WOKINGHAM BOROUGH COUNCIL

Wokingham Borough Council

Information Security

and

Acceptable Use of ICT Policy

Principles: This document sets out Wokingham Borough Council's (WBC) Information Security Policies and procedures, and the responsibilities of everyone using WBC Systems and IT.

Must do: All users of IT must:

√ **Consider the sensitivity of the information they handle**

√ **Protect information in proportion to its sensitivity by ensuring that information, whatever its format, is secured by physical or approved electronic means**

√ **Ensure that they take appropriate action within the appropriate procedures when there is a breach of policy**

Document Control

Organisation	Wokingham Borough Council
Title	Information Security and Acceptable Use of IT Policy
Author	Ivan Ayres, Information Security Officer
Filename	G\Government Connect\WBC Policies
Owner	Head of Customer Services & IMT
Subject	Information Security; Use of IT
Protective Marking	UNCLASSIFIED
Review date	July 2016

Revision History

Revision Date	Reviewer(s)	Previous Version	Description of Revision
02/14	The Information Governance Team	1.0	Updated and reformatted after annual review
July 2015	Ivan Ayres	V2.0	Annual Review and updated to confirm Document Marking Classification Changes

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Strategic Director of Resources & Section 151 Officer	Graham Ebers	
Joint Head of Customer Services & IMT and SIRO	Sally Watkins	
Service Manager, Human Resources	Sarah Swindley	

Document Distribution

- This document will be made available as a source of reference to all staff.
- All persons who require access to the Council's IT Network and/or IT systems will be required to read and understand this Information Security and Acceptable Use of ICT Policy (AUP) and sign the Personal Commitment Statement which can be found on page 16. *(Note: Electronic signatures are also acceptable).*

Contents

1 EXECUTIVE SUMMARY

This document sets out Wokingham Borough Council's (WBC) Information Security Policies and Procedures, and the responsibilities of everyone using WBC systems and IT. Information security 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 can risk, at worst, the safety of individuals, loss of financial information, breach of commercial confidentiality and subsequent financial penalties from the regulator, the Information Commissioner.

There are three main principles to this policy:

- All staff must consider the sensitivity of the information they handle.
- All staff must protect information in proportion to its sensitivity by ensuring that information, whatever its format, is secured by physical means (such as locking paperwork away or appropriately archiving it when no longer current) or by using approved electronic means (such as only using Council IT equipment).
- Managers must ensure this policy is applied within their areas of work and should also lead by example.

This policy is mandatory. Any breach of the policy may result in disciplinary action being taken under the Council's Disciplinary Procedure.

Any breaches of security (non-compliance with this Policy) must be reported to the Information Security mailbox Information.Security@wokingham.gov.uk , or via the Report an Information Security Incident form on the WBC Grapevine at the earliest opportunity. This is to safeguard the Council and limit potential damage from information loss.

2 POLICY STATEMENT

It is the policy of Wokingham Borough Council to ensure that all information systems operated by the Council are secure and aspire to comply with the requirements of the Data Protection Act, the Computer Misuse Act and (at the level of principles) the International Standard for Information Security ISO270001:2005 and PSN requirements. It is also the aim of the Council that all staff must be fully aware of the need to maintain secure systems and fully understand their responsibilities as outlined in this document.

All staff are responsible for ensuring that they understand and abide by this policy. Failure to do so will be viewed as a serious matter and may result in disciplinary action.

It is the policy of the council to ensure:

- Information is protected against unauthorised access.
- Confidentiality of information is maintained.
- Information is not disclosed to unauthorised persons through deliberate or negligent action.
- The integrity of information is maintained by protection from unauthorised modification
- Information is available to authorised users when needed.
- Regulatory and legislative requirements are met.
- Contingency plans are produced and tested as far as is practicable to ensure business continuity is maintained.
- Information Security training is provided for all staff.
- All breaches of information security and suspected weaknesses are reported, investigated and appropriate action taken.
- Sharing of information with other organisations/agencies is permitted providing it is done within the remit of a formally agreed information sharing protocol.
- That there is a fair and consistent approach to the enforcement of standards of conduct expected from employees when using social media sites.

3 APPLICABILITY

All employees of the Council, contractual third parties and agents of the Council with access to Wokingham Borough Council equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the Council's equipment and the information that they use or manipulate.

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 the contract.

4 REQUIREMENTS

For the avoidance of doubt, the Information Security and the Acceptable Use of ICT Policy requires that;

- Individuals must ensure that as far as is possible no unauthorised person has access to any data held by the Council.
- Individuals must ensure that physical security measures are properly used.
- Individuals must not deliberately or negligently corrupt, damage or destroy data, software or hardware belonging to the Council. This includes the proliferation of viruses or other similar computer programmes.
- 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.
- Individuals must not load or download software packages onto WBC PCs and under no circumstances should games software be loaded on WBC PCs.
- 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.
- 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.
- All employees must read, understand and sign to acknowledge that they have read and accepted this policy and the specific requirements of it, which are as follows.

4.1 Network Security

- Only Wokingham Borough Council owned Laptops and PC's are allowed to be connected to the Council data (Computer) network.
- If remote access is required from outside the E.U. specific permission must be sought from the Councils ICT Technology & Service Manager.

4.2 Physical Security

- Access to data held on the Council's information systems is minimised by restricting physical access to the Council's buildings.
- Where information is kept in the Council's offices, access to buildings is restricted by ensuring that 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.

- Visitors to Council buildings must be accompanied at all times and signed in and out of the premises on arrival and departure.

4.3 Computer Security

4.3.1 Data Storage

- All staff must abide by the rules of the Data Protection Act and the Computer Misuse Act.
- Access to individual data areas will only be granted following a written approval from the "owners" of that area.
- Storage of data on PC or Laptop's C: drive is discouraged and all users are requested not to store files on PC or Laptop's C:\drives because in the event of failure, all data stored on the C: drive would be lost as it not backed up.
- 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 G:\ or M:\ or Z:\ drive on the network). This is a secure storage area which is regularly backed up and is therefore resilient to failure.
- The following types of file can only be stored if they relate to explicit business needs.

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];.	SCRScreen Savers

4.3.2 File Storage and Naming Conventions

- All documents and files should 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.
- 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.

4.3.3 Screen Locking

- Computers must not be left unattended with screen unlocked when logged in to the Council's Network.
- Whenever staff move away from a workstation they must ensure that they have logged off or locked the workstation.
- When leaving a place of work staff must ensure they have logged off and closed down the workstation correctly.

4.3.4 Memory Sticks and removable media

- Only WBC supplied encrypted (Kingston) memory sticks are to be used.
- Council Data marked **OFFICIAL** and **OFFICIAL-SENSITIVE** must not be transferred to a home PC / Laptop.

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

4.3.5 Passwords

- Passwords given to you are for your use only.
- Passwords should not be written down or given to others to use under **any** circumstances.
- Passwords must be a minimum of 7 case sensitive characters[2] and should be a combination of upper/lower/numeric/special characters. Ideally Passwords should also contain random characters such as #@**?!$&** etc. Passwords must include at least three different character types, or they will not be accepted.
- Passwords must be changed every 90 days as a minimum.
- 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.

4.3.6 Viruses

- All files received on disc from outside the Council or received via electronic mail must be checked for viruses before being used on Council equipment. You must not intentionally introduce/send or download files or attachments which contain viruses, or which are meant to compromise the Council's systems.
- If a virus is suspected, the ICT Service Desk must 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.

4.3.7 3rd Party Network Connections

- All requests for external 3rd Party network connections must be processed by the Council's ICT Partner and will be strictly governed by relevant standards and approval process.

4.3.8 Document Marking

- All information assets (paper, files, electronic media, emails or other) to be processed by Wokingham Borough Council, must be protectively marked in accordance with the sensitivity of their content, following the requirements of HMG Security Policy Framework, and in compliance with standards laid down for the Government Connect Programme (GCSX).
- The protective marking of an information asset provides people with information on:-

    a. The correct level of protection for the information asset;
    b. Principles for the production, dispatch, receipt and destruction of the information asset;
    c. The severity or impact of the loss or compromise of the information asset.

4.3.9 Document Handling

- All paper documents should be securely locked away when no longer required, by being placed in appropriate secure containers.
- The clear desk policy requires that all information protectively marked **OFFICIAL** and **OFFICIAL-SENSITIVE** shall be put away and locked when the desk is unattended.

[2] This is the minimum standard required under GCSX CoCo requirements for connection to the Government Secure Extranet.

4.3.10 Printing

- Staff must ensure adequate care is taken when printing information, utilising the use of WBC's secure printing solution. If there is a printer fault when printing **OFFICIAL** or **OFFICIAL-SENSITIVE** material please phone the IT service desk who will ensure that any unprinted files are deleted from the print queue.

4.3.11 Scanning

- Staff must ensure adequate care is taken when scanning documents and using WBC's secure scanning solution. Checking the destination file or email address.

4.4 Clear Desk

- All manual files and paper records must 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.

- All **OFFICIAL-SENSITIVE** and **OFFICIAL** information must be held securely in locked containers, lockers, drawers and filing cabinets to prevent unauthorised access.

- **OFFICIAL-SENSITIVE** and **OFFICIAL** waste must be disposed of securely. **OFFICIAL-SENSITIVE** and **OFFICIAL** waste shall be shredded or placed in the appropriate confidential containers for secure disposal.

4.5 Mobile Workers and Home Workers

4.5.1 Laptops

- Care must be taken to avoid being overlooked whilst using Council equipment in any public area

- Laptops must be kept in a secure location when not in use.

- Laptops 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.

- When using portable equipment on the move, or outside of office hours, reasonable care should be taken to secure it.

4.5.2 Manual Files

- Manual files processed outside of the Council's property must be kept with the individual completing this work.

- When left unattended, Manual Files must be in a locked container and out of view.

- Computer equipment or manual files that are travelling with an employee must be locked in the boot of the car or kept with the individual at all times when travelling by public transport.

- Computer equipment or manual files must not be left unattended on a train or bus or left in a vehicle overnight.

4.5.3 Home Printing

- Home printing is only permitted in exceptional circumstances where a business case has been approved by the Smart Working Board in consultation with the Technology and Service Manager, IMT. Every business case submitted will be assessed individually.

4.5.4 Mobile Telephones, Blackberry Devices and Smart Phones

- Staff issued with mobile phones, Blackberries, Smart Phones or other Personal Digital equipment are responsible for safekeeping and security.
- Security lock and pin protection must be used where available to protect the device and any stored data.
- Blackberry and Smart Phones devices must be protected with a password
- Council-issued mobile devices are provided for work-related purposes only.
- If Council-issued mobile phones are used for private purposes the Council must be reimbursed for personal call charges including VAT . (When dialling personal calls, place an asterisk (*) after the number (0118 974 1234*) and all such calls will be easily recognised must be reimbursed to the Council and are the responsibility of the mobile device user).

4.5.5 Lost or stolen mobile devices

- If a mobile device is lost or stolen, staff must;

1) Contact the IT Servicedesk on 0118 974 6666 to report the loss and ask for the mobile device to be suspended so that it can no longer be used.
2) Complete a Report an Information Security Incident form on the Grapevine
3) Notify the local Police station of the loss.
4) Raise an IT request for a replacement device via Intranet by using the Equipment and Applications for existing staff (UNC) form.

Please note that replacement of lost or stolen handsets is not covered by any insurance so the relevant department will need to pay for the replacement.

4.5.6 Leaving WBC or moving into another role

- Staff who are issued with Laptops, Cryptocards or any mobile devices must ensure their safe return on termination of employment or acceptance of a different post within the Council which does not require the use of a those devices.

4.6 Use of the Internet

4.6.1 Downloading of Information Resources

- Individuals must not download non-work related information 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.
- Individuals requiring any new software, including any plug-ins, must make a formal request to the ICT Service Desk (Ext 6666).
- Software must not be downloaded and/or installed onto Council ICT equipment unless it has been approved by the Corporate IMT and can be validated that it is licensed for current use.
- Graphical, audio and video files may be downloaded and stored on WBC's network for business use only.
- 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.

4.6.2 Uploading Data / Information to the Internet

- Any users who are responsible for uploading data / information to the Internet must be sure that the information being uploaded is suitable to upload, and not **OFFICIAL-SENSITIVE** or **OFFICIAL**.

4.6.3 Internet Filtering and Blocking

- Users should not attempt to by-pass the Council's Internet filtering software. Users are allocated quota time for personal internet usage that must be deducted from their timesheet

- Staff 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 6666) and request the site is on an approved list of websites.

4.7 E-MAIL USE

E-Mail is a useful tool that enables individuals to organise themselves and communicate with others. This policy sets out the expectations for all WBC 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.

4.7.1 Sending email

- Individuals must use the default settings and not make changes to the disclaimer.

- E-mail is set up by default to conform with WBC branding and house style, and a corporate disclaimer is applied to all outgoing messages.

- 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.

- 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 OFFICIAL-SENSITIVE or OFFICIAL e-mail, individuals should be mindful of any delegate permissions that recipients may have set up.

- 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.

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

- All emails should be finished with an email signature that includes your name, title, service and contact details.

4.7.2 Agreements by email

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

4.7.3 Mailbox size and housekeeping

- The standard individual mailbox size provided is 1GB. In addition to individual mailboxes, shared mailboxes can be provided where there is a specific business need. Please contact the IT Servicedesk 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.

4.7.4 Distribution lists

- 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.

4.7.5 Mailbox management

- 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.

- 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.

- When an email is received with an attachment which needs to be retained, individuals should save the attachment to the departmental network drive, and not leave the attachment within the email.

4.7.6 Misuse of email

- 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.

- Staff must take care with any suspected malicious or nuisance e-mails received (e.g. chain e-mail, hoax and spam e-mails) and delete them. If any suspicious e-mails are received they should be reported to the IT Service Desk.

- Individuals must never open attachments to an e-mail of unknown origin as they may contain viruses and other malware.

4.7.7 Mail and absence

- An "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.

- Officers should not just put “Contact Customer Services” as their out of office contact unless they have prior agreement from the Joint Head of Customer Services & IMT.

4.7.8 Calendars

- Calendars should be set to be viewable by all WBC 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 IT Servicedesk.

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

4.7.9 Attachments

- Attachments should not be included in any internal mails or meeting invites, wherever it is possible links to documents should be used instead

4.7.10 GCSX EMAIL

- Employees are required to have a Government Connect Secure Extranet (GCSx) e-mail account if they need to:

    - Send or Receive Client-based or financial information to another person or organisation who is part of the GSi network (for example, central government departments, other local authorities, the NHS, the police).

    - Receive client-based or financial information from another person or organisation who is part of the GSi network (for example, central government departments, other local authorities, the NHS, the police)

  Staff should refer to the Intranet Government secure email for further and more detailed information about GCSx email, what is it, who should use it, and why it is important for some people to have these separate accounts.

4.7.11 [SECURE] MAIL

- The Global Certs secure mail system must be used when an email needs to be sent securely, and the recipient does not have a Government Secure (GCSx) eMail account. (Please refer to the Intranet pages Secure Mail for further and more detailed information about Secure Mail, what is it, who should use it, and why it is important for some people to have these separate accounts).

- To gain access to secure mail employees and associates simply need to complete a short e-learning module.

5 SECURITY INCIDENT REPORTING

- Information Security Incidents must be reported within two Business days of occurring in accordance with the Council's Security Incident Policy which classifies the type of security incident and ensures appropriate notification of relevant parties including IMT, Legal SIRO, Data Protection Officer and external organisations set out in the PSN Code of Connection (GCSX).

- Loss of **any** piece of ICT equipment (computer, laptop, blackberry, mobile phone, USB storage device, VPN token etc), is classed as a security incident and must be reported.

- Information Security Incidents should be reported via the Report an Information Security Incident form form which can be found on the Intranet.

6 MANAGERS RESPONSIBILITIES

- All Managers and Team Leaders must give their full backing to all the guidelines and procedures as set out and agreed in this document.

- Managers must follow the Council's New Starter process to ensure that new staff who require access to ICT are provided with log-in credentials and access privileges as appropriate.

- Managers must also take responsibility to ensure:

    - All new staff receive a briefing on this policy as part of their Day 1 introduction to Wokingham Borough Council and formally sign the Acknowledgement of Acceptance before they are given access to any of the Council's IT Systems.

    - All new staff must review the Council's Policy Document as part of their Day 1 introduction to Wokingham Borough Council and also have taken the Council's Data Protection, Information Security and Document marking e-Learning module which is available on MyLearning.

    - All staff review this Policy and re-confirm acceptance on an annual basis or when invited to do so.

A more detailed explanation of Managers responsibilities can be found on the Intranet.

6.1.1 Leavers - Management of User Accounts

- Managers must follow the Council's Leaver Process and submit a Leavers Form to the ICT Service Desk which will ensure that the leavers IT account is closed immediately and also that all IT equipment is returned for re-use.

- Managers must 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.

6.1.2 Leavers - Return of IT Equipment

- When an employee leaves WBC, Line Managers must ensure all IT equipment is returned to IMT by either:

    - Emailing the IT ServiceDesk advising of items which need to be collected.

      or ;

    - By responding to an email generated from Wiser, (which is automatically sent to all managers when a member of staff is leaving). The email asks you to let IMT know what equipment you need collecting.

    - On the last working day, Managers must collect all the leavers IT equipment and ensure it is returned to IMT

    - Failure to comply with the requirements of this policy in relation to the return of ICT equipment is regarded as a serious breach of this policy.

7 CONTROLS

It is up to all managers of staff in the Council to ensure that individuals adhere to this Policy. IMT staff will be responsible for monitoring systems under their control for signs of:

- Illegal or unauthorised software having been loaded.
- Password misuse.
- Unauthorised access

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

The Council's Internal Audit staff will review the Council's performance in implementing this policy.

8 APPENDIX 1: REFERENCES

Related policies

- GCSX Acceptable Usage Policy and Personal Commitment Statement
- Data Protection Act 1998 Policy and Guidance
- Smart Ways of Working Policy

The following Wokingham Borough Council policy documents are indirectly relevant to this policy:

- Human Resources Information Security Standards.
- Communications and Operation Management Policy.
- Policy for Conduct and Personal Behaviour.
- Internet Social Networking Policy.

Legal references

- Data Protection Act 1998
- Companies Act 1985
- Copyright, Designs and Patents Act 1998
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Civil Contingencies Act 2004

Regulations – guidance

- 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
- ISO27001:2005 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.

If you have any questions about this policy, in the first instance, speak to your Line Manager, who might refer you to your Information Governance Group Representative if appropriate.

9 ACKNOWLEDGEMENT OF ACCEPTANCE

Each user must read, understand and sign to verify they have read and accepted this policy.

I understand and agree to comply with the Information Security and Acceptable Use of IT Policy of my organisation.

Signature of User: ……

A copy of this agreement is to be retained by the User and Employee Services.

Document Date:	<Date signed and agreed by staff member>
Name of User:	<Surname, First Name>
Job Title:	<Job Title>
Service:	<Service>