Information Systems Security & Acceptable Use Policy

City of York Council

Issue Date: June 2025
Version: 5.6

Table of contents

Attention: This document is uncontrolled when downloaded or printed! Please be advised that the policies, regulations and procedures in this document are subject to change without prior notice, if necessary, to maintain compliance with current legislation and/or with rules and regulations as directed by the ICT Department Management Team (DMT) and/or CYC Corporate Management Team (CMT). To ensure compliance with the most current version of this policy please be sure to review it regularly.

Current Document Status

Approving Body: ICT DMT
Date of Formal Approval: October 2023
Responsible Officer: ICT Infrastructure Manager
Document Retention Period: Until superseded

Version History

Date	Version	Reviser	Comments
	< 4.4		No previous version history
June 2017	4.4	ICT Security Officer	New front cover + added document control
July 2017	4.5	ICT Security Officer	Updated references to other policies (end of document)
November 2017	4.6	ICT Infrastructure Manager	Typo amended re admin password length
March 2018	4.7	ICT Infrastructure Manager	Amendment to password section re reuse and unique passwords
January 2019	4.8	ICT Infrastructure Manager	Additions and rewording of some elements
April 2020	5.0	ICT Infrastructure Manager	New section covering Audio Visual communication systems
October 2020	5.1	ICT Infrastructure Manager	Changes to the printing guidance added
October 2020	5.2	ICT Security Officer	Ported to Markdown

Date	Version	Reviser	Comments
October 2020	5.2	ICT Security Officer	Minor spelling, grammar, style tweaks. Sections flagged for review with comment syntax.
October 2021	5.3	ICT Infrastructure Manager	Updated standard user access control section - passwords.
October 2022	5.4	ICT Infrastructure Manager	Multiple updates and amendments in line with new requirments
October 2023	5.5	ICT Infrastructure Manager	Change to policy on use of Googledrive for approved business cases
June 2025	5.6	ICT Security Officer	General review and corrections

Review History

Review Period: 12 months

Date Reviewed	Reviewed By	Next Review Date
Apr 2020	ICT Infrastructure Manager	Apr 2021
Oct 2020	ICT Infrastructure Manager	Oct 2021
Oct 2021	ICT Infrastructure Manager	Oct 2022
Oct 2022	ICT Infrastructure Manager	Oct 2023
Oct 2023	ICT Infrastructure Manager	Oct 2024
June 2025	ICT Security Officer	June 2026

Purpose

The City of York Council's (CYC) Information Communication and Technology department (ICT) provide computing resources primarily to facilitate a person's essential work as an employee. The objective of this policy is to set out how anyone using CYC Information Systems are to use corporate IT facilities provided to them, what responsibilities they have, and what is acceptable and not acceptable when using the corporate IT facilities.

This policy is in place to protect both CYC and its employees, as inappropriate use exposes all parties to risks and can compromise the integrity and security of the corporate IT systems, compromise the network systems and services, and may cause legal issues.

Information and information technology systems are important business assets. The availability, integrity, security, and confidentiality of information are essential for CYC to maintain service delivery, fulfil its statutory obligations, monitor financial health, provide evidence of legal compliance, and enhance the status of the authority.

The objective of this policy and its associated documents is to assist CYC business continuity and minimise business disruption or damage by ensuring acceptable use of CYC information systems, and preventing or controlling the impact of security incidents. Information security provides the essential framework in which information may be shared, whilst ensuring the protection of information and computing assets.

Scope

This policy applies to:

- All users of CYC ICT systems and employees engaged in work for CYC, including working from home or non-CYC locations;
- All users of the CYC network infrastructure, whether accessed from within the Council or remotely;
- Any other use of the CYC network infrastructure by CYC employees which identifies the person as a CYC employee, or which could bring CYC into disrepute and create a liability for CYC;
- Other people working for CYC, engaged on CYC business, or using CYC equipment and information;
- Elected members;
- All those granted permission to use the CYC infrastructure for any purpose.

Where those using the CYC systems or network infrastructure are not employed by CYC, this policy should be read in conjunction with any local policies, and where any contradictions between such policies occurs, clarification should be sought from the CYC Head of ICT or their representative.

Information Security is the process by which data is secured from inadvertent or malicious changes, and deletions or unauthorised disclosure. The main concerns of Information Security relate to information confidentiality, integrity, and availability. These three factors apply to all forms of information, irrespective of the means of storage or communication, and include information that is:

- Sent via e-mail
- Transmitted across networks

Managers have a key responsibility for communicating this policy to their staff, and in ensuring adherence to this policy. They must discuss this guidance with their staff to ensure compliance within their business area. This policy will be reviewed regularly to take into account changes in legislation, instances of abuse, and concerns from employees/unions.

Actions in accordance with the council's agreed and approved disciplinary procedures including possible dismissal could result, where it is deemed that serious breaches of this policy have occurred, which in turn could lead to a substantial threat to the council's ICT infrastructure or data integrity.

The security of data stored in other, non-digital formats, is dealt with in a separate policy, although many of the principles in this policy will also apply.

Principles

CYC is under certain obligations stemming from contractual and/or legal requirements such as software licensing agreements and the Data Protection Act 2018 (DPA). All users of CYC IT Systems, employees, and elected members are required to assist the council in this by complying with this and related CYC policies, as well as seeking appropriate advice when in any doubt. Representatives of CYC are required to behave in a manner of the utmost professionalism and integrity, ensuring that access to information is strictly limited to that which is needed to perform their role.

The council's ICT systems may be susceptible to malware or attacks by malicious actors given the diversity of connections with external information systems such as the Internet. They may also be at risk from theft of assets, given the open access arrangements in some areas of the authority. Elected members and employees are required to take special care, and observe and use the protective measures published. Any actual or suspected malware incident or attack, or any theft of assets, should be reported to ICT immediately via the ICT Service Desk on Ext. (55)2222 (Internal), or on (01904) 552 222 (External).

Preserving the integrity of the network is paramount to maintaining a continued effective ICT service to the CYC business and service areas. It is therefore very important that no unauthorised/unchecked devices are connected to the network. If in doubt, advice must be sought via the ICT Service Desk on Ext. (55)2222 (Internal), or on (01904) 552 222 (External) before the equipment is connected.

CYC adopts a flexible storage policy to enable employees to use the amount of space on the corporate electronic storage system required for them to perform their duties. There are no hard limits on the quantities of data that can be stored, however, usage will be monitored, and any use or storage of data may be deleted by ICT if it is deemed unacceptable or in breach of this policy.

The City of York Council will comply with all mandatory Information Security related standards including, but not restricted to:

- The Public Service Network (PSN) Secure Extranet Code of Connection (CoCo)
- Payment Card Industry Data Security Standards (PCI DSS)
- General Data Protection Regulations (GDPR)
- Data Protection Act 2018 (DPA)

Roles and Responsibilities

All employees and members are required to familiarise themselves with, and comply with, the contents of this policy, and meet the obligations and responsibilities identified herein.

Managers must ensure that all employees within their direct line of responsibility have read, understood, and comply with the practices and procedures outlined in the Information Systems Security and Acceptable Use Policy, and are adequately trained in the use of any business applications before being granted access to them.

Group chairs must ensure that all elected members have read, understood, and comply with the practices and procedures outlined in the Information Systems Security and Acceptable Use Policy, and are adequately trained in the use of any business applications before being granted access to them.

All Users of CYC ICT Systems Must:

- Only access ICT systems which they have been given the appropriate authority to access by their line manager and/or the system owner.
- Not disclose their password to any third party (including managers, colleagues, contractors, etc.) with the exception of ICT employees who need to log on as a specific user for the purposes of fault analysis and rectification. Should the password be given to ICT, then it should be changed immediately once the fault has been rectified.
- Not use someone else's username or password under any circumstances with the exception of ICT employees who need to log on as a specific user for the purposes of fault analysis and rectification.
- Not write down their username and password or store their username and password on any device, mobile or fixed.
- Lock or log out of their workstation or the machine they are logged into if leaving it unattended.

- Keep all data contained within or obtained from ICT systems secure.
- Not load any non-approved or unlicensed software, including “free” software, shareware, or screensavers onto CYC ICT equipment. This includes downloading applications from the Internet without prior permission from the Head of ICT or their representative.
- Not introduce onto any CYC ICT system any data not connected with the discharge of CYC related duties, unless specifically given authority by the Head of ICT or their representative.
- Not illegally copy any CYC-owned software or data, and not transfer any CYC-owned software or data onto a non-CYC owned computer.
- Not use any functionality in breach of security restriction, unless they have a business exemption signed by a Director and Information Governance, i.e. autocomplete, autoforward, etc.
- Not save CYC data onto cloud storage (e.g. Dropbox, JustCloud, Google Drive, etc.) except where part of a process specifically set up for the sharing of non-personally identifiable information/council data as part of an agreed and managed business process, i.e. the sharing of data between the Council and schools.
- Not introduce onto any CYC ICT computer system any data or software without ensuring it is checked using the approved anti-virus procedure. (Contact the ICT Service Desk on Ext. (55)2222 (Internal), or on (01904) 552 222 (External) for further details).
- Never use their council email account to register on websites unrelated to work, especially social media sites such as Twitter, Facebook, Linkedin, etc.
- Never use their CYC domain password on any non-CYC system or website.
- Ensure that passwords are not reused or similar to the previous, or other passwords. Every password should be totally unique across systems and after a password change.
- Not introduce any copyrighted software or data onto any CYC ICT system without gaining the prior permission of the copyright holder.
- Not use file sharing software or Peer to Peer (P2P) software on machines connected to the CYC network. These include, but are not limited to: Kazaa, Limewire, eMule, Ares, BitTorrent, Direct Connect, Morpheus, etc.
- Not reveal any confidential CYC information (by whatever means) from any computer system to any unauthorised person or organisation.
- Not play games on CYC ICT systems (unless related to work, i.e. educational, etc.), make unauthorised use of Internet connections, or misuse the e-mail system (see CYC Electronic Communications Policy).
- Follow any specific instructions given by the Head of ICT or their representative regarding software, anti-virus procedures, security, acceptable use, or any other aspect of computer systems.
- Not, whilst acting in a supervisory capacity, knowingly allow any other person to carry out any activity in breach of this or any other CYC policy.
- Not remove any software, including but not exclusively, anti-virus, firewall, spyware-blocking, etc. from a CYC ICT system without permission from ICT.

- Complete regular housekeeping of all data owned by them which is stored on the corporate storage system. Documents that are no longer needed, no longer relevant, out of date, or duplicated elsewhere should be deleted to ensure the shared corporate storage resource is efficiently used.
- Not retain or circulate any material that is offensive, obscene, or indecent.
- Not attempt to break into, or damage computer systems or data held thereon.
- Not store sensitive or person-specific data on a non-secure device, hard drive, network share, or removable media, unless the data is encrypted and protected by a password which confirms to CYC's minimum standard.

Housekeeping

All users are required to complete regular housekeeping of all data owned by them which is stored on the corporate storage system. Documents that are no longer needed, no longer relevant, out of date, or duplicated elsewhere should be deleted to ensure the shared corporate storage resource is used efficiently.

Users must not store personal or non-CYC business related data on any CYC ICT system including PCs, corporate storage, laptop, mobile device(s), etc. This includes, but is not limited to, any data including music files, videos, photos, software, emails, documents, etc.

Users must comply with Data Protection and Freedom of Information legislation, which provides guidance on file storage retention and management. For more information, please contact the Information Management Officer or the ICT Service Desk on (55)2222 (Internal), or on (01904) 552 222 (External).

ICT reserve the right to remove any data that is in contravention of this, or any other CYC policy, without notice. The user and their line manager will then be informed, and the appropriate action under the corporate disciplinary procedure will be taken.

All software must be purchased via central ICT procurement. This means that licence details can be recorded centrally which will simplify auditing.

Physical Security

CYC ICT computer and telecommunications equipment, data, and software should be afforded physical security appropriate to its business and intrinsic value. This includes equipment provided for home working.

All hardware assets are subject to the CYC asset tagging process and must be logged in the asset database against the inventory of the user, or the department for which the assets have been purchased.

All staff or department moves must involve the ICT department so that the relevant asset databases are updated. Line management must also approve and record any CYC asset that needs to be taken off site, either temporarily, or on a permanent basis.

The CYC ICT department must carry out the disposal of all ICT hardware and software belonging to CYC, and will manage this process so that information security risk is managed and controlled.

All staff should be aware of the access control to CYC buildings and must not try to enter secure areas to which they do not have expressly permitted access, and must not facilitate access by any other person who does not have express permission to enter the area.

All staff must report any physical security breach of CYC buildings, rooms, secure cabinets, etc. immediately to their line manager and the ICT Service Desk on Ext. (55)2222 (Internal) or on (01904) 552 222 (External).

All staff must protect printed or written data in the same manner they do electronic data. Hard copies of data must not be left unattended and unsecure, must be disposed of confidentially, and must be stored securely.

Audio Visual Conferencing and Instant Messaging

Platforms

Meetings and conferences at which City of York Council business will be discussed must not be hosted on platforms that are not approved or supported by CYC ICT.

Responsibilities

Users of Audio Visual Conferencing and Instant Messaging must:

- Follow the same rules as for email data.
- Not sign up to or into non-approved platforms with their CYC email address and credentials.
- Ensure that they are fully aware of who all parties involved in the conference are before sharing any sensitive, personally identifiable, or commercially sensitive data.
- When personal and confidential information is to be discussed, ensure all participants only either use CYC managed devices or, if there are third-party participants, their own organisation's managed devices.
- Ensure all content whether verbal, visual or text is accurate, relevant and appropriate, and in strict compliance with the same rules pertaining to email content.
- Ensure content is not recorded, copied or forwarded to any other party without the express permission of all parties involved in the conference.
- Ensure when working from outside or inside the office that care is taken to ensure no content is visible or audible to people not directly involved in the conference. This can best be achieved by the use of headset and microphone, ensuring you are in a quiet location and being fully aware of your surroundings.
- Be sensitive to others in the immediate proximity and not cause a nuisance that disturbs others. This can best be achieved by the use of headset and microphone, ensuring you are in a quiet location and being fully aware of your surroundings.

- Ensure that if the file sharing functionality of the platform is active you do not share files that are of a sensitive nature without being fully aware of who the recipient is and without clearly defining what the recipient can and cannot do with that data in accordance will all other policies and data sharing agreements.
- If screen sharing functionality is available in the platform, take care when using this to ensure that there are no sensitive emails, documents or other data, not relevant to the meeting, that is visible on the desktop before presenting a desktop.
- Assess whether the platform they are proposing to use for conferencing and message is secure enough for the information they intend to share, especially personal and confidential information. If in doubt, contact the ICT Service Desk on Ext. (55)2222 (Internal) or on (01904) 552 222 (External) for advice.
- If not using CYC approved systems, notify meeting participants before conferencing and messaging, that the third-party application being used could potentially introduce privacy risks.
- Wherever possible, ensure they enable all available encryption and privacy modes when using such services.
- When not using a system approved and supported by CYC ICT, review the platform provider's privacy notice, especially around how they potentially may use voice and messaging data, e.g. for marketing purposes.
- Ensure a procedure is in place where information held on equipment in their area in any non ICT supported system is searched, and relevant information retrieved for both FOI/EIR requests and SARs (this is for the individual business user to arrange and cannot be facilitated by ICT).

Printing

Responsibilities

To protect the integrity of data users must:

- Not attempt to print personally identifiable or commercially sensitive data to a non-CYC print device without the express permission of the data owner
- If given permission to print outside a CYC office, must comply with all the rules and guidance from the SEC102 – Risk Acceptance for Printing at Home Form, namely:

  – Read and comply with all relevant CYC policies and procedures
  – Not, under any circumstances, leave any printed documents unattended containing such information.
  – Securely store any printed documents containing such information in a lockable draw/cupboard when you leave your working area/desk.
  – Not dispose of any such documents in personal waste at home, even if shredded. All prints must be securely stored in a lockable draw/cupboard until it is possible to

securely transport them to a CYC office for disposal in a designated confidential waste bin.

  - Ensure that your home network is secure, including making sure you have an appropriate complex password on any Wi-Fi network you use, and that you are not using the default router admin password supplied with the router.
  - Ensure that any SMART features of the device are switched off if applicable and no data is stored on the device in memory.
  - Not use the 'print over the internet' feature which some printers come with.

Malware Protection

To protect the integrity of software and information:

- Directorates must ensure that up to date anti-virus software is installed on all standalone PCs; assistance can be obtained by contacting the the ICT Service Desk on Ext. (55)2222 (Internal) or on (01904) 552 222 (External).
- Malware protection and updates for all servers and PCs that connect to the CYC corporate network will be deployed automatically via a centrally managed service that is delivered and supported by CYC's ICT department.
- Updates to devices and software will be deployed automatically by ICT. It is the responsibility of all users of CYC laptops, PCs, smart devices, etc, to ensure they have the latest up-to-date corporate antivirus software installed, and that they install any updates as requested on devices.
- If a laptop is suspected to have a virus or contain malware, then guidance should be sought from the ICT Service Desk on Ext. (55)2222 (Internal) or on (01904) 552 222 (External) before connecting to the CYC network.
- All users of CYC ICT computers and laptops are expressly prohibited from removing the corporate anti-virus software from any device that will be connected to the CYC network, or installing any additional antivirus software. Any device that does not have the corporate antivirus software installed must not be connected to the CYC network at all. All enquiries relating to this should be made via the ICT Customer Service Desk.
- All malware or suspected malware must be reported to the ICT Service Desk on Ext. (55)2222 (Internal) or on (01904) 552 222 (External) immediately.

Access Control

To maintain adequate security of data:

- Each employee has a personal responsibility for password security and must not disclose their passwords to any other individual.
- Users must never use their CYC domain password on any non-CYC system or website.
- Users must never write down their password or store it where someone else may have access to it.

- Users must ensure that passwords are not reused or similar to the previous or other passwords. Every password should be totally unique across systems and after a password change.
- Information Systems must be protected by password security to ensure unauthorised access cannot be gained onto PCs, servers, the network or applications.
- All new systems should force periodic password renewal automatically and should comply with this and all other CYC policies.
- Directorates and system owners/data owners should assess whether their critical systems require additional password security.
- Unique passwords should be used for each system and not reused on multiple systems. All username and password accounts on ICT systems must be de-activated for officers who leave the authority. It is the responsibility of their line manager or their authorised representative to inform ICT of any leavers or movers.
- All requests for elevated levels of access accounts on PCs, laptops and servers etc, must be accompanied by a business case from the appropriate line manager, and will be granted at the discretion of the Head of ICT, or their approved representative on an individual basis.
- Systems will be set to lock out users after multiple failed login attempts. To unlock accounts, users should use the self serve password reset function via the reset.york.gov.uk website.
- Generic accounts and passwords will only be granted in exceptional cases and with a supporting business case signed by CYC Head of ICT or their approved representative.
- Accounts with elevated or administrative privileges must not be used for accessing the internet or email, and not for general everyday operational tasks.

Standard User Access

Passwords are case sensitive, and should not be nouns or names that could be gleaned via guessing, or social media snooping (i.e. partners, children or pets names). Passwords should also not be adjusted incrementally when changed (i.e. rover1, rover2, rover3, etc.).

Passwords MUST meet the following criteria:

- Must be in the format of three random words which must be separated by a space (for example: daring lion race).
- Must be at least 10 characters long (including the spaces).

Passwords can contain a mix of upper and lower-case, alpha-numeric and special characters if you wish. They will be automatically checked to ensure the password you have chosen is secure and hasn't been seen in previous breaches or uses words that are in a blocklist, but it is your responsibility to choose a secure password and not something you use elsewhere.

- If you choose a password between 10 and 14 characters your password needs to be changed every 90 days.

- If you choose a password 15 characters or more your password only needs to be changed every 365 days.

Domain Admin/Elevated Privilege Access:

Due to nature of these accounts they are only given to a very small number of ICT staff and are audited on a regular basis. A valid business case must be submitted before these type of accounts are given and will not be given to anyone outside ICT. A policy is now in place (like with standard user accounts) that will force all users with these accounts to change their login password every 45 days.

Passwords are case sensitive and should not be nouns or names that could be gleaned via guessing or social media snooping (i.e. partners, children or pets names).

Passwords should also not be adjusted incrementally when changed (i.e. rover1, rover2, rover3, etc.).

All passwords must be 14 characters or more; preferably passphrases containing three random words, and must contain characters from three of the following five categories:

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek, and Cyrillic characters).
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek, and Cyrillic characters).
- Base 10 digits (0 through 9).
- Non alphanumeric characters: ~!@#$%^&*_-+=`|(){}[]:;"’<>,.?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

Administrator accounts may only be used for administration tasks and must not be used for every day operational work. These accounts may not be used to access email or internet, and never used for subscribing to web services.

All administrator access to servers is via a jump server and the passwords are managed in a system called Password Manager Pro. Passwords are randomised by the system for check out and one time use, by those who are given privilege to do so.

All activity carried out while logged in with an admin account is logged step by step for replay and audit purposes.

All additions or changes to the group who have access to use them is logged and monitored by AD Manager Pro, with alert emails going to managers advising of any change.

All access to live production servers must be via a dedicated hardened jump server with no internet access.

All admin access must be submitted on a **Request for Elevated Privileges Form**, available from the ICT Service Desk, and may need a **Managed Risk Form** prior to approval.

Network Security

To safeguard the telecommunications network and information transmitted across it:

- All remote connections to the CYC ICT telecommunications network must be approved by ICT and be subject to normal managerial control.
- No equipment should be connected to the CYC ICT telecommunications network before CYC ICT has carried out a network impact assessment. This assessment must confirm that the equipment conforms with all CYC ICT standards.
- Secure network connection methods must be employed for the remote connection of staff and partner organisations, e.g. appropriate authentication and firewalls.
- All LAN equipment should be housed in a secure room with access control.

Investigation of Alleged or Potential Breach of Law or CYC Policy

Any ICT actions required to support any investigation into alleged or potential breaches of Law or CYC Policy that require review or extraction of information that may include personal or confidential material, shall only be initiated on receipt of formal written authorisation from the originating Directorate Head, through the Head of ICT or their duly appointed deputies. The request for access and request for information can be submitted by using the forms on Colin.

Employees being requested to execute investigative actions must similarly only do so on formal written authorisation by the Head of ICT, or deputy in their absence. Employees in receipt of a request of this nature without this written authorisation must refer the initiating manager to the contents of this policy, and are so authorised to refuse to enact the request.

Employees that are/have been involved in supporting actions concerning the investigation of electronic information are expressly forbidden to discuss or disclose any aspects of the investigation with any other staff member, or member of the public, unless otherwise directed, by the person who authorised the task, the Head of ICT, or a legal officer. Discussion must be strictly limited to objective details required to complete the authorised task.

Employees, unless directly authorised to do so by the appropriate person, are expressly forbidden to review any data extracted or recovered through the actions of investigation. This data is to be placed in a secured location, appropriately protected from access beyond that which has been identified by the investigating manager.

Removable Media

User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- All data stored on removable media devices must be encrypted where possible.
- Virus and malware checking software must be used when the removable media device is connected to a machine.
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.
- Removable media devices must not to be used for archiving or storing records as an alternative to other storage equipment.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

Disposal of Removable Media

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within the council or for personal use, must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to ICT for secure disposal.

Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the council’s ICT Service Desk should removable media be damaged.

Fully patched and up-to-date virus and malware checking software must be operational on both the machine from which the data is taken and the machine onto which the data is to be loaded. Any doubt about the virus or malware state of any removable media must be reported to the ICT Service Desk before being connected to any CYC device.

Whilst in transit or storage, the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the council, other organisations, or individuals, from the data being lost whilst in transit or storage.

Legislation

There are currently three Acts of Parliament that specifically govern the use of computers, software, and computer generated information. There are other acts of Parliament that can also be related to the use of computers and computer software. These should be read in conjunction with this policy:

The Data Protection Acts 1998 and 2018

Data Protection legislation is designed to protect any individual (the Data Subject) from suffering physical, mental or financial harm due to the processing of incomplete/inaccurate personal data or the misuse of that data. This is achieved by adherence to eight principles of good working practice in the handling of personal data. All data users must be registered for data use and Data Subjects have enforceable rights to prevent unlawful processing. Officers can be held personally responsible for breaches of the legislation. Further information can be obtained by contacting the Information Management Officer on Ext (55) 3450.

The Copyright, Designs and Patents Act 1988

This Act protects against unauthorised copying of any property (including intellectual property), which is covered by copyright, design or patent. The Act makes provision for copyright licensing and the payment of royalties or other sums for rental of licences works, including computer programs.

The Computer Misuse Act 1990

This Act prohibits unauthorised access to computers, unauthorised access with intent to commit serious crime and unauthorised modification of computer material.

Other acts which may apply include:

- The Copyright (Computer Programs) Regulations 1992
- General Data Protection Regulations (GDPR) 2018
- Data Protection Act (DPA) 2018
- Regulation of Investigatory Powers Act 2000
- Malicious Communications Act 1988
- Criminal Justice and Public Order Act 1994
- Trade Marks Act 1994
- Human Rights Act 1998
- Freedom of Information Act 2000
- Communications Act 2003
- Any new legislation that becomes UK law relevant to this policy

Approval

Position	Name	Signature	Date
Director HRSS	Helen Whiting		
Head of ICT	Roy Grant		
CYC Chief Operations Officer	Ian Floyd		

Related Documentation

Document Reference	Document Name
	CYC ICT Electronic Communications Policy
	CYC Data Protection Policy
	CYC ICT Mobile and Remote Working Policy