CRANLEIGH PARISH COUNCIL

Information Security Policy

1 Introduction

1.1 Background

Cranleigh Parish Council has a large investment in information, which is an essential resource that is used either directly or indirectly in the delivery of all of the Council's functions. The Council is the custodian of electronically and manually stored information, much of it of a personal and sensitive nature. When we receive the information, we are trusted to look after it and to make sure we comply with our legal responsibilities. There is a high reputational risk attached to the misuse or unauthorised publication of sensitive information.

In order to carry out the business of the Council, much of this information must be accessed by computer application systems and transmitted across communications networks operated by the council. It is vital therefore that it is protected from any form of disruption or loss of service and it is essential that the availability, integrity and confidentiality of the IT systems and data are maintained to the highest standards.

Information Security is not limited to managing ICT. It also covers the physical security of buildings, equipment and manual records; procedures for starters and leavers; good practice advice, and a reporting mechanism should an incident occur. Staff guidance on the use of the network, email and the Internet exists in the IT, Email and Internet Policy supplement the general guidance within this document.

Information is a valuable asset, which must be protected to ensure the effective and accurate operation of the systems on which the Council relies. There are legislative and regulative obligations placed on the Council in respect of the confidentiality of much of this information, which must be observed. Failure to protect information could jeopardise the ability of the Council to provide efficient, cost-effective services to the general public.

It is essential that all staff are aware of their responsibilities under the policy and that Information Security controls are established to prevent information being accidentally or maliciously misused, corrupted, lost or destroyed.

1.2 Information Security

The purpose of Information Security is to protect information in the following key areas:

- Confidentiality ensuring that information is protected against unauthorised access or disclosure.
- Integrity ensuring that information is accurate, complete and free from corruption.
- Availability ensuring that information is available when it is required.
- Non-repudiation ensuring the ability to prove the origin of information or disprove a denial of receipt.

1.3 Purpose of the Policy document

The purpose of this Information Security Policy document is to define the stance of Cranleigh Parish Council with regard to certain aspects of information security which are described in the body of the document.

The policy document is a framework for the establishment of standards and procedures for information security management and is based on the guidance contained in BS7799, a code of practice for Information Security Management.

The policy document has a number of appendices which give practical advice and guidance to users in specific areas of information security.

1.4 Scope

The Information Security Policy applies to all Council locations and elsewhere where Council business is undertaken, and applies to all staff, councillors, agents, contractors and volunteers working for, or on behalf of, the Council.

The policy will form part of the standard contract terms and conditions, or other agreement, for external users working on behalf of the Council. Contractors or other external users are directed to the Clerk.

The generic terms user and users are used within this policy to refer any of above.

For the purposes of this document, the term 'information' covers:

• paper records, whether stored in council premises, off site or in transit between the two;
• data, software, recorded data and images stored on and accessed by computer systems;
• data, software and images transmitted electronically across networks, both internal and external;
• data, software and images stored on removable media or storage.

The guidance within the policy document also applies, where relevant, to other kinds of information which may be printed, sent or received by fax and stored on film or microfiche.

Note: The Council has a specific code of practice for the use of CCTV equipment.

The guidance will also apply to certain manual records covered under UK GDPR. These will include records (e.g. application forms) relating to computerised information and may include manual filing systems where they are structured to enable easy reference to personal information e.g. a personnel filing system. If in doubt please seek advice from the Clerk.

This Information Security Policy is a Council policy and infringements may result in formal action against those found to have breached it . The disciplinary process, offences and outcomes are documented in a Code of Conduct or similar. This process can be found in the staff handbook.

1.5 Objectives

The objectives of the Council's Information Security Policy are:

- To ensure that all users of Council information and Information Technology systems are aware of the need for information security and have an appreciation of their responsibilities.
- To define broad organisational roles and responsibilities.
- To provide a framework which gives guidance on a number of aspects relating to information security, as defined in the policy document.
- To establish the need for every information system to have specific security controls, which are adhered to.
- To establish the corporate level controls to the IT network.

2 Roles and Responsibilities

2.1 Parish Clerk

The Parish Clerk has overall responsibility for the development and implementation of this Policy.

The Parish Clerk will, subject to approval by the Council, develop, publish and maintain Cranleigh Parish Council's Information Security Policy. These activities will include developing, reviewing and auditing procedures compliant with this Security Policy. They will also be responsible for the dissemination of the information contained within the policy. They will oversee the Information Management processes relating to Data Protection, Freedom of Information, compliance with records management good practice and liaison with the Data Protection Officer who advise on corporate issues relating to records management.

2.2 Council System

The Council must ensure that:

- Access controls are in place, which are appropriate to the sensitivity of the information used by the system.
- The major risks which may threaten the security of the information are identified and, where possible, mitigated;
- Instances of misuse or abuse of the system are reported as per section 5.0.
- Checks are made to verify the validity of information which is being entered.
- Efforts are made to prevent and/or detect data corruption.

Netcom IT Solutions Limited is responsible for procuring new software items on behalf of the council; for managing and controlling software licences; for providing a secure area for the storage of definitive versions of software; for the distribution and implementation of new and amended software versions, and for the automated back-ups of networked systems.

2.3 All Users of IT systems – Members, staff and other authorised people

Users of computer systems must ensure that they comply with the guidance contained within the Information Security Policy, and report any actual or suspected breaches via the Clerk. See Section 5 for further guidance on reporting security incidents.

2.4 IT development, support and maintenance staff

Staff working within Netcom IT Solutions Limited are responsible for the support and maintenance of computer systems. Their ICT staff may therefore have privileged access to computer systems and to personal and confidential information in order to carry out their normal responsibilities. They must ensure that they are aware of and comply with the information security provisions relating to each computer system as well as this general policy guidance.

Duties will include ensuring that regular back-ups of both software and data are taken, and copies are stored in a secure remote location and that changes to the system are authorised and made in a controlled and effective manner, including any remote support arrangements agreed with a software provider.

2.5 Monitoring compliance

The diverse nature of this policy means that responsibility for monitoring its compliance will be shared between the Clerk and the Council depending on the facet of the policy being considered.

2.6 Physical Security

Unless otherwise stated, the enforcement of physical security measures is the responsibility of the Parish Clerk for the Council Office, Community Centre, Snoxhall Pavilion and Village Hall.

2.7 Personnel Security

The Parish Clerk is responsible for the security countermeasures to be used in recruitment, whilst staff and contractors are employed, and on termination. In addition, the policy addresses security awareness and training aspects to ensure that personnel are fully aware of their security responsibilities and the necessary security procedures that they use.

3 Legal Requirements

The Council will observe all laws and regulations which apply to Information and computer systems. These include:

3.1 Data Protection Act 2018 - UK GDPR

The Regulation seeks to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information.

The Regulation gives individuals certain rights regarding information held about them e.g. to ask for a copy of the data held about them. It places obligations on those who process information (data controllers) while giving rights to those who are the subject of that data (data subjects). Personal information covers both facts and opinions about the individual. The Council is a data controller and is required to register its uses of the processing of personal data and to comply with the data protection principles to ensures (inter alia) that:

- Data is obtained and processed fairly and lawfully;
- Data held will be accurate and not excessive for the purpose required;
- Data will not be retained for longer than is necessary;
- Data is protected from accidental or unauthorised loss or destruction;

If you require any guidance on the UK GDPR please contact the Parish Clerk or visit the Information Commissioner's website http://www.ico.gov.uk/

3.2 The Copyright, Designs and Patents Act 1988

This Act makes it illegal to copy any piece of software without the owner's permission. Most proprietary software is supplied under a licence agreement which limits the use of the software to specified platforms and numbers of users. Copying of the software will normally be restricted to the creation of back-ups.

To comply with the law:

• all purchased software must have appropriate licence agreements;
• purchased software can only be used on platforms covered by the licence;
• definitive versions of proprietary software and the licence agreements must be stored in a secure place.

Criminal prosecutions may result from infringements of copyright law.

3.3 The Computer Misuse Act 1990

This Act recognises that certain activities constitute computer crime, and provides legal redress against offenders.

Broadly speaking, computer misuse is categorised as:

• attempted unauthorised access to a computer system;
• attempted unauthorised access to information;
• access with a view to personal gain.

Users must report any instances of potential or suspected misuse of computers via the mechanism described in Section 5.

3.4 The Regulation of Investigatory Powers Act 2000 (RIPA)

The Regulation of Investigatory Powers Act 2000(RIPA) governs the interception of communications, covert surveillance operations and access to encrypted data.

A Code of Practice on the Use of Personal Data in Employer/Employee Relationships. has been developed which addresses the impact of the Data Protection Act 2018 on the monitoring by employers of telephone calls, e-mails and Internet access involving their employees. The Council is authorised in relation to its internal communications network to monitor or record all communications transmitted over its system without consent for the following purposes:

(a) establishing the existence of facts;
(b) ascertaining compliance with regulatory or self-regulatory practices or procedures;
(c) ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system;
(d) preventing or detecting crime;
(e) investigating or detecting unauthorised use of the Council's telecoms system;
(f) ensuring the effect of the proper operation of the system.

The Council may monitor (but not record) communications to check whether or not communications are relevant to the Council.

The Council is required to "make all reasonable efforts to inform those people who use the Council's telecom systems that interceptions may take place". Cranleigh Parish Council through this Information Security Policy, informs all users of council systems of its intention to access, record and monitor information in order to ensure the appropriateness of their use of information and activities performed through information systems, facilities, and processes established for Cranleigh Parish Council business purposes. If you require any guidance on RIPA please contact the Parish Clerk

3.5 Freedom of Information Act 2000 (FOI)

The Freedom of Information Act 2000 (FOI) creates a general right of access to information held by public bodies (including local authorities) but subject to wide-ranging exceptions.

The general principle is that any person making a request for information to a public authority is entitled to be informed whether the public authority holds information of the description specified in the request, and, if yes, to have that information communicated to him/her.

The Council has adopted a Freedom of Information Act 2000 Publication Scheme.

For further guidance on the Freedom of Information Act contact the Parish Clerk.

3.6 Human Rights Act 1998

Under article 8 of the Human Rights Act ‘everyone has a right to respect for his private and family life, his home and his correspondence’. Information should be kept securely and only shared in accordance with guidance mentioned elsewhere in this policy.

4 Education and awareness

4.1 Job descriptions

The Council will ensure that:

- Where appropriate, specific security roles and responsibilities are defined and documented in job descriptions.
- Individuals who have a responsibility for the protection of information assets are aware of their specific responsibilities.
- All Council employees are aware of, and have access to information relating to security procedures.

4.2 Recruitment

Appropriate security screening measures may be taken when dealing with applications for employment, especially when the job involves dealing with information which the recruiting officer considers to be sensitive. Certain job roles require DBS checks and further checks will be carried out where the job role involves working with children. These screening procedures may also be invoked if employees change roles within the organisation, and their new role involves dealing with information of a sensitive nature.

The Parish Clerk must sign a request for non-employee access to network. They will be expected to comply with the guidelines set out in this policy.

4.3 Leave of Absence

It is recommended that Netcom IT Solutions Limited be informed of staff being away for an extended length of time (i.e. sabbatical/sickness/maternity) so an account is not inadvertently deleted. Any staff brought into cover any posts may be liable for the cost of additional licences e.g. Outlook because they are considered additional staff.

If a member of staff requires access to information held in the personal folders of an absentee then the permission of Parish Clerk must be obtained in accordance with the process in section 6.12 of this policy. Users are reminded that the IT, Email and Internet Policy applies when accessing data from another person's folders.

4.4 Training

The Council will ensure that all users of IT systems are aware of security requirements and procedures as part of the induction process, and that training is available on the correct and secure use of IT facilities. This is the responsibility of the Clerk.

4.5 Confidentiality

The Council's code of conduct says that it is the duty of staff not to disclose to a third party or otherwise use any of the Council's confidential information either during or after the termination of employment with the Council.

Agency, contract staff and contractors must abide by the relevant conditions of contract with regard to security matters, and may be required to sign confidentiality and nondisclosure undertakings prior to being allowed access to IT facilities, as may volunteers. This is the responsibility of the Clerk.

4.6 Terms and Conditions of Assignment/Employment

The terms and conditions of employment by Cranleigh Parish Council state the individual's responsibility for security. These are included in job descriptions, detail of generic security responsibilities and statements of compliance with legislation such as the Computer Misuse Act 1990, UK GDPR 2018, Copyright, Designs and Patents Act 1988. These also include descriptions of relevant information on the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000, and solicit any consent necessary for the proper conduct of business.

These statements of agreement are reviewed when there are changes to the terms of employment. These are also included in the conditions of service handbook, which is available to all staff.

4.7 Leaving the Council

Before an employee leaves the Council's employment the Clerk should be informed of important information held within their account – email or home directory.

5 Reporting security incidents

It is the responsibility of all users to report any observed or suspected security weaknesses in IT systems or services. The Council will maintain various methods for users to report actual or suspected breaches in security procedures.

Users must not attempt to test or prove suspected weaknesses themselves. Such action may be misconstrued as an attempted breach of security and investigated and dealt with in accordance with the Council's Disciplinary Procedure or Member Code of Conduct, as appropriate. For external users under contract to the Council, such action could be considered to be breach of contract or investigated under the provisions of the Computer Misuse Act 1990.

5.1 Who to report an incident to?

Where fraud and/or money laundering is suspected this should be reported in the first instance to the Parish Clerk or in their absence, GDPR-info Ltd in their capacity as Data Protection Officer. The anti-money laundering policy or the anti-fraud, corruption and whistleblowing procedure may be used for this purpose.

In other cases, staff should normally report actual or suspected breaches in security procedures via the Clerk.

Members should report actual or suspected breaches of the Policy to Parish Clerk who in turn must report it to GDPR-*info* Ltd as our Data Protection Officers.

5.2 Netcom IT Solutions Limited

Users should report or discuss security matters of a general systems nature rather than individual behaviour with Netcom IT Solutions Limited.

The Netcom IT Solutions Limited staff record all incident reports, and will maintain an incident category for security incidents. Netcom IT Solutions Limited will ensure that steps are taken to test suspected weaknesses, and to rectify breaches.

Issues relating to viruses should be reported to Netcom IT Solutions Limited.

5.3 Confidentiality

The Council's Whistleblowing Policy provides guidance as to how employees can raise a concern without fear of recrimination.

5.4 Disciplinary proceedings

This Information Security Policy is a Council policy and infringements may result in the invocation of the Council's Disciplinary Procedure (in respect of staff) or Member Code of Conduct (in respect of Members).

6 Policy Statements

Section six sets out all of the policy statements that inform the Information Security Policy. It explains how the council will enforce information security.

6.1 Identification and control of assets

The Council will identify all assets which are important for the provision of IT systems and services. Assets can be characterised as:

- Information databases and files, documentation and manuals, procedures and plans etc.
- Software applications, operating systems, tools and utilities which may be developed in-house, or bought-in packages.
- Physical computer and network hardware, ancillary equipment, furniture, telephones etc.
- IT Services will maintain inventories of all computer hardware and software. IT equipment must not be purchased directly or without their knowledge.

6.2 Procurement

All requests for new equipment and software must be agreed by the Council to ensure that what is bought for use on the Council's network is both compatible and appropriate in terms of the requirements of this Policy.

6.3 Inventory

Assets which are deemed to be an important component of computer systems or service delivery such as base units and monitors will be physically identified and their existence will be recorded in the IT Inventory. This is used as a key component of the Netcom IT Solutions Limited system, provide information for the insurance policy and a means of recharging IT costs. The Council is are responsible for procuring, identifying and recording assets of this nature, and for maintaining the IT Inventory. Netcom IT Solutions Limited also maintain an inventory of the Council's software and software licences. The IT Inventory forms part of the Council's general inventory.

All key equipment and software assets at all sites are supported by a maintenance contract.

6.4 Change Management

All changes to physical and software assets must be made under the control of Netcom IT Solutions Limited. The Clerk must ensure that any changes made to the assets for which they are responsible are assessed as to whether there is any impact on security controls

6.5 Physical and environment security

The Council will ensure that the following general controls on physical access and security are maintained.

- Council offices and areas accessible only by staff, Members and authorised visitors will be protected by appropriate security controls from areas of Council premises accessible by the general public.
- Wherever possible visitors to Council premises will be supervised. Panic buttons are installed under staff desks, Council Chamber, Village hall foyer, small kitchen and stage.
- All staff are aware of the specific actions they need take during a bomb warning.

- Suitable secure accommodation has been created within locations containing information or equipment in order to protect these facilities from unauthorised access.
- Fire Alarms are tested weekly and the council holds fire evacuation tests twice a year. has fire extinguishers throughout the buildings.
- Natural Disaster/Lightning - The vulnerability to a natural disaster for all sites has been assessed and at this time it is not classed as a great risk to the council or its information systems.

6.6 Information security

Users must ensure that information considered to be sensitive to which they have access, such as passwords, computer discs etc., are locked away when offices are unattended.

The Clerk must ensure that suitable facilities are provided for the storage of sensitive information. The nature of the information will determine what is suitable. This could include a locked desk drawer, locked cupboard or in some instances a safe.

Unwanted equipment and media must be returned to Netcom IT Solutions Limited for reuse or disposal. A third party contractor carries out the removal of unwanted equipment and media, who certify that all media is securely erased before disposal of the equipment.

Information systems media, such as backup tapes, in transit to secure storage are encrypted to protect data from unauthorised access, misuse or corruption. They are stored in a locked cupboard at an alternative site.

6.7 Maintenance of manual records

All staff should take steps to ensure that they comply with the council's records Management Policy and ensure good practice for the management of paper records.

The Council does not operate a classification scheme to cover all records. Steps must be taken to make sure that all records are accessible, including those held in personal files to ensure the council can provide information on request. This is particularly important in relation to Access to Information requests (i.e. Freedom of Information, Data Protection, Environmental Information Regulations).

6.8. Equipment security

Netcom IT Solutions Limited must ensure that appropriate security measures are considered when positioning, installing and connecting new or relocated equipment. These measures include prevention of unauthorised access, either directly or remotely and prevention of unauthorised copying, modification and deletion of information and software.

6.8 Off-site considerations

The Council must comply with the Data Protection Act 2018 (UK GDPR), which includes the principle 'to take appropriate technical and organisational measures' to guard against unauthorised or unlawful processing of data or accidental loss.

Management authorisation must be acquired prior to removing Council IT equipment offsite. For practical reasons, staff issued with laptops will be deemed to have received authorisation by virtue of the fact they have been issued with a portable PC.

It is the responsibility of the user removing equipment to ensure that appropriate security controls exist at the off-site location, and that sensible measures are taken to protect equipment whilst in transit. Users should also ensure the security of data in portable computer media e.g. memory sticks is only taken off site when absolutely necessary and the data removed as soon possible after use or transfer.

The Clerk must ensure that a record is maintained of either the current location of portable IT equipment, or the person responsible for it, and must be aware of any provisions regarding the insurance of items in transit or located off-site. Subject to normal domestic security arrangements being applied, items held at home are covered by insurance but items are NOT covered if left in an unattended vehicle.

The council does not have a single policy to cover working away from the office. It does have a lone working policy.

6.9 Personal computers and terminals

The Council will provide Members and staff with appropriate computer equipment to carry out their Council function, and it is the duty of those individuals to ensure that basic security controls are applied to personal computers, printers and other IT related equipment used by them.

These basic controls include:

- Ensuring that the correct start-up and close-down procedures are carried out at the beginning and the end of working periods. For safety, security and environmental reasons all PCs and equipment should be switched off at the end of the day and not left on overnight.
- Ensuring that personal computers are not left logged-in while unattended. The PC should be locked using Windows/L during any absences. Note that there is currently no limit to connection time to the network by authorised users. Remote access timeout is set to 15 minutes.
- Ensuring that no unauthorised software is introduced onto personal computers. Netcom IT Solutions Limited are responsible for the installation of all software.
- Ensuring that password controls are understood and adhered to - this includes the procedures for changing and storing passwords. The network password must be at least seven characters long, contain one alphanumeric digit and must be changed every 40 days. Passwords should not be shared with colleagues, family or partners.
- Ensuring that the standard build of the personal computer is not altered.

6.10 Network

Netcom IT Solutions Limited staff are responsible for the installation, maintenance and management of the Council's internal data networks, and for installing, maintaining and managing links to external data networks such as those owned by other organisations, and the Internet.

Netcom IT Solutions Limited are responsible for ensuring that the network is protected from:

- unauthorised access to information and systems;
- interception of data;
- exposure and modification of data;
- hacking, abuse and misuse.

Netcom IT Solutions Limited are responsible for the introduction of measures to protect the integrity of the network and the information flowing across it. Auditing of the systems runs on an ad hoc basis. Security Audit Trails/Logs are not kept automatically, but can be activated if required.

6.11 The Internet and email

Members and Staff must ensure they comply with the Council's IT, Email and Internet Policy. The policy sets out a list things staff must or must not do relating to the network, internet and email. Staff should be aware that Netcom IT Solutions Limited will monitor use of the network. If any misuse is suspected then the Clerk may request a report of usage to establish whether an investigation is required.

6.12 Access to systems

The Council's computer systems and equipment must only be used by authorised personnel and only in pursuance of their duties.

Staff who require access to the Council's computer systems must first gain authorisation from the who must follow a user registration process.. Staff must make themselves familiar with the relevant log-on, logoff and password control procedures.

If access is required into another users account they should complete an Employee data access request form, having made efforts to contact the individual concerned for permission/notification and follow the guidance set out in the IT, Email and Internet Policy.

6.13 Development and maintenance

Significant changes made to the Council's computer systems must be assessed for their security implications by the system owner together with Netcom IT Solutions Limited. The Council and Netcom IT Solutions Limited are jointly responsible for the procurement and installation of new computer systems, and must ensure that appropriate Information Security controls are included in system design and specifications.

Further advice can also be obtained from the Clerk.

6.14 Back ups

Security copies (back ups) of systems operating on the network will be taken on behalf of users by Netcom IT Solutions Limited at predetermined frequencies. These are automatically scheduled at regular intervals dependent upon the importance and quantity of the data concerned.

The general approach for the backups is that on at least a weekly basis a snapshot of the system is taken (and at least 3 generations are retained) and on a daily basis each of the main business systems is backed up. The nature of the system determines the period for which these are kept, typically 2 weeks.

No information stored on the hard drive of a PC is backed up. Users should ensure that all important information is stored on the cloud. Storage of data that might be required for legislative purposes must always be stored in the cloud. Information stored on portable media such as CDs or DVDs is less secure and is therefore strongly discouraged unless it is for non-essential and non-sensitive material (see 6.20).

6.15 Business Continuity Planning

Council Services are responsible for maintaining the continuity of their own business processes in the event of a major incident. Netcom IT Solutions Limited are responsible for the recovery of IT systems to support Council Services and maintain a separate disaster recovery plan.

There is a managed process in place for developing and maintaining business continuity throughout the information systems. Each service has been assessed to establish how quickly it needs to be established in the event of a disaster.

The Business Continuity strategy will be based on business impact analysis results from the security risk analysis and management review, agreed minimum resource, accommodation, IT infrastructure and communications requirements, and agreed recovery time periods.

6.16 Records Management - Information sharing

All staff who share information with other agencies must be aware of the data sharing guidance relating to personal information.

The council maintains appropriate contacts with law enforcement authorities, regulatory bodies, service providers and telecommunications operators. These include: the Police (for relevant security incidents, especially breaches of the Computer Misuse Act); the Information Commissioner (for relevant Access to Information enquiries) and other public service agencies. Staff should familiarise themselves with the Access to Information guidance set out on the council's intranet system and ask for advice if required.

Information required as part of the 'council records' should not be stored solely in personal user areas that cannot be accessed by other officers. The use of shared folders is encouraged for council records that will not be stored on a document management system or alternative central record.

6.17 Records Management – electronic and manual

The council's responsibilities under section 46 of the Freedom of Information Act 2000 require that the Council properly manages the creation, management, archive and destruction of records, which includes written or recorded information.

The Council is responsible for the management of its retention schedules, ensuring the timely disposal of out of date or inaccurate information.

6.18 Re-use of Council Information

The Re-use of Public Sector Information Regulations, encourage the re-use of public sector information - that is, information for which the council holds the copyright. The Regulations allow any company or individual to re-use information held by for commercial or non-commercial gain. To do so they must apply for a licence and pay any licence fees that the council may impose.

'Re-use' means using the information for a purpose other than the purpose for which the document was originally produced. It is not compulsory for public authorities to allow reuse. At present, the council does not apply any charge over and above those for research or photocopying.

There is separate legislation to cover the sale of the ‘full’ and ‘public’ register of electors, covered by Regulation 111 of the Representation of the People Regulations 2001.

6.19 Confidential waste disposal

The council has a contract for the secure disposal of confidential paperwork.

6.20 Removable Media

Removable media including floppy disks, CDs and USB memory sticks should only be used for transferring business related data to and from the computer.

Media that has been used for home PCs previously must not be used and before the media is accessed on your work PC it must be scanned by the resident antivirus software for viruses and other malware.

6.21 Audit and control

The Information Security Policy has been authorised by the Council. The Clerk manages contents under constant review. Any changes required that are other than of a minor factual nature must be authorised by the Council.

Empowerment to carry out spot checks and audits of equipment, software, users and procedures to ensure conformance to the Policy will be shared between Netcom IT Solutions Limited, Internal Audit and the Clerk depending on the facet of the policy being considered.

Adopted: February 2023

Review; October 2026