-owned equipment to be connected or installed to the Council IT computer network (with the exception of the public wireless facility) or any Council-owned computer, or for any software to be installed without the consent of the ICT Service Desk.**

1. You will have a log on account which is unique to you and which you must not let anyone else use. You will reload your computer on a regular basis to activate software security patches.
2. You will maintain a password as set out below which you will not allow anyone else to use (access to other people's data through your own account may be arranged through the ICT Service Desk in exceptional circumstances)
   - In all cases any passwords given to you personally are for your use only. Passwords should not be written down in an insecure location or given to others under any circumstances.
   - Passwords should be a minimum of 9 characters and should be a combination of seven characters and one number as a minimum, ideally 8 characters comprising of upper and lower case, numbers and random characters such as #@?!$& etc.
   - Do not use family or pet names and if at all possible try not to use proper words.
   - Your passwords must be changed if you ever suspect it has been compromised.
   - Please do not reuse passwords you use at home.
3. You must report any suspected tampering with your log-on accounts to your head of department and the ICT Service Desk.
4. You must not load any private programmes or games onto any Council owned ICT equipment.

5. You must not load any other software (other than data) without the express permission of the ICT Service Desk.
6. No unauthorised private work/projects are to be carried out on the Council's devices.
7. All data disks and all files from any source (including e-mail) must be virus checked prior to being used. Please contact the ICT Service Desk for assistance with virus checking.
8. All data to which you have access during the course of your work is to be treated in strict confidence and its accuracy must be maintained.
9. You must not access information unless your job specifically requires it.
10. You must abide by the terms of the Data Protection Act 2018 (GDPR) and the Computer Misuse Act 1990.
11. Do not store personal data or other confidential data on portable ICT equipment which is taken out of the office and/or will be left insecurely unattended.
13. Any Personal Identifiable Data (PID) sent via e-mail must be sent in an encrypted format which meets the Council standards. Standard, non-encrypted e-mail must not be used. If you need to request a secure e-mail account, please contact the Corporate ICT Service.
14. No Council files are to be transferred to any home PC for working at home. The Council secure VPN system is to be used for this purpose.
15. Use must ensure any equipment or data losses are treated as security incidents and reported to the Northgate Service Desk (ext 72861). Under GDPR the Council has 72 hours to report to all affected stakeholders any data breach and what action has been taken to recover the position.
16. You will be careful not to take unnecessary risks when click on links or opening attachments in emails sent from external sources. If in doubt on the authenticity of an email check with your Manager or the Northgate Servicedesk.

209 **Failure to carry out these responsibilities will be treated as a serious matter and may result in disciplinary action.**

Line Manager's Security Responsibilities

210 As a line manager responsible for other staff you have the following responsibilities in addition to those you have as a user.

211 **Under no circumstances is any non-Council owned equipment to be connected or installed to the Council computer network or any Council owned computer, or any software to be installed without the consent of the ICT Service Desk.**

212 You are not permitted to give any local exemptions to this policy. All exemptions must be issued and agreed by CICTS. Specifically:

1 You must maintain a record of the access rights your staff have to line of business applications where these are granted by someone other than the ICT Service Desk. As a minimum, this should include: user's name, access rights granted, data granted, date rescinded.

2 You must notify the ICT Service Desk or the manager responsible for particular computer systems of any changes of staff (i.e. joiners and leavers) and what levels of access you require your staff to have to the various systems.

3 You must notify the ICT Service Desk of any starters and leavers where these staff have access to any ICT equipment.

4 You must ensure that all your staff are aware of their responsibilities and that they carry them out. Any breaches must be treated as serious and be reported to the ICT Service Desk or in the case of serious breach to the Monitoring Officer or ICT Manager.

5 You must only provide staff with the minimum access required to carry out their duties.

6 You must ensure that all your staff are aware of their responsibilities and have the appropriate training before they are allowed access to the Council's computer systems.

7 You must set an example to all your staff in your conduct and attitude towards computer use and security.

8 You are to ensure that staff who work on Council information at home do so in accordance with this policy.

9 You must ensure that mailboxes for staff who are away from the office due to unplanned sickness are monitored as required for their role.

10 You must ensure all equipment and data losses are reported as security incidents to the Northgate ServiceDesk (Ext 72861).

11. You must ensure Privacy Impact Assessments (GDPR) are undertaken when your service process changes, along with the publication of Fair Processing Notices where applicable for your service.

213 **Failure to carry out these responsibilities will be treated as a serious matter and may result in disciplinary action or action under the Member Code of Conduct for councillors.**

Chief Executive, Directors and Assistant Director Security Responsibilities

214 As a Director or Senior manager in addition to your responsibilities as a computer user and a line manager user you must also:

1. Ensure that your line managers are implementing this security policy.
2. Set an example to all your staff in your conduct and attitude towards computer use and information security.
3. Properly investigate and implement remedial measures where appropriate for any reported Security Incident reported regarding your service.
4. Ensure appropriate Risk Management reviews and Privacy Impact Assessments are undertaken following any significant changes to your services.
5. Ensure the following key roles are in place and adequately trained to discharge their duties:

    Senior Information Risk Officer (SIRO)

    Data Protection Manager

    ICT Security Manager

    Caldicott Guardian

    Information Asset Owners

6. Ensure Information Governance responsibilities are set out in Job Descriptions so all staff know their responsibilities and roles.
7. Ensure sound Information Governance Processes are embedded soundly into the Council and Information Assets are appropriately protected.
8. Ensure appropriate Information Governance and Security Induction training and guidance is in place for Councillors and staff.

215 **Failure to carry out these responsibilities will be treated as a serious matter and may result in disciplinary action.**

21. Appendix 2 - Use of E-mail and Calendar

216 Outlook is a useful tool that enables individuals to organise themselves and communicate with others. This policy sets out the expectations for all RBC computer equipment users who are provided with access to Outlook. Outlook is provided as a business tool and should not be used for non-work related matters. Individuals with a need to send personal mail during working hours must do so using personal webmail accounts (such as Hotmail or Google-mail). All users must be aware of the emerging threats from Social Engineering, Phishing, Malware, Ransomeware and Viruses and be especially vigilant in not opening any supsicious unsolicited emails, or clicking on internet links in unsolicited emails.

20.1 Mailbox Size and Housekeeping

217 The standard individual mailbox size provided is 100mb. There will also be unlimited archive space when e-mail archiving is introduced[3]. In addition to individual mailboxes, shared mailboxes can be provided where there is a specific business need. Please contact the ICT Service Desk for assistance. Each mailbox will have a designated owner who will be responsible for housekeeping (archiving or deletion) all types of Outlook items. Once the mailbox limit is reached, users of that mailbox will not be able to send or receive any further mail and therefore housekeeping must be planned well in advance of reaching the space limit.

20.2 Distribution Lists

218 Mail distribution lists are provided to enable business communications to be made to groups of individuals, and each list must have a designated owner. Lists should only be used for related business purposes, and any queries related to their use or composition should be directed to the list owner in the first instance. All Staff and Councillors should take particular care in the selection of distribution lists and ensure associated content is suitable for onwards transmission to the full list of recipients in the distribution list especially where these are external contacts. Secure email must be deployed if sensitive information is sent externally via the

[3] A Corporate archiving system will shortly be introduced for all staff.

use of a distribution list. For risk management reasons, distribution lists that reference external contacts should be avoided wherever possible in the General Address List to avoid the risk of accidental selection and onwards email transmission to unintended recipients.

20.3 Mailbox Management

219 Individuals are expected to treat their mailbox like an electronic in-tray, ensuring that it is regularly checked and that messages requiring further action are dealt with promptly – including sending holding responses where appropriate.

220 Individuals should only archive and retain messages that need to be kept and these should be selected in line with business needs and any corporate retention schedules that may exist. All other e-mail that does not constitute a necessary record of business should be deleted once it is no longer required.

20.4 Sending E-mail

221 E-mail is set up by default to conform with RBC branding and house style, and a corporate disclaimer is applied to all outgoing messages. Individuals must use the default settings and not make changes to the disclaimer. All e-mails must have the subject line completed and should be checked for accuracy of spelling, punctuation and grammar. Bold text should only be used sparingly, and for emphasis, and underlining should only be used for links. The use of upper case text should be avoided as this may be interpreted by recipients as shouting.

222 To avoid information overload, individuals should consider carefully who needs to be included in any e-mail and whether face-to-face or telephone contact could be an alternative method. When sending confidential or sensitive e-mail Individuals should be mindful of any delegate permissions that recipients may have set up.

223 Individuals must not alter the text of any received messages, including when forwarding them to others. Similarly, individuals should not assume that a forwarded message matches what was originally authored.

224 Individuals must not use others people's mail accounts nor attempt to impersonate someone else or appear anonymous when sending e-mail.

225 For full guidelines on considerations when communicating by e-mail, please see the Communications Handbook (chapter 7, section 3).

20.5 Agreements by E-mail

226 Individuals should take care not to enter into any agreements via e-mail that could constitute a contract unintentionally, and if in doubt must seek the advice of RBC's legal and procurement advisors.

227 Where the text of an e-mail or any attachments are deemed to need specific marking to indicate that they are confidential or commercial (protectively marked), this should be clearly flagged at the top of the e-mail.

20.6 Misuse of E-mail

228 Individuals must not send or forward any abusive, threatening, defamatory or obscene messages. Likewise individuals should avoid sending messages in the heat of the moment, taking time to reflect on drafts and how they may be interpreted before sending them.

229 RBC has spam filtering software in place to help reduce the volume of unsolicited e-mail. However, such software is not infallible and individuals should therefore take care with any suspected malicious or nuisance e-mails (e.g. chain e-mail, hoax and spam e-mails) they receive, ideally deleting them. Individuals must also never open attachments to an e-mail of unknown origin as they may contain viruses and other malware.

20.7 Mail and Absence

230 The "out of office" notice must be used whenever an individual is away from their normal office base, and messages should clearly indicate a date of return and contact details for those who can deal with issues whilst the individual is away. Full guidelines can be found in the Customer Care Handbook (chapter 7, section 4).

Individuals with a Blackberry should note that they can turn on or switch off out of office using their Blackberry.

231 In the event of an unforeseen absence where there is a need for the "out of office" function to be turned on, the line manager should provide the ICT Service Desk with the required text.

232 To protect individual privacy, access to other individuals' mailboxes is not normally provided. Where there is a business need for emergency temporary access, this can be provided with the individual's explicit written consent. In the absence of consent, the manager should contact the ICT Service Desk for advice. The ICT Service Desk will not be able to arrange access without sight of the written advice from the Council's data protection adviser.

20.8 Calendar

233 In order to help with setting up meetings and locating colleagues, calendars will be set by default to be viewable by all RBC Outlook users. Consequently, it is important that individuals use the "private" option for all confidential appointments. If you are unsure how to do this, please contact the ICT Service Desk. It is acknowledged Councillors may wish to operate an off-network electronic diary to facilitate single source diary management (which includes ward work) and is allowable under this policy.

234 Individuals are required to keep their calendars up to date, and must indicate their whereabouts when away from their normal office base.

20.9 Attachments

235 Attachments should not be included in any internal mails or meeting invites wherever it is possible to use a link to a document instead. Care should always be taken to ensure any sensitive attachments are appropriately protected by Secure Email when sending to external email addresses.

20.9 Signatures

236 All staff must adhere to the Corporate Style for email Signatures to aid communciations within the Council and externally with Partners.

Format should include the follow Information:

Name

Job Title

Team/Service/Directorate

Address

Landline telephone number / extension

Mobile Telephone Number / mobex

RBC Email addresses

RBC Logos

Document Marking advisory

Example:

John Smith
ICT Project Manager
CICTS | Corporate Support Services

Reading Borough Council
CICTS Floor 1
Civic Offices
Bridge Street
Reading
RG1 2LU

0118 937 2869 (72869)
0796 613 3869 (83869)

Email:John.Smith@reading.gov.uk

Website | Facebook | Twitter | YouTube

Reading Borough Council
Working better with you

Please Note that Public Sector Protective Document Marking is in operation. All sensitive emails and documents originating from Local Authorities should be marked OFFICIAL or OFFICIAL-SENSITIVE. Documents & emails unmarked are to be treated with usual professional courtesy. Those marked OFFICIAL are to be circulated with consideration. Those marked OFFICIAL-SENSITIVE should usually be circulated only to those the author has included in the send field. Secure email will also be used as an additional control measure where applicable for OFFICIAL and OFFICIAL-SENSITIVE external emails.

Appendix 3 – References

21.1 Related Policies and Documentation

- Information Sharing Code of Practice
- Document Retention Schedule
- Information Asset Ownership
- Document Marking Policy
- ICT Security Policy Statement
- ICT Information Risk Management Document Marking Policy
- ICT Standards Expected of Third Parties Policy
- ICT Email Monitoring Policy
- ICT Internet Monitoring Policy
- ICT Camera and Video Usage Policy
- ICT Huddle Acceptable Use Policy
- ICT GlassCubes Acceptable Use Policy
- ICT Removable Electronic Media Usage Policy
- ICT PSN Personal Commitment Policy
- ICT PCI DSS Personal Commitment Policy
- ICT Security Golden Rules
- ICT Controls for Storage & Carriage of Hardcopy Documentation
- Data Protection Policy application
- Freedom Of Information Policy
- Incident Reporting
- Disciplinary procedure and rules
- Whistleblowing Policy
- Grievance and Disputes procedure
- Records Management Policy
- The Code of Conduct
- RIPA (Regulation of Investigatory Powers Act) guidance
- Data protection policies, including subject access request procedures
- Information sharing policies
- Customer Care Handbook

- Equality and diversity procedures
- Joiners & Leavers process
- RBC Breach Management Procedure

21.2 Legal References

- Computer Misuse Act 1990
- Data Protection Act 2018 (GDPR Revision)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Human Rights Act 1998
- Regulation Of Investigatory Powers Act 2000

This list is not exhaustive and may be subject to additions or deletions to be approved by the Council from time to time.

21.3 Regulations - Guidance

CoP 45	Code of Practice On The Discharge Of Public Authorities Functions Under Part 1 Of The Freedom Of Information Act 2000
CoP 46	Code of Practice On The Management Of Records Issued Under Section 46 Of The Freedom Of Information Act 2000
ISO27001/2013	International Standard for Information Security Management

These lists are not exhaustive and may be subject to additions or deletions to be approved by the Council from time to time.

22. Appendix 4 – Information Security Incidents

Information Security Incidents should be reported in accordance with the Council's Security Incident Policy which classifies the type of security incident and ensures appropriate notification of relevant parties including CICTS, Legal SIRO, Data Protection Manager and external organisations set out in the PSN Code of Connection (GCSX).

Security Incidents should be reported to the Northgate Service Desk (Ext 72861) by telephone call or Web Form (IRIS) at the earliest opportunity.

Additional detail relating to loss of data must be recorded using form below and attached to call or sent separately to council's SIRO (Legal Section).

READING BOROUGH COUNCIL

INFORMATION SECURITY

REPORT OF LOSS OF DATA
Data lost: *Describe the data that has been lost – including its level of security.*
What happened? *Describe how the data was lost – give specific details of how/when you realised the data was lost, and what actions you took to recover or cancel it.*
Who lost the data: *Name and post of officer holding the data.*
When was it lost? *Date and time of loss. GDPR requires all parties to be informed within 72 hrs including time lapse over w-e's.*
Where was it lost? *Give precise location.*
Which individuals are affected by the personal data breach? *Include the approximate number of individuals concerned.*
How are the individuals likely to be affected by the breach? *An assessment of the risks to the individual form the nature of the data lost.*
Who received it? *Give information about any steps taken so far to retrieve the data from them*
Security of Data *Describe how the data was stored*

Was the data encrypted?
Action taken ***What have you done since the incident to manage and communicate the situation?***
Has the lost data been recovered/destroyed? *Give details of any steps taken to confirm that the lost data has been recovered or destroyed by ay third parties who received it*
Data Protection Training: *Has the individual who lost the data attended the mandatory Data Protection Training whilst at RBC, if so when did they attend*
Information Asset Owner: ***Who is the business owner responsible for the data (normally HOS unless formally delegated).***
Management Action Taken: *What Management Action has been taken to manage the incident?*
Notification to Others: □ **Data Protection Mgr** **Date ……** □ **Head of Service** **Date ……** □ **Monitoring Officer** **Date ……** □ **Internal Audit** **Date ……..** □ **Head of IT** **Date ……..**
Signed: **Date:**

End of Document