Item 8 - Appendix 2

Information Security and Conduct Policy

Warwick District Council

WARWICK DISTRICT COUNCIL

www.warwickdc.gov.uk

Information Security and Conduct Policy

Revision History

Document	Information Security and Conduct Policy
Author	Ty Walter
Date Completed	10 August 2009
Review Date	08 March 2018

Version	Revision Date	Revised By	Revisions Made
1.0	31 Dec 2008	Ty Walter	Original Document
1.1	20 Oct 2010	Ty Walter	Update to include Card Data Policy
1.2	13 Oct 2011	Ty Walter	Minor updates, plus revised Compliance, Monitoring and Assurance section and inclusion of a new sub-policy on Digital Forensic Readiness.
1.3	15 Nov 2011	Ty Walter	Update to the System Owner responsibilities.
1.4	21 Nov 2011	Ty Walter	Minor update to the disposal of equipment.
1.5	13 Jan 2012	Ty Walter	Minor update to explicitly indicate that the use of Council equipment by non-council staff is prohibited.
1.6	28 May 2012	Ty Walter	Inclusion of the section: Joint Working – Warwickshire Councils Inclusion of a section on 'Personal Data Storage'
1.7	06 Aug 2012	Ty Walter	Inclusion of the Physical & Environmental Security Policy
1.8	09 Sept 2013	Ty Walter	Reference to the sub policies was moved to a separate appendix.
1.9	02 Mar 2016	Ty Walter	Update to Internal Audit (IA) section permitting IA access to systems and data without approval from system owners.
1.20	07 Mar 2018	Anna Moore	Update to include references to GDPR and associated requirements of the regulations.

Approvals

This document requires the following approvals:

Name	Title
ICT Steering Group	
Senior Management Team	
Employment Committee	

Distribution

This document has been distributed to:

Name	Title
All Staff	
All Members	

Table of Contents

1 Management Summary

This high level policy is one of a series that forms the policy core of the Information Governance (IG) Framework. The IG Framework recognises that sound information management relies on best practice from a number of different disciplines. These are privacy management, Information law and rights, information security and risk management, records management and information quality management.

Information resources are vital to the Council in the delivery of service to residents, businesses and visitors. Their confidentiality, integrity and availability are essential to maintain service levels, legal compliance and the public image and public perception of our Council.

It is important that citizens are able to trust us to act appropriately when obtaining and holding information and when using the authority's facilities. It is also important that information owned by other organisations made available to our Council under secondary disclosure agreements is also treated appropriately by us.

Any Public Authority that uses or provides information resources has a responsibility to maintain, safeguard them and comply with the laws governing the processing and use of information and communications technology.

As an organisation we must take security very seriously and that relies on all staff playing their part. We are all personally responsible for following the requirements set out in the Council's Information Security & Conduct Policy.

Warwick District Council has a significant investment in computer systems and networks and is increasingly dependent upon the processing of the data which it holds.

The increasing use of mobile computer devices and the need to transmit information across networks both within the Council and to/from external organisations renders the data more vulnerable to accidental or deliberate modification or disclosure. Some of the information systems contain highly critical data which, if not handled securely, could present a serious problem to the Council, its employees, Members and customers.

The loss of data, computer processing facilities or breaches of data access security could incur significant costs, loss of revenue and damage to the Councils reputation. Furthermore, defamation and harassment actions, negligence cases, breaches of copyright and claims in respect of disclosure of trade secrets are just some of the legal claims that have arisen recently as a consequence of e-mail, Internet and other electronic activities.

Information security management is an on-going cycle of activity aimed at continuous improvement in response to emerging and changing threats and vulnerabilities. It can be defined as the process of protecting information from unauthorised access, disclosure, modification or destruction and is vital for the protection of information and the Council's reputation.

This policy, and its associated sub-policies (See Appendix 1), describes what is required of us and how security is to be implemented for all the information systems concerned. Line Managers are responsible for implementing the necessary procedures to bring these Policies to operational life and ensure individuals' compliance with them

2 Policy Statement

Warwick District Council is committed to the development and maintenance of an Information Security and Conduct Policy as part of the wider. The Information Security and Conduct Policy will ensure that:

- Information will be **protected against unauthorised access**.
- **Confidentiality** of information will be assured.
- **Integrity** of information will be maintained.
- **Regulatory** and **legislative** requirements will be met.
- **Business Continuity plans** will be produced, maintained and tested.
- **Information security training** will be available to all staff.
- **All breaches of information security**, actual or suspected, will be reported to, and investigated by the Information Security Officer.
- **An Information Asset Register is maintained**
- **Information security risks are regularly re-assessed**

3 Purpose

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

This policy document, and sub-policies, establishes the ICT Security and Conduct Policy for Warwick District Council (the Council) to ensure efficient and effective use of all information and communication systems. Further, this policy and sub-policies, aims to ensure that the Council's investment in information, software, hardware and electronic resources is protected.

This policy is designed to:

- Provide direction and support for ICT security in accordance with business requirements, regulations and legal requirements;
- State the responsibilities of staff, partners, contractors and any other individual or organisation having access to the Council's ICT systems;
- State management intent to support the goals and principles of security in line with business strategy and objectives.
- Provide a framework by which the confidentiality, integrity and availability of ICT resources can be maintained.
- Optimise the management of risks, by preventing and minimising the impact of ICT security incidents;
- Ensure that all breaches of ICT security are reported, investigated and appropriate action taken where required;
- Ensure that supporting ICT security policies and procedures are regularly reviewed to ensure continued good practices and protection against new threats;
- Ensure ICT information security requirements are regularly communicated to all relevant parties.

This policy, and sub-policies, are based on industry good practice and intend to satisfy the requirements set out by the Government's Code of Connection (CoCo) and establish an organisational structure and framework of controls from which detailed security procedures can be implemented. To this end, the document contains a number of Policy Statements which are supplemented by a series of security guidelines. The guidelines are for reference by Service Area Managers, System Owners, line managers etc. in ensuring that their systems are protected in the most appropriate and effective way.

4 Scope

This policy, and its sub-policies, applies to all Warwick District Council employees, Councillors (Members), temporary / agency staff, consultants, suppliers, partners, contractual third parties and agents of the Council who have been designated as authorised users of Council electronic communication systems. Any reference in the document to "employee" or "staff" is deemed to include all of these groups of authorised users.

5 Exceptions to this Policy

If any member of staff feels that they cannot comply with this policy, they must first discuss the matter with their line manager. If these discussions do not lead to an agreement by the individual to comply, then the line manager may apply to the Information Security Officer for:

- An exemption for the individual and / or,
- An amendment to the policy

If, after consideration of the risks and consultation with the appropriate Information Asset Owners, the Information Security Officer cannot agree an exemption or change to the policy, they will write to the individual giving reasons for refusal and requiring written confirmation (within a reasonable timescale) of the individual's intent to comply. If no confirmation is received, Warwick District Council's disciplinary procedures will be invoked.

6 Responsibilities

Whilst information security policies, guidelines and measures have been devised, implemented and managed by specific functions and individuals, everyone within the council has a responsibility to ensure that they take basic steps to safeguard the security of the information that they are using and seeing. Line managers must ensure that the all staff under their control receive and adhere to the guidelines.

6.1 Employment Committee

Warwick District Council's Employment Committee is responsible for:

- approving the council's Information Security and Conduct Policy.

6.2 Senior Information Risk Officer (SIRO)

The SIRO has overall responsibility for information as a strategic asset, ensuring that the value to the organisation is understood and recognised and that measures are in place to protect against risk. The Council's SIRO is the Deputy Chief Executive & Monitoring Officer.

6.3 Information Security Officer (ISO)

Corporate Management Team has nominated *the ICT Manager* as Information Security Officer who is responsible for:

- co-ordinating the operational implementation and monitoring of this policy and associated guidelines;
- arranging for the review and monitoring of security incidents and investigation of major breaches of security;
- arranging for the policy and guidelines to be updated as new technology and systems change the risk scenario.
- co-ordinating awareness initiatives across the Council to maximise impact and effectiveness.
- developing administrative, physical, and technical security controls to meet the Council's information security objectives.
- joining forums, user groups, institutes and other relevant organisations to keep up to date with security and regulatory issues.

6.4 HR & OD Manager

This policy will be reviewed regularly by the HR Manager, in consultation with the Information Security Officer and representatives from recognised Trade Unions, to ensure that:

- a copy of this policy is contained within the Induction Pack issued to new staff and a signature of receipt and understanding held on individual personal files before access to computer systems is provided.
- induction training courses outline the key elements of this policy, provide general guidance on the use of electronic systems and cross-reference with the Council's Equal Opportunities Policy.

The HR & OD Manager will take responsibility for any disciplinary actions resulting from breaches of this policy.

6.5 Heads of Service

Heads of Service will overview the implementation of, and adherence to, the policy within their respective Service Areas. Service Area Managers will ensure that:

- this policy is transmitted to all staff, contractors, consultants and agency staff within their Service Area and to all Members who access Service Area systems.
- new starters attend the council's ICT Induction training.
- the procedures within this policy are complied with and appropriate security measures are established and maintained.
- Service Area property used by an employee is returned prior to leaving/terminating employment with the council.
- contingency plans exist to enable service delivery in the event that the council's computer facilities and services are unavailable
- Heads of Service are also designated Information Asset Owners and are responsible for the management of information risk for their service's information assets. This

includes ensuring that their information assets are properly recorded in the Council's information asset register.

6.6 Line Managers

Line managers have day to day responsibility for ensuring that their staff understand and comply with this Policy and associated guidelines.

6.7 System Owner

For each information system, there shall be a named senior member of staff designated as System Owner - typically the manager or section head responsible for the principal service(s) for which the system operates. The System Owner is responsible for:

- determining who can access the system and the scope of operation available to each permitted user as appropriate to the user's business needs;
- approving remote access connections from third parties, including the system supplier;
- ensuring that the system is appropriately licensed for its business use and that the correct number and type of licence exists for the users of the system;
- removing users and associated access rights from the system when an employee leaves the organisation or changes job role and no longer requires access to the system;
- ensuring that a risk assessment is carried out on a new or replacement system, prior to going live;
- ensuring that the system is maintained in an effective and controlled manner;
- ensuring that all changes to the software are performed to an agreed change control mechanism;
- ensuring that staff immediately report any violations or misuse of the system to their line manager;
- ensuring that the sharing of information between internal departments, the public, suppliers, contractors and partners is in accordance with Council security policies and the Data Protection Act.
- dealing with requests under the Data Protection Act / Freedom of Information Act in a timely manner.

The ICT Services Applications Support Manager is responsible for ensuring that each system has a nominated System Owner prior to any system going live and that all System Owners are contacted at least annually to reaffirm their role and responsibilities.

6.8 Information Governance Manager

The Information Governance Manager is responsible the development, implementation and maintenance of the Information Governance Framework and the coordination of all component elements that ensure compliance with information law and best practice.

6.9 All Users

All end users of information systems are responsible for ensuring that the Information Security Policy and guidelines are complied with.

In addition, all staff must take reasonable steps to protect the information in the care of Warwick District Council, and report all actual or suspected information security incidents.

Staff are encouraged to join mailing lists, forums and other relevant organisations that provide accurate and timely information/ advice on information security issues relevant to their job role.

6.10 ICT Services

ICT Services has specific responsibilities for managing the security of the ICT service that it provides, but is not responsible for the security of the information that they process. That is the responsibility of each System Owner, whose role is to establish and manage the security of the information in their application. In addition, ICT Services is responsible for:

- Wide Area Network Security
- Local Area Network Security
- Electronic links to and from third parties
- Corporate backup services

6.11 Internal Audit

The principal role of the Council's Internal Audit Service is to provide an independent opinion to management on the control environment governing all the Council's affairs and activities. As part of this, Internal Audit will:

- plan and implement reviews to evaluate and report on risks and controls in relation to ICT provision and management of the ICT infrastructure;
- undertake tests to verify that Council policies, guidelines and procedures are being complied with;
- provide general advice to management on risks and control in relation to ICT provision, including the implementation of new systems and technologies.

To facilitate the above, to support the Council's audit plan and to undertake any necessary investigations, the Internal Audit function shall be given temporary access to those systems, applications and data required to meet their audit needs. Temporary access to data shall be granted by ICT Services without prior approval from the appropriate system owner. Internal Audit must notify ICT Services when access is no longer required to enable permissions to be reset.

6.12 Human Resources

Human Resources will:

- provide the ICT Services Helpdesk with a list of Starters at least two weeks before their start date and Leavers one week before their last working day so that user information is kept up to date.
- ensure that background verification checks on all candidates are undertaken in accordance to the relevant laws and are proportional to the business requirements. See **Human Resources Information Security Policy** for further details.

7 Joint Working – Warwickshire Councils

ICT Services will enable network access for any of the Warwickshire authorities if authorised to do so by a member of Warwick DC's Senior Management Team. Under such Circumstances staff from the connecting Warwickshire authority will not be required to undertake Warwick's security induction training, providing the connecting authority has a current CESG approved Code of Connection and the staff member has completed the connecting authority's security induction/training.

If a connecting staff member is responsible for any security breaches, the connecting authority will be responsible for undertaking any associated disciplinary action.

Access to individual Council systems will be subject to approval by the relevant System Owner. System Owner responsibilities apply to connecting staff members.

8 Confidentiality of Information

All employees and contracted third parties working for the council must observe the utmost care and attention in dealing with personal information – in no circumstances must any information about the Council or its customers be divulged to anyone outside the organisation, without proper authority from a line manager who must ensure that such a disclosure would not contravene the Data Protection Act 1998, the General Data Protection Regulations or Data Protection Act 2018.

All information developed by or on behalf of Warwick District Council will remain the property of Warwick District Council and shall in no way be sold, copied or used without the express permission of Warwick District Council.

All third parties who require access to council information are required to sign a confidentiality and non-disclosure agreement. If network access is required, then connections must be approved in accordance with the Council's **Third Party Network Access Policy**.

For further information on data handling, please see the council's **Data Handling Policy**.

9 Contingency Planning

It is the responsibility of Service Area Managers to ensure the availability of the service(s) under their control in the event of various system breakdown scenarios. Service Area Managers must ensure that alternative procedures and processes are in place to deliver the service in such scenarios and that appropriate data is available. These Scenarios might typically include failure for two hours, one day, one week, or one month.

Service Area Managers are responsible for ensuring that any data that has been entered into a computer system is recoverable in the event that their system(s) fails before the system is next backed up.

Each system contingency shall form part of an overall Business Recovery Plan determined by Senior Management and co-ordinated by the Chief Executive.

10 Inventory Management

ICT Services is responsible for maintaining a current and complete inventory of production, test and hosted systems hardware and software. (See **Software Policy**)

All software packages used on Council owned, leased or rented computer systems, including copyrighted freeware and shareware, must be registered prior to installation in the Council's Inventory managed by ICT Services.

All ICT hardware will be registered, when procured, with a unique asset number recorded on ICT's inventory.

Employees should not move PCs, printers, scanners or other ICT equipment without the permission of ICT Services Helpdesk

11 Usage of Council Owned Hardware and Software

11.1 Responsible Usage

Council electronic equipment and software must be used in a responsible, legal, and ethical fashion. Staff or Members must not take any action that could bring the Council into disrepute, cause offence, interfere with Council work or jeopardise the security of data, networks, equipment or software.

11.2 Personal Use

Council computer equipment and software, as well as telecommunication services and other electronic equipment, are for Council business purposes. Occasional personal use by staff is permitted at the discretion of line managers provided it does not interfere with Council work, is not conducted in Council time, conforms to this policy and is not associated with personal business interests. However, under no circumstances should staff/members allow Council owned equipment to be used by individuals not employed by the Council. For further clarity, this means family, friends, etc are **NOT** permitted to use Council equipment (laptops, PCs, phones, or any other devices supplied by the Council).

Members may use Council equipment for personal use and for Council and ward matters. However, Council equipment must **never** be used to promote support for a particular political party nor for conducting personal business interests.

11.3 Personal Equipment

Those who use their own PCs or other equipment to connect to the Council's network remotely and who use that connection in contravention of this policy will face disciplinary action in the same manner as those using Council owned equipment.

11.4 Workstation Risk Assessments

Risk assessments must be carried out by each Service Area on workstations used by staff in their Service Area. Help on this can be obtained from the Council's Health and Safety Officer.

11.5 Connection of Equipment / Devices

No hardware, such as peripherals or laptops, should be connected to the Council's network without the permission of ICT Services.

Representatives of outside agencies visiting WARWICK DISTRICT COUNCIL premises are not permitted to connect laptops or other items of portable equipment to the Council's internal network.

Only ICT Services are permitted to install software and hardware on council owned PC's and equipment. The connection of personal portable devices such as cameras, phones and tablets to a Council owned PC constitutes hardware installation and presents a risk to the integrity of the network and therefore is strictly prohibited without prior agreement by ICT Services.

For further information on connecting peripheral devices such as USB memory sticks, cameras, mobile phones, etc, please refer to the Council's **Removable Media Policy**.

11.6 Personal Data Storage

Staff must **not** store personal data on Council equipment or the corporate network. This includes, but is not restricted to, photos, videos, music files etc.

In the event that personal data is identified on Council devices, including the corporate network, the Council shall have the right, in its sole discretion, to remove (whether by remote means or otherwise) all or any personal data from the device. In no event will the Council be liable for any damages resulting directly or indirectly from the deletion of personal data

12 Secure Disposal or Re-use of Equipment

All items of equipment containing storage media (e.g. fixed hard disks) must be checked by ICT Services to ensure that any sensitive data and licensed software is removed or overwritten prior to disposal.

Equipment that is to be 'donated' to other organisations or sold must have all data erased via overwriting. This must be done via an approved tool which is capable of deleting data so recovery is impossible. All Council owned software which is still required by the Council for compliance reasons, must be removed.

If a third party disposal company is used, certificates confirming the destruction of all data on the equipment must be provided.

Damaged storage devices containing sensitive data may require a risk assessment, to determine if the item should be destroyed, repaired or discarded.

All Waste Electrical and Electronic Equipment (WEEE) shall be disposed of in accordance with European Community directive 2002/96/EC.

13 Corporate Desktop Security Profile

ICT Services is responsible for identifying and implementing a Corporate Desktop Security Profile which will enforce a consistent and best practice approach to desktop security.

14 Unattended Workstations

If a workstation is to be left unattended, users must save all open documents and securely lock their PC using the [CRTL][ALT][DEL] [lock computer] facility. This will prevent unauthorised access to PCs and the use of unauthorised credentials to gain access to applications.

However, if the workstation is to be left unattended for a significant period of time, e.g. going to lunch or a meeting, then all open systems must be closed and the workstation should be locked as above.

15 Intellectual Property

Warwick District Council owns all data, information and software design or code produced by or on behalf of WARWICK DISTRICT COUNCIL, regardless of format, unless otherwise specified by a valid third party agreement.

All information or Software developed by or on behalf of the Council will remain the property of WARWICK DISTRICT COUNCIL and must in no way be sold, copied or used without the express permission of the Council or authorised designate.

All contracts with third parties, including contract personnel, must define the ownership of software and information. Any information used shall comply with relevant legal instruments.

16 Password and Logins

All users of any Council computer system must be issued with an individual password and login, unless a generic user name and password has been approved by the System Owner.

Employees and Members must adopt sound password practices:

- Passwords must be kept secret and must not be disclosed to others.
- Passwords must not be recorded unless the record is stored securely.
- If a Password is disclosed, for whatever reason, it must be changed immediately
- Passwords must not be saved and option boxes for saving passwords must not be checked (i.e. not ticked).
- Passwords must be changed at frequent intervals.
- Passwords must be a minimum of six digits and must be alpha-numeric (unless there are system constraints)
- Passwords must not be recycled (i.e. used again)
- If temporary passwords are required these must be changed or deleted as soon as possible
- Temporary passwords must be conveyed to users in a confidential manner.
- Where generic user logins are in use, the password must be changed when a member of staff leaves Warwick District Council or moves to another job role.
- Employees and Members must use only their own user name and password to access any system, unless a generic user name and password has been approved by the System Owner.

Employees and Members must not allow anyone else to use their user name and password. This is not only a security risk but could lead to false accusations of misuse.

Users must not attempt to find out the password of another user.

Outside suppliers dialling in remotely to the Council's network to support applications are not required to have individual user names and passwords, but should have a company user id and password created.

Where laptops are used for home logins the password file must not be saved (i.e. the dialogue box indication to save the password should not be activated) in order to prevent unauthorised access if the laptop is lost or stolen.

17 Computer Viruses

Anti-virus software is running in the background on all Council PCs, but all PC and laptop users still face a potential threat from computer viruses.

Users should ensure that they are aware of the nature and danger of computer viruses and should take all care to ensure that they are not introduced to the Council's computers or its networks.

There are two types of viruses. A benign virus may simply flash an annoying message on the screen, whilst a malicious virus may destroy information. Viruses are most frequently spread via the downloading of files from the Internet, through the use of an infected memory sticks or CD or by attachments to email messages.

To reduce the chance of getting a virus, users should virus check all discs before using them. Software should only be downloaded from the Internet by the Council's ICT Services. ALL suspected viruses must be reported to the ICT Services Helpdesk IMMEDIATELY.

Any information about virus warnings should be given to ICT Services who will check the information and issue a message to all users if appropriate.

Employees and Members should be cautious about opening email from an unknown source and should not open attachments to such emails. Any suspicious emails should be referred to ICT Services Helpdesk.

Users should also refer to the Council's Removable Media Policy.

18 Compliance, Monitoring and Assurance

The Council is ultimately responsible for all business communications but will, as far as possible and appropriate, respect your privacy while you work. It is important, however, that you understand that the Council will monitor the use of all of its ICT Equipment for reasons which include:

- Ensuring that the Council's procedures and policies are adhered to;
- Monitoring standards of service and staff performance;
- Record keeping;
- Preventing or detecting unauthorised use of Council Equipment and systems, including compliance with this policy;
- Complying with legal obligations and preventing and detecting criminal activities; and
- Maintaining the effective operation of the Council's communications systems.

In particular the Council will monitor the use of the telephone, email and internet traffic data (i.e. sender, receiver, subject, attachments to emails, numbers called and duration of calls and pages/files downloaded from the internet) at a network level, irrespective of whether they are for Council or private use. The Council may also monitor the content of communications where it appears to the Council that the use of the ICT equipment is being abused or used inappropriately. More details on the use of monitoring information is given in the Monitoring Policy.

You should be aware that this monitoring may reveal personal information about you, for instance which websites you visit, the identity of people you email for personal reasons etc.

If inappropriate use of Council equipment is suspected, a line manager may request access to the required log files. ICT Services will seek authorisation from the individuals Service Area Manager prior to their release, and will assist in the interpretation of the logs. Where necessary ICT Services, the HR Services Manager or the Chief Executive will advise on the suitability of material, investigate sites or seek the opinion of the police.

Further to the above, the Council will only disclose information obtained through monitoring to:

- A relevant external agency if required by law or regulatory compliance; or
- To those directing an investigation for criminal, civil or disciplinary purposes.

Information obtained through monitoring will only be held for as long as operationally necessary or required by compliance regimes such as the Code of Connection (CoCo). However, monitoring logs for Internet and e-mail usage which are not required for disciplinary or legal proceedings will only be retained for two weeks. Where information is part of disciplinary proceedings, the information will be kept in accordance with the retention period for such proceedings.

All of the above monitoring will be carried out for legitimate purposes only and in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Furthermore the Council reserves the right to access data files held within personal folders or password protected files in connection with the legitimate business of the Council.

19 Policy Compliance

Any breach of this policy by staff may lead to disciplinary action being taken and, in cases of gross misconduct, termination of employment without notice. Some cases may result in the council informing the police and criminal action may follow. For Members, references in this policy to disciplinary action will be considered under the Arrangements for dealing with complaints about Councillors and this document will be treated as a local protocol for this purpose. Any breach of this policy by suppliers will be subject to appropriate action by the relevant Deputy Chief Executive.

Should the Council be sued due to misuse of Council ICT equipment or the actions of a user which contravene this policy, the Council reserves the right to claim damages from the authorised user concerned.

19.1 Infringements of Policy

In support of the above, attention is drawn to the following infringements:

- Viewing, creating, circulating, distributing, storing, downloading or printing material that might be offensive, illegal, pornographic or sexually explicit, that brings the Council into disrepute or that exposes it to legal action. For staff, such action is likely to be considered as gross misconduct and, if so, would result in termination of employment without notice. The Council reserves the right to recover defamatory material and use it as evidence against an individual.
- Using communication facilities for purposes that may be illegal or contravene Council policy such as disclosing official information without authority.
- Hacking, hoaxing, spamming, phishing, damaging Council or other networks

- Knowingly using unlicensed software.
- Bulk personal e-mailing without permission.
- Using communication facilities for unreasonably extensive private use.

20 Policy Governance

The following table identifies who within Warwick District Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Accountable	Deputy Chief Executive & Monitoring Officer
Responsible	ICT Services Manager
Consulted	ICT Steering Group, Human Resources, CMT, Trade Unions & Employment Committee
Informed	All council personnel, temporary / agency staff, contractors, consultants, suppliers and Members.

21 Review & Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the council's Information Security Officer.

22 References

The following statutes, policies and other references are applicable:

- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Obscene Publications Act 1959
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Protection of Children Act 1978
- Telecommunications Act 1984
- Criminal Justice Act 1988

- Protection from Harassment Act 1997
- The Data Protection Act 1998
- General Data Protection Regulations
- (following Royal assent) The Data Protection Act 2018
- Human Rights Acts 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act, 2000
- Copyright, Designs and Patents Acts
- European Convention on Human Rights
- Dignity at Work Bill
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- BS7799 Code of Practice for Information Security Management
- Disposal of Surplus and Obsolete Equipment Guidelines

The following Warwick District Council policy documents are relevant to this policy:

- Staff Handbook
- Equal Opportunities Policy
- Disciplinary Policy and Procedure
- ICT Strategy
- The Council's Constitution

Appendix 1

1. ISCP Sub-Policies

Policy	Description
Internet Acceptable Usage Policy	Describes the acceptable use of the Internet
Email Acceptable Usage Policy	Describes the acceptable use of the Council's email facilities.
Removable Media Policy	Establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media e.g. CDs, DVDs, memory cards, USB memory sticks, USB hard drives
Remote Working Policy	This policy covers the provision of facilities to users to have secure and reliable remote access to any of the Council's information systems from locations other than their usual office base and/or from their own home.
Software Policy	Describes the policy associated with Council software ownership including acquisition, software use and licensing.
Information Security Incident Management Policy and Procedure	How to react appropriately to any actual or suspected security incidents relating to information systems and data.
Data Handling Policy	It aims to identify and protect data which is personal, sensitive and/or critical to the organisation, by describing how data should be handled i.e. emailed, posted, etc.
PSN / GCSx Mail Acceptable Usage Policy	For users who require pan-government secure email. A separate secure email address is issued for this purpose.
Card Data Policy	This policy ensures that all credit and debit card payments received by the Council are processed in accordance with PCI security standards.
Monitoring Policy	Explains the monitoring arrangements that the Council has in place for electronic communications.
Mobile Phone Policy	This policy gives guidance to staff on the acceptable use of a Council owned mobile phone.
Physical & Environmental Security Policy	Sets out the minimum level of physical security for Warwick District Council facilities to safeguard information resources, including visitor/contractor access and deliveries.
Digital Forensic Readiness Policy	Describes the requirements to collect, preserve, protect and analyse Digital Evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or in a court of law
Human Resources Information Security Policy	Ensuring staff are vetted, authorised and trained to use Council ICT systems.