Reading
BOROUGH COUNCIL

READING BOROUGH COUNCIL

ICT USE
&
INFORMATION SECURITY POLICY

July 2007

Version No.	Date	Change Description	Approved By
1.1	March 2007		ISMF; Personnel Committee
1.1	July 2007	Launch	

All revisions agreed by the Councils Information Security Management Forum and Personnel Committee will be notified to employees and organisations as identified within this Policy Statement.

Reading
BOROUGH COUNCIL

ICT USE AND INFORMATION SECURITY POLICY

CONTENTS: PAGE

1. INTRODUCTION

This policy sets out a framework on the **permitted and prohibited** use of the Council's electronic systems – a definition which includes all computer systems as well as the Council Intranet, Internet and e-mail systems, mobile telephones, PDAs etc.

It is intended to help and guide all users of Council's ICT facilities as to acceptable and unacceptable use. For Council employees this will constitute an addition to the Council's Code of Conduct and therefore it should be stressed that the requirements and restrictions in this policy, if breached, could lead to disciplinary action in accordance with the Council's existing procedures for dealing with such matters.

The associated **ICT USE AND INFORMATION SECURITY - ADDITIONAL INFORMATION AND GUIDANCE** document has been produced which gives staff and managers advice on **'best practice'** in electronic systems usage as well as guidance on e-mail and Internet etiquette and **'housekeeping'**. This associated document has been developed to assist all staff to make more effective use of the systems and equipment currently available and may also be used as a framework for discussion between managers and staff/teams on appropriate or acceptable methods of working.

This policy has been agreed between the Council and its recognised trades unions and constitutes an incorporated term of individual contracts of employment.

This policy will be reviewed annually by the Information Security Management Forum and revisions communicated to employees and key organisations as defined in this document. Any change to the policy will be taken through normal consultation routes and approved through Personnel Committee.

2. PURPOSE AND SCOPE OF THE POLICY

2.1 The **purpose** of this policy is –

a) To provide guidance to users of the Councils electronic information systems on acceptable and unacceptable use of these systems and related equipment.

b) To facilitate effective and efficient use of ICT Assets and specifically:

- Protect all staff against the downloading and/or dissemination of offensive images and writing

- Ensure that private use of these systems and equipment does not hinder the effective working of members of staff and the service that they are employed to provide

- Ensure that the systems and equipment are kept secure from attack from any external and internal source

- Keep the systems working at optimum efficiency and performance levels

- Protect the Council from legal action arising from misuse as well as liability for the actions of its employees and 3rd parties

c) Encourage the skills, confidence and development of staff to use the Council's ICT facilities within the context of achieving the Council's overall business objectives.

2.2 Scope

2.2.1 Policy Application

This policy, as amended from time to time, applies to all employees of Reading Borough Council whether full or part time and whether working at Council offices or remotely, unless (in the case of schools based staff) a specific alternative local policy has been formally agreed and communicated to relevant staff replacing parts of or all of this document. This document will form part of the contract for services for agency or contract staff. This document will also apply to other third party organisations using the Council's ICT facilities unless specific alternative terms have been agreed.

2.2.2 Exemptions

If an employee or contractor's job role requires exemption from any part of this policy, this must be authorised by the relevant Head of Service and permission sought from the IT Programme and Service Delivery Manager. The application and permission should be recorded on the individual's personal file (RBC HR) or sent to the relevant third party organisation.

2.2.3 Personal Use – Condition of Use

Personal use of the Internet and Internet email (Yahoo recommended) is allowed at the discretion of the Council and may be withdrawn at any point. Any personal use is undertaken at the employee's own risk and the Council cannot be held accountable for any problems or consequential losses that may result from an employee's own personal transactions. Any personal use must be conducted in accordance with this policy.

3. Specific Policy Sections

Each of the following sections 3.1 to 3.7 includes all or some of the following instructions / advice:

REQUIRED:

✓ Describes the actions and behaviours REQUIRED of staff and managers. Failure to comply will indicate a breach of this policy which may render staff liable to investigation and action under the Council's Disciplinary Procedure.

ACCEPTABLE:

👍 Indicates ACCEPTABLE behaviours or use of facilities, services and equipment, although particular permission will often need to be sought (this will be specified).

UNACCEPTABLE:

👎 Indicates UNACCEPTABLE behaviours or use of facilities, services and equipment. Such breaches of this policy may render staff liable to investigation and action under the Council's Disciplinary Procedure.

FORBIDDEN:

✘ These actions and behaviours represent more serious breaches, where it is difficult to envisage any circumstances in which they may be justified. Such breaches may be considered as gross misconduct under the Council's Disciplinary Procedure and staff are at risk of dismissal.

OTHER INFORMATION YOU SHOULD REFER TO:

ⓘ Cross references to additional guidance, advice, information. In particular, reference to the associated 'ICT USE AND INFORMATION SECURITY - ADDITIONAL INFORMATION AND GUIDANCE' document.

3.1 GENERAL USE OF ICT INFORMATION, DATA, EQUIPMENT, RESOURCES AND SERVICES

REQUIRED

✓ This ICT Use and Information Security Policy is incorporated into each employee’s contract of employment, conferring rights and responsibilities. This policy and associated key guidance must be read before using any ICT services. Failure to comply with the policy could lead to disciplinary action being taken against the employee, which could lead to dismissal, and in some cases could lead to legal action.

✓ Employees are responsible for maintaining their awareness and complying with this policy and line managers are responsible for monitoring compliance.

✓ Any employee discovering a breach of this policy, or who is in receipt of an electronic mail or telephone call that appears to contravene the policy described below, should raise the issue with their line manager in the first instance. Where the concern or issue persists and cannot be resolved within the departmental management structure, the matter may be escalated to the ICT Programme & Service Delivery Manager, the Head of HR, Head of Legal Services or the Head of Internal Audit.

✓ Data Protection - The Data Protection Act 1998 puts certain legal obligations on the Council for the recording and storing of personal information. As an employee of the Council who uses our ICT facilities, you will almost inevitably be involved in processing personal data for the Council as part of your job. Data protection is about the privacy of individuals, and is governed by the Data Protection Act 1998. All employees are responsible for storing, accessing, recording and using data in accordance with the legislation and Council instructions, advice and guidance. An outline of the requirements is set out in the associated guidance document ‘ICT Use and Information Security Policy - Additional Information and Guidance.’

✓ Starters and Leavers - Directorates are responsible for notifying ICT service providers of new employees and those that are leaving. Responsibility rests with line managers to ensure that all appropriate notice is given, and all required forms completed. Managers must refer to the Additional Information and Guidance document on starters and leavers.

✓ Third Party ICT Services - Directorates must involve ICT Client and Directorate ICT Teams when considering changes to their IT Service requirement. Third Party Suppliers must be sent the Council’s Policy Document - “Standards Expected of Third Parties” as part of the contractual documentation issued by the Council to ensure compliance with required Council ICT Standards.

✓ Purchase of ICT Equipment and Software - ICT Equipment should be purchased under the Corporate ICT Outsourcing Contracts unless agreed otherwise with IT Client and Directorate ICT Teams.

✓ Compliance with Programme and Project Standards - Employees will follow Corporate ICT Programme and Project standards when involved in any ICT Project. Third Parties must also comply with these standards whenever working on ICT Projects for the Council.

✓ Contract Advice - Employees should contact the IT Client Contract Manager on any performance problems or contractual issues relating to ICT Contracts.

✓ Turn Off - Employees should turn off personal IT equipment when not in use.

ACCEPTABLE

👍 Whilst ICT services are provided for Council business only, it is recognised that employees may reasonably carry out some personal tasks during working hours (although not in recorded work time). In all cases, you must ensure that such use at the Council's discretion:

- does not compromise the Council's ICT security infrastructure;
- does not interfere with the performance of your duties;
- does not take priority over your work responsibilities;
- does not cause unwarranted expense or liability to be incurred by the Council;
- does not contract the Council to goods or services procured by personal use;
- does not have a negative impact on the Council in any way;
- is lawful and complies with this policy.

FORBIDDEN

✘ Employees must not use any Council ICT services for copying, storing, sending, knowingly receiving or retrieving unacceptable material. "Unacceptable material" includes any documents, messages, information, graphics, music, pictures, video or other electronic data that:

- Breach UK legislation;
- Contravene the Council's Equality Policy;
- Contain offensive, pornographic, sexist, racist, obscene language or material;
- Contain material subject to copyright not owned by the Council;
- Plan, promote, incite or facilitate any illegal or terrorist activities;
- Contain defamatory or slanderous language or material;
- Denigrate, insult or ridicule another person;
- Intimidate, bully or harass another person;
- Adversely comment on the integrity, personality, honesty, character, intelligence, methods or motives of another person unless it is a factual response to a formal reference request;
- Provide or facilitate the use of computer hacking tools or virus toolkits.

(Material received, gathered or sent genuinely and necessarily in the course of work duties (e.g. pictures of offensive graffiti) will be exempt from this restriction).

✘ Employees must not use the Council's Internet, external electronic mail, external telephone or mobile, fax or any other form of electronic communication intentionally to transmit sensitive or subversive information, contrary to the Employee Code of Conduct.

FORBIDDEN (Continued)

✘ When using the Council’s ICT services for personal use at the Council’s discretion, employees must not knowingly:

- Undertake electronic processing relating to commercial or political activities;
- Import or download documents, data or software from other devices or sites;
- Undertake any activities that could potentially reduce the security of Council systems and data;
- Save large amounts of personal data (e.g. personal picture files) to the council’s network drives (employees should note that there is no right to privacy of personal information on the Council’s systems);
- Undertake to operate or manage any business other than that of the Council or an agreed client of the Council, or undertake activities for private gain;
- Misrepresent the Council Logo for your own gain;
- Gain unauthorised access to external networks and systems.

✘ Employees must not procure ICT goods, services or ICT staff outside of the Councils ICT Outsourcing Contracts without the agreement of ICT Client and Directorate ICT Teams.

OTHER INFORMATION YOU SHOULD REFER TO:

ⓘ Data Protection - Section 1.1 ‘ICT Use and Information Security Policy - Additional Information and Guidance’ document.

ⓘ Intellectual Property Rights - Section 1.2 ‘ICT Use and Information Security Policy - Additional Information and Guidance’ document.

ⓘ Starters and Leavers - Section 1.3 ‘ICT Use and Information Security Policy - Additional Information and Guidance’ document.

✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷ ✷

3.2 System and Network Security and Passwords

REQUIRED

✓ Reading Borough Council’s computer network is only as secure as the passwords in use. All staff should ensure that they adhere to this policy to ensure the safety and security of the network, and thus any data stored on the network.

✓ Corporate IT is responsible for establishing and enforcing a password policy on the Council’s networks, Internet, Intranet and e-mail systems. Application system owners are responsible for establishing and enforcing a password policy on their systems based on the level of security required. For each computer system that has its own acceptable password policy, this must be complied with by all users of that system.

✓ Employees must be aware of the importance of ensuring that all passwords to our systems remain secret. All employees that require access to the Council’s computer network will have passwords. There is a considerable amount of sensitive information contained in the Council’s systems and every effort must be made to ensure that the Council's systems do not become compromised.

✓ Employees must protect their passwords as they will be held accountable for all activities undertaken under their usernames. Employees must keep their passwords private and where written down must as far as possible be kept in a secure location such as a locked filing cabinet, safe or cash box, or effectively disguised. Other advice on choosing and securing passwords is included in the associated ‘ICT Additional Information and Guidance’.

UNACCEPTABLE

Managers should agree arrangements for reasonable access to employees’ work related information at times of absence.

👎 Other than this, employees must not…

👎 …use the username and password of another employee, share or allow others access to passwords; or let others know their passwords (this excludes shared usernames where issued or authorised by the Council).

👎 … give any person not employed by the Council access to any computer system (including via a laptop or mobile device) without management authorisation. (Managers are responsible for getting ICT Client authorisation for non-employees, drawing this policy to their attention and monitoring use).

👎 … set up any remote access facilities to any Council computer system or network other than through the approved corporate arrangements for home / flexible working.

👎 … use windows functionality to remember and pre-fill passwords to any Council system (thereby negating the security of that system).

FORBIDDEN

✘ Employees must never attempt to gain unauthorised access to other computers, networks or information either within or external to the Council. In the UK this is an offence under the Computer Misuse Act.

✘ Employees must not:

- damage or compromise the integrity of any computer system;
- subvert any system that controls or monitors access to a computer system;
- exploit known, published security flaws to bypass security and systems to access data
- deliberately obtain unauthorised access to systems whether internal or external, deliberately attempt to disguise the identity of the user
- seek to gain access to restricted areas of the Council's network or access or try to access data which you know or ought to know is confidential
- seek to monitor or intercept electronic files or messages (other than where specifically authorised in your job role)
- knowingly allow any unauthorised 3rd party access to any computer system

✘ In particular, employees must not deliberately and knowingly:

- introduce or download software used for hacking or cracking passwords
- introduce any form of computer virus
- carry out any hacking activities or unauthorised monitoring activities
- disclose Council security information to third parties

OTHER INFORMATION YOU SHOULD REFER TO:

ⓘ System & Network Security & Passwords - Section 2 'ICT Use and Information Security Policy - Additional Information and Guidance' document.

✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵

3.3 Electronic Mail (e-mail)

REQUIRED

✓ Employees must use the Council's communications facilities professionally, sensibly, lawfully, consistently with your duties, with respect for your colleagues and in accordance with this policy and the Council's Customer Charter.

✓ Employees who are authorised to use e-mail to complete transactions (e.g. transfer funds) or provide references of a personal nature (e.g. employment, financial, medical) must seek and comply with local management instructions to ensure authenticity and confidentiality.

✓ Other than for normal day-to-day use, employees should expressly agree with the recipient that the use of e-mail for confidential, privileged or commercially sensitive material is an acceptable form of communication bearing in mind that un-encrypted e-mail is not secure. Secure email (Global Certs) must be used for email containing any personal data.

✓ Employees, when attaching documents to emails, should ensure sensitive documents where the content must not change from the original Council wording (especially those documents of a contract nature) are protected from unauthorised amendment by sending the document in a write protected format (e.g. Adobe .pdf).

✓ Employees are required to comply with, and follow, Council processes for processing Freedom of Information Requests and Data Protection Subject Access requests which are received by email.

ACCEPTABLE

👍 The RBC e-mail system/address should not be used for personal e-mail. However, employees may sign up to an E-mail Account accessed via your web browser (e.g. Yahoo) which may be used for sending and receiving personal e-mails (not work-related) providing this does not interfere with your work duties. The time you spend doing this will be monitored, and action taken if this use becomes excessive (the time will be included in the overall limit for personal surfing time - see section 3.4 Internet).

👍 By making personal use of the Council's facilities for sending and receiving e-mail you signify your agreement to abide by the conditions imposed for their use, and understand that the Council will monitor the duration of use (not content) of your personal e-mail in accordance with this policy.

UNACCEPTABLE

👎 Employees must not…

- 👎 … send irrelevant or inappropriate e-mail to mailing lists or bulletin boards e.g. jokes, images; …use the council's e-mail service to conduct e-mail "chatting" or participate in chain or pyramid letters or similar schemes;
- 👎 … use personal web based e-mail to send Council business e-mail. All official e-mail communications must come from @reading.gov.uk;

UNACCEPTABLE (Continued)

👎 Employees must not…

- 👎 … maliciously amend any messages received and, except where specifically authorised by the other person, must not access any other person's in-box or other e-mail folders nor send any e-mail purporting to come from another person;
- 👎 …delete e-mail to avoid disclosure under the Data Protection Act or Freedom of Information Act following receipt of a disclosure request;
- 👎 … subscribe or sign up to non-work related e-mail subscription services, mailing lists, response services, acknowledgements, newsletters using the Council's e-mail domain name address (@reading.gov.uk). If this has already occurred then the employee should unsubscribe and use a personal e-mail address instead;

👎 Employees should avoid the receipt of personal e-mail on the corporate e-mail account. You should encourage friends and family to use your personal (web-based) e-mail account. Employees should not e-mail personal documents to their own council account for the purposes of printing the e-mail or attachment (e.g. personal digital photographs). Emails of this nature will not be released from the corporate email filter.

FORBIDDEN

✘ Employees must not originate, reply to or forward e-mail containing unacceptable material (as defined in section 3.1) to internal or external recipients - to do so would render both the individual employee and the Council liable for the consequences. (Material received, gathered or sent genuinely and necessarily in the course of work duties (e.g. pictures of offensive graffiti) will be exempt from this restriction).

✘ To avoid a breach under the Data Protection Act under no circumstances should confidential, privileged or sensitive information be sent out as unsecured external e-mail (either in the main body of an email or in attached documents) without further security measures being used (e.g. use Council Secure Email Global Certs, or place content in word document with Zip encryption, Zip file password protection). Employees must seek further advice from the ICT Helpdesk (x 2861) if in any doubt.

✘ To avoid a breach of the Data Protection Act, employees must not email client records to a private email account to work on for any reason. All Client data must be held and managed by the Council or an approved agent of the Council. Employee's needing to work out of hours from home must use one of the Council's approved flexible home working solutions which can give controlled secure access to Council held data without downloading it to private PCs or laptops.

OTHER INFORMATION YOU SHOULD REFER TO:

ⓘ Electronic Mail (Email)- Section 3 -'ICT Use and Information Security Policy - Additional Information and Guidance' document (includes how to sign up to Yahoo mail).

✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵

3.4 INTERNET

REQUIRED

✓ The Internet should be used sensibly, in accordance with this policy and in such a manner that it doesn't interfere with the efficient running of the Council, or expose the Council to financial risk, or damage the reputation of the Council within the community or with its partners.

ACCEPTABLE

👍 The Council encourages employees to become familiar with the Internet and does not currently impose any time limitation on work-related use. However, browsing and downloading information from the Internet can become unfocused and time-consuming and business efficiency will therefore be kept under review.

👍 Activities that are encouraged are:

- Acquiring or sharing information necessary or related to the performance of an individual's job duties and responsibilities
- Participating in educational or professional development activities associated with their role

👍 For personal use at the Council's discretion, employees will be allowed a period of time to be determined by the Council (currently up to 5 hours a week) for personal surfing at break times. Sites accessed by the Internet or Intranet will be monitored and unacceptable sites will be blocked. This activity must not be included in any recorded work time for an employee. Once any quota is exceeded no further personal access will be granted.

UNACCEPTABLE

👎 Employees must not…

👎 … access the Internet through any means other than the Council provided service except with the written permission of the IT Programme and Service Delivery Manager, Departmental IT Manager, or one of his/her nominated officers. (Exceptions: There are a number of standalone Council workstations that have authorised access to the Internet via another service provider.);

👎 … knowingly download or install any software from the Internet without the permission of the IT Programme & Service Delivery manager or one of his/her nominated officers;

👎 … use any images, text or material which are identified as copyright-protected, other than in accordance with the terms of the license under which you were permitted to download them;

👎 … use personal chat services, such as ICQ, MS Messenger, AOL Instant Messenger, Yahoo Messenger, as these are not permitted on the Council's networks.

👎 Employees should not tie up internet resources on non-work related activity, e.g. leaving live internet feeds open (e.g. accessing news, sports results).

FORBIDDEN

Breach of the following provision may also amount to an offence under the Computer Misuse Act 1990 (offences include unauthorised access to computer material i.e. hacking; unauthorised modification of computer material; unauthorised access with intent to commit or facilitate the commission of further offences).

✘ Employees must not attempt to bypass the security, filtering or monitoring services on the Internet service, or access any unsuitable material that is not filtered.

✘ Employees must not undertake any Internet activity that exposes the Council to legal liability, financial risk, damage to or loss of reputation within the community or with its partners.

OTHER INFORMATION YOU SHOULD REFER TO:

ⓘ Internet Section 4 -‘ICT Use and Information Security Policy - Additional Information and Guidance’ document.

✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵

3.5 Software and Hardware

REQUIRED

✓ Employees must take proper care of ALL Council ICT equipment and hardware, whether in use within Council offices or at other locations.

✓ All software must be properly licensed and the use of all software must comply with the conditions of the relevant licence agreement. Corporate IT is responsible for ensuring that Corporate systems and software are licensed e.g. the Council's e-mail system. Directorates and system owners are responsible for licensing for their systems and software, e.g. applications that are owned by the Directorate. Individual employees must only use properly licensed software in accordance with this policy.

✓ If an employee is in any doubt as to whether software is authorised or unauthorised then checks should be made in the first instance with the employee's line manager, followed by a further check as necessary with Corporate IT.

✓ All Software is to be installed by the Council's outsourced desktop partner unless specific permission has been otherwise granted by the Council's IT Programme and Service Delivery Manager and this is recorded for audit purposes.

✓ Non-corporate software (including free, public domain or shareware software) may be installed on a workstation or laptop ONLY if it is relevant to the work of the individual employee, team, section or directorate, and ONLY where permission has been given by the employee's line manager, the IT Programme and Service Delivery Manager, and the Council's ICT outsourced service providers. However appropriate Licenses and records of Licenses must still be maintained.

✓ Employees are required to inform the Councils IT Programme and Service Delivery Manager of any upgrades including third party access requirements.

✓ USB data / peripheral devices may only be used to store sensitive work data if an encrypted secure area is configured to protect the data if the device is lost or stolen. Sensitive personal data must not be held on any open, unsecured device.

UNACCEPTABLE

👎 Employees must not…

- 👎 … distribute their copy of any software to others. "Bundled" software must be kept together, parts should not be distributed.
- 👎 distribute software developed in-house without express permission of their line …manager, directorate IT team or Corporate ICT.
- 👎 Load non-standard wall paper onto Council work stations or servers.

FORBIDDEN

- ✘ Employees must not…
  - ✘ … wilfully damage any ICT equipment in any circumstance and in any location;
  - ✘ … install or copy privately owned software or software for which they do not hold a licence; install pirated (unlicensed) software or install multiple copies of software for which only a single-user licence is held;
  - ✘ … Copy any corporate software for personal use;
  - ✘ … load games software, screen savers, utility software or any other free software issued with magazines or other media, onto Council workstations or servers;
  - ✘ … knowingly download software that modifies the desktop or browser (examples include emoticons smiley faces, screensavers, tool bars etc);
  - ✘ … use their work desktop or laptop to store large amounts or print any personal digital photographs;
  - ✘ … download or upload unauthorised software over the internet;
  - ✘ … attempt to circumvent any security system installed on a workstation or server by management or Corporate IT. This includes, but is not limited to, remote control software, automatic control software, lockdown software and anti-virus software.
- ✘ No employee should relocate any non-portable IT equipment without the specific permission of the Council's IT Programme and Service Delivery Manager and the Council's ICT outsourced partners. All office moves should proceed in accordance with Accommodation Move Instructions.
- ✘ Employees are reminded that the Council no longer owns its ICT infrastructure and therefore no employee has any right to change or modify any part of the ICT infrastructure without the agreement of the Council's ICT outsourcing partners.
- ✘ Employees must not use their work ICT equipment to create, store or transfer copyrighted material for which the Council has not been granted a business licence.
- ✘ It is forbidden to retain any mobile equipment (hardware and software) provided by the Council for work purposes when you leave the Council's employment. All such assets must be returned to the Council.

OTHER INFORMATION YOU SHOULD REFER TO:

ⓘ Software And Hardware - Section 5 -'ICT Use and Information Security Policy - Additional Information and Guidance' document.

✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵ ✵

3.6 Home Working and Remote Access

More employees are working from home or using mobile computers to keep in touch with work whilst travelling or working off-site and this is likely to proliferate in the future. The Council recognises this and provides remote access for business use, and facilitates home working. Employees should note, however, that current ICT support contracts do not extend to home visits to resolve problems (telephone support is available).

Remote access users and home workers should be aware of the importance of using the facilities in an appropriate manner, and that they are subject to the same security measures as if they were working in the office, and in certain circumstances more stringent measures.

Remote access covered by this policy includes, but is not limited to, dial-in modems, ISDN, DSL, VPN and Broadband etc. used when working from home, outstations or whilst travelling on Council Business.

The following apply to use of the Council's systems and equipment, and also use of an employee's own (or third party) computer equipment whenever that employee is working on Council business away from Council premises. Employees must also refer to the Council's policies and guidance on Work/Life Balance, Home and Flexible Working.

REQUIRED

Using Council ICT hardware off-site

✓ Line Managers must familiarise themselves with the advice offered in the IT Managers Advice for Flexible / Home Working and undertake to discuss this with the employee and, where necessary, the Council's ICT outsourced providers before embarking on home working or flexible working;

- ✓ the employee must seek authorisation from their line manager stating the nature and duration of off-site use; the employee accepts responsibility for any ICT equipment once it has been signed for;
- ✓ the employee and their line manager must sign a document stating the item of equipment, serial number or other relevant identification, the date that the equipment was taken from the Council's premises and the duration that it will be off-site, and sign a document stating the date that an item of equipment is returned to the Council's premises; and a copy sent to the employees personnel file (this document should be appropriately modified where mobile equipment is taken on and off site on a regular basis);
- ✓ Corporate IT or the appropriate departmental ICT team must be informed on the first occasion that an item of hardware is used off-site and the documents referred to above must be made available for their inspection as required.

REQUIRED (continued)

Employees working remotely must:

✓ Ensure the security of work-related data and information:

- ✓ Where an encrypted area is provided on mobile ICT equipment, all locally stored work should be saved to this area to ensure security;
- ✓ Ensure that any work that you do remotely is saved on the Council's system or is transferred to the Council's system as soon as reasonably practicable;
- ✓ Ensure proper consideration is given to the moving of any documents or data to any mobile device so as to remain compliant with the Data Protection Act and not to cause embarrassment to the Council in the event of accidental loss.

✓ Take reasonable precautions to safeguard the security of Council laptops and any computer equipment on which you do Council work. Any theft must be reported to the police immediately and an incident number obtained. Theft or loss must also be reported to your line manager, the relevant ICT service provider, Directorate ICT team and the Council's insurance section as soon as possible.

✓ Line managers must retrieve all ICT equipment & software from employees, contractors and temporary staff leaving the Council and all records should be updated accordingly.

✓ Return Council equipment when directed to do so.

✓ In the event of hardware faults the employee may be required to return the asset to the council for problem diagnosis and fixing.

✓ Employees will be required to adhere to the Council's ICT Policies and Procedures when working on Council equipment and when connected to the Council's network.

✓ Employees must adhere to normal operational workplace procedures when working from home (including sensible Health and Safety considerations and operating best practise (e.g. not leaving equipment logged in when you are not present, not saving passwords within windows, not holding passwords on the equipment, not using Council ICT Equipment as if it's your own personal home pc).

ACCEPTABLE

👍 Employees' own personal home computers may be used for Council business providing this does not involve transferring personal or confidential or sensitive data which conflicts with the Data Protection Act and other relevant Legislation controlling the use or movement of data, or could be considered damaging to the Council's reputation if revealed outside of the direct Council environment.

👍 To transfer approved, non-sensitive data away from the Workplace a USB "flash drive"/pen with an encrypted secure area can be utilised to avoid using the insecure email system. If in doubt what constitutes approved non-senstive data please refer to end of this section for further information sources or talk to the Council's IT Client or your Directorate IT Team.

UNACCEPTABLE

Employees working remotely must not…

- 👎 … access / use any 3rd party or unauthorised computer, system or network,
- 👎 … use any other unauthorised dial up-link whilst working on the Council's network;
- 👎 … install software on, or change the configuration of the Council's equipment including loading alternative ISP Internet Services (unless specifically authorised for work purposes);
- 👎 leave Council mobile ICT equipment in vulnerable locations unattended for periods of time, inviting theft (e.g. cars).

FORBIDDEN

- ✘ Employees must not change any hardware or configuration settings for the purposes of working in the employee's home environment without the prior knowledge and agreement of the Council's IT Programme and Service Delivery Manager and Councils ICT Outsourcing Partners.
- ✘ Employees must not store Client data on non-Council equipment. If Client data is held on mobile council equipment this must be protected by additional security measures.
- ✘ Employees must not give unauthorised persons (e.g. family and friends) access to Council equipment, or the Council's network or ICT Systems, or disclose details or confidential information to unauthorised third parties.
- ✘ Employees must not allow Council equipment to be used for personal use other than that permitted under this policy.

OTHER INFORMATION YOU SHOULD REFER TO:

- ⓘ Home Working & Remote Access- Section 6 -'ICT Use and Information Security Policy - Additional Information and Guidance' document.
- ⓘ Personnel Advice: IT Managers Advice For Flexible / Home Working

❋ ❋ ❋ ❋ ❋ ❋ ❋ ❋ ❋ ❋ ❋ ❋

3.7 MOBILE PHONES, PDA'S AND OTHER MOBILE TECHNOLOGY

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.

REQUIRED

✓ Employees 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 or in public places, and use appropriate caution and safeguards to minimise those risks.

✓ Employees issued with a mobile phone or Personal Digital Assistant - PDA - (and peripheral equipment) are responsible for its safekeeping and security. You should use the security lock code or PIN number (as appropriate) to protect the phone/PDA and the stored data. This should not be disclosed to anyone else, and you should not leave the phone/PDA unattended.

✓ Employees should use Mobex codes on Council mobile phones when dialling internal Council numbers.

✓ Employees should record the security number of their mobile to allow the mobile network operator to bar the service in the event of loss.

✓ Asset details of Council purchased PDA's must be recorded with personnel.

✓ Before entering into a new mobile phone contract, checks should be made with the Directorate representatives as to whether there is an existing spare contract phone available for transfer.

✓ Broken/faulty mobiles under warranty (currently 12 months) should be returned to the Directorate representative for replacement.

✓ Damaged and out of warranty mobile phones or obsolete mobile phones as a result of paid upgrades should be disposed of, in consultation with Directorate representatives, for recycling in accordance with the Councils "Green" policies.

✓ When taking work-related photos using a Council mobile phone, care must be taken not to include members of the public / staff without their prior permission (Data Protection).

ACCEPTABLE

Mobile phones

👍 Council-issued mobile phones are provided for work-related purposes. However, 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).

UNACCEPTABLE

Mobile Phones:

- 👎 Employees should not respond to unsolicited commercial text / voice-mail messages as this could introduce viruses onto your Council mobile phone.
- 👎 Employees must not send inappropriate content from a Council mobile phone, or download chargeable ringtones, wallpapers or screen savers to a Council mobile phone.
- 👎 Personal mobile phones should be used appropriately in the workplace - avoid disrupting colleagues and have due regard to maintaining work performance. Phones should be set to discrete ring settings or turned to silent mode wherever possible. Similarly, texting personal messages should not disrupt an employee's work performance.

FORBIDDEN

Mobile Phones:

- ✘ 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.
- ✘ Personal mobile phones must not be connected to any Council equipment, with the exception of laptops for dialling in.
- ✘ No inappropriate photographs, images or jokes received on a Council mobile should ever be forwarded on. (Material received, gathered or sent genuinely and necessarily in the course of work duties (e.g. pictures of offensive graffiti) will be exempt from this restriction).
- ✘ Mobile phones must not be used to harass any persons.

PDA's:

- ✘ Business data / confidential information must not be stored on a PDA without additional security measures employed.
- ✘ Employees must not send e-mail with confidential personal information from a PDA or mobile phone without using further security measures.

OTHER INFORMATION YOU SHOULD REFER TO:

ⓘ Mobile Phones, PDA's & Other Mobile Technology - Section 7 - 'ICT Use and Information Security Policy - Additional Information and Guidance' document.

4 MONITORING AND CONFIDENTIALITY

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.

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 ICT environment.

The Council will monitor your business communications for reasons that include:

- Providing evidence of business transactions;
- Ensuring that 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 unauthorised use of the Council's communications systems or criminal activities; and
- Maintaining the effective operation of the Council's ICT systems.

4.1 E-mail

The Council will monitor and filter corporate e-mail (e.g. sender, receiver, subject, attachments to e-mail, numbers and patterns of e-mails) for the reasons specified above. IT Client alongside the Council's outsourced desktop service provider will control and manage the e-mail filtering software.

Employees must not send e-mails with personal content from the Council's corporate e-mail system. E-mails with personal content should not be sent to the Council's corporate e-mail system (@reading.gov.uk). Any e-mails sent from or received by the corporate e-mail system will be treated and monitored as business related e-mail.

Employees must send and receive e-mails of a personal content using a private web based e-mail account signed up separately. However use of this personal account must not customise the Councils desktop software (including toolbars and browser). The Council will grant limited rights of use to access this web based e-mail account using the corporate Internet facilities and will undertake not to monitor the personal content of the e-mails. The Council will however monitor the time and duration private web based e-mail accounts are accessed in accordance with maintaining staff performance and efficiency.

Whilst automatic monitoring of personal e-mail content will not be undertaken, if inappropriate personal use is revealed following any routine ICT maintenance activity this will still be treated as a breach under this policy and may be subject to disciplinary procedures.

The Council reserves the right to withdraw access to the internet/personal e-mail account if an employee abuses this privilege.

Any work related e-mail sent to a personal e-mail account must not:

a) breach the Data Protection Act (revealing personal sensitive information)
b) breach the Freedom of Information Act (failure to disclose information that due to timing resides at home personal account or PC)

Sometimes it is necessary for the Council to access your business communications received at your @reading.gov.uk account during your absence, such as when you are away because you are ill or while you are on holiday. Unless your mailbox settings are such that the individuals who need to do this already have permission to view your inbox, access will be granted only with the permission of your line manager or Head of Service.

All incoming e-mails to @reading.gov.uk addresses are scanned using monitoring software. The software will block unsolicited marketing e-mail (spam) and e-mail which have potentially inappropriate attachments. If there is a suspected virus in an e-mail that has been sent to you, the sender will automatically be notified and you will receive notice that the e-mail is not going to be delivered to you because it may contain a virus.

The Council reserves the right to alter, modify, re-route or block the delivery of e-mail messages as appropriate. This includes but is not limited to:

- Rejecting, quarantining or removing the attachments and/or malicious code from messages that may pose a threat to Council resources.
- Discarding attachments, such as music, considered to be of little business value and of significant resource cost.
- Rejecting or quarantining messages with suspicious content.
- Rejecting or quarantining messages containing offensive language.
- Re-routing messages with suspicious content to the IT Client Team for manual review.
- Rejecting or quarantining messages determined to be unsolicited commercial e-mail (spam).
- Appending legal disclaimers to messages.
- Filter out inappropriate content downloading from an Internet website initiated from an e-mail.

Regular reviews and reporting of business e-mail activity will be undertaken and reported through the Council's Information Security Management Forum and where necessary on to CMT.

4.2 Internet

Access to the Internet will be controlled and monitored for appropriate business use.

All employee Internet usage will be monitored and filtered using appropriate software for the business communication reasons specified earlier in this section. Internet activity recorded will include the employee's login, domain names of web sites visited, time and duration of visits and content downloaded from the Internet.

Restricted appropriate access to the internet for personal surfing will allowed as determined by the Council. The Council reserves the right to withdraw Internet surfing from any employee in the event of abuse of this privilege.

IT Client alongside the IT Communications and Network service provider will manage the Council's Web Filtering. The software will block access to inappropriate web sites, and will also stop auto downloads from inappropriate web sites.

The Council reserves the right to block access to web sites and downloading of files as appropriate. This includes but is not limited to:

- Blocking downloads, such as music, considered to be of little business value and of significant resource cost.
- Blocking access to web sites that are known to contravene legislation to which the Council must adhere.
- Blocking access to web sites containing offensive language or content.
- Blocking or restricting access to any site when it is felt that access is causing impaired business performance either through productivity, or through the demand on ICT facilities e.g. network or server capacity.

Any inappropriate Internet surfing activity undertaken through the Council's Internet facilities may result in disciplinary procedures against the employee.

The Council also reserves the right to withdraw business and personal Internet surfing rights from any employee in the event of abuse of this privilege.

Regular reviews and reporting of Internet surfing will be undertaken and reported through the Council's Information Security Management Forum and where necessary onwards to CMT.

4.3 Telephones

Telephone landlines will be controlled and monitored for appropriate business use.

Council telephone landlines should only be used for work-related purposes but may be used for private purposes during working hours in the case of an emergency. The Council must however be reimbursed for personal call charges incurred in or out of working hours.

Software Systems are in place whereby telephone usage can be reported upon when required

GLOSSARY OF TERMS

- "**computer system**" refers to any combination of computer hardware, computer software and data that can be considered a discrete system;

- "**contracted persons**" refers to any organisation with whom there is a contractual agreement which requires the organisation's employees working with or for Reading Borough Council to work to the Council's ICT Polices and Procedures (recognising where disciplinary action is necessary this will default to the organisations own procedures);

- "**Council**" refers to Reading Borough Council;

- "**database**" refers to either one or more electronic files used to record information in a highly structured format;

- "**document**" refers to either one or more electronic files used to record information in a loosely structured format;

- "**employee**" refers to any permanent, temporary or part-time employee, or casual worker, of Reading Borough Council (contract staff **should** be covered by the same policy in their contractual agreement);

- "**key organisation**" refers to key organisations contracted to work with the Council who use Council provided ICT (e.g. Council's ICT Outsource Partners);

- "**ICT**" refers to Information Communications Technology;

- **"ICT equipment and resources"** refers to all ICT hardware, software, peripherals, media, data, systems and user accounts/logins;

- "**legislation**" refers to all relevant current ICT related legislation that by law the Council must be compliant with. This includes:
  a) Data Protection Act
  b) Freedom of Information Act
  c) Human Rights Act
  d) Computer Misuse Act
  e) Electronic Communications Act
  f) Copyright Designs & Patents Act
  g) Regulation of Investigatory Powers Act
  h) Disability Discrimination Act
  i) Caldicott Guidelines for Social Services (DOH)
  j) Race Relations Act
  k) Sex Discrimination Act
  l) Health & Safety Act

- "**Operator**" – Councils mobile phone contracted supplier/operator;

- **"personal use"** – Discretional personal use of the Councils Internet facility to access the Internet and Internet email for personal use. The preferred Internet email provider for personal use is Yahoo;

- **“remote”** refers to use of Council ICT equipment at outstations or at home and whilst travelling;

- “**system owner**” is the responsible officer in charge of ICT Systems or the officer who developed the solution (in the case of locally developed desktop solutions e.g. spreadsheets, access databases etc);

End of Document