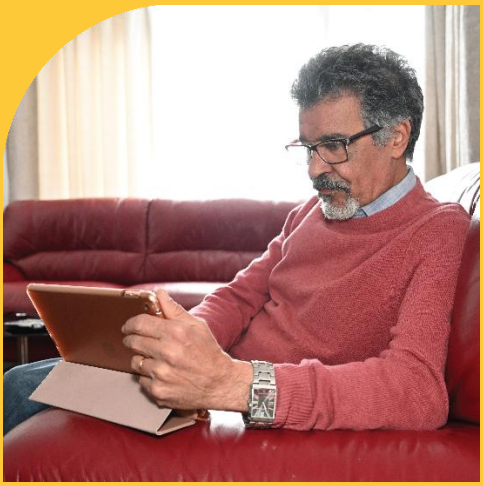
ICT & Information Security Policy



CHS GROUP
housing, care, and community services in Cambridgeshire

Review lead / author name and job title	Ken Lowe Assistant Director of ICT and Facilities Management		
Consultation process	CMT Employee Forum	**Distribution and training**	CHS Staff Synergy
Last reviewed	December 2025	**Next planned review**	December 2027
Approved by and date	CMT & Employee Forum December 2025		

Change record			
Version no	**Nature of change**	**Last approved**	**Approval**
11	Review December 25		
10	Amended to reflect audit recommendations		10 May 2025
9	Planned review		Updated 17 August 2023
8	Planned review		Updated 17 July 2020



1.0 Purpose

The CHS ICT & Information Security Policy identifies the rules and procedures for all individuals accessing and using our ICT systems and information. The purpose of this policy is to protect to a consistently high standard all information held by CHS. The policy covers security which can be applied through technology and encompasses the behaviors of those who access and use information as part of their duties.

Information security is about people's behaviour in relation to the information they are responsible for, facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- assurance that information is managed securely and in a consistent and corporate way;
- assurance that CHS is providing a secure and trusted environment for the management of information used in delivering its business;
- clarity over individual responsibilities around information security expected of colleagues whilst conducting work for CHS;
- assurance that information is accessible only to those authorised to have access;
- demonstration of best practice in information security

This policy observes the rights of customers, employees, and other workers (e.g. temporary, agency and casual/relief workers, volunteers, contractors and Board members) to have their information held securely, accessed only by those who are entitled to it, and be used for the effective response to queries and complaints.

1.1 Objectives

The CHS ICT & Information Security Policy is based on three core objectives:

- Confidentiality. Data and information assets shall be confined to those with authorised access
- Integrity. Data must be kept intact, complete, accurate and retained in accordance with agreed timescales as set out in the Data Retention Schedule for each service
- Availability. Information is at the disposal of authorised persons when needed

2.0 Scope

The CHS IT & Information Security Policy covers all data, programs, systems, facilities, other technical infrastructure, users of technology and third parties at CHS Group, including employees, agency and casual/relief workers, volunteers, students and Board members without exception.

ICT systems include the use of mobile devices such as laptops, tablets and smart phones that have been provided by CHS for work purposes.

3.0 Responsibilities

3.1 Chief Executive

Responsibility for information security resides ultimately with the Chief Executive.

3.2 Board and Directors

The Board and Directors are accountable for governance and compliance with data protection.

3.3 Assistant Director of ICT and Facilities Management

The Assistant Director of ICT and Facilities Management is accountable for the availability and integrity of data and backups.

3.4 Data Protection Officer (supported by Data Protection Advisor)

The Data Protection Officer:

- is responsible for monitoring internal compliance with data protection legislation;
- informs and advises on CHS's data protection obligations;
- provides advice regarding Data Protection Impact Assessments (DPIAs);
- acts as a contact point for data subjects and the Information Commissioner.

3.5 Managers

Managers are responsible for the security of their physical environment where information is processed and stored. They are also responsible for:

- ensuring that all colleagues (permanent, temporary and contractors) are aware of the data protection and information security policies, procedures and user obligations applicable to their area of work;
- ensuring that all colleagues (permanent, temporary and contractors) are aware of their personal responsibilities for information security;
- ensuring that all colleagues (permanent, temporary and contractors) are aware that ICT systems should not be used for any purpose other than to support the legitimate business operations of CHS;
- determining the level of access to be granted to specific individuals
- ensuring that colleagues have appropriate training for systems they are using
- ensuring colleagues know how to access advice on ICT and information security matters.
- ensuring colleagues take responsibility for the security of passwords and hand-held or portal electronic devices that are taken off site for work purposes.

3.6 Colleagues

Colleagues are responsible for information security and must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. All colleagues must undertake GDPR and data security training and understand:

- what information they are using, how it should be protectively handled, stored and transferred;
- what procedures, standards and protocols exist for sharing of information with others;
- how to report a suspected or actual breach of information security within the organisation;
- who they can go to for advice and guidance on data protection issues;
- their responsibility for raising any information security concerns to the Data Protection Officer and/or Assistant Director of ICT and Facilities Management;

- their responsibility for the security of passwords and hand-held or portable electronic devices at all times, and that such devices are only used by authorised users for business purposes. NB: hand-held or portal electronic devices must not be left in unattended parked cars or on public transport;
- that ICT systems should not be used for any purpose other than to support the legitimate business operations of CHS.

3.7 Contractors

Contracts with external contractors that allow access to the organisation's information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

4.0 Authorisation and Access Control

4.1 Starters, leavers and role-based access

CHS Group will give access only to the data and applications necessary for each individual role. The HR department notifies ICT of starters and leavers in advance so that access to the systems is permitted and revoked only for the time required (immediately before and after employment). The level of required access is determined by line managers, before being passed to the ICT department for action. This is detailed in the CHS Group starters and leavers procedures, which are referenced in the associated documents section below.

New employees and workers will be given data security and privacy awareness and GDPR training.

The CHS ICT department ensures that access to the computer systems is terminated on the day of leaving. If required ICT will, on instruction from HR, suspend employee or worker accounts with immediate effect. Data associated with leavers (excluding HR records), including files in their working file store and email will be removed after consultation with the leaving staff member's manager. This is detailed in the CHS Group starters and leavers procedures, which are referenced in the related documents section below.

Employees must not delete files and emails immediately prior to leaving employment at CHS, other than day-to-day housekeeping.

4.2 Password management

Colleagues and other workers have an individual password and username which allows access to the areas of the CHS computer system to which they are authorised. Passwords and usernames are confidential and should not be divulged to any other person; this includes access requested by ICT staff both inside and external to CHS. The password must be a 12-character complex password. At intervals, the computer system will automatically prompt for the password to be changed, locking out a user who does not change the password after repeated requests. Three incorrect attempts to enter an existing password will also automatically lock a user's account. Each user will be provided with a method of verifying their password using multi-factor authentication.

Where deemed appropriate an application will be given a completely separate username and password. High risk or sensitive data may be protected in this way.

Remote access to CHS systems is controlled by CHS remote access servers. Staff will only be able to see applications that they are authorised to run.

4.3 Access to network and servers

Standard employee accounts have no administrator access to networks and servers. They are unable to install applications or make any changes. This is to prevent unauthorised access, potentially leading to catastrophic changes, and protect against accidental damage. Only authorised and trained ICT users have access to the networks and servers.

4.4 Physical access and timeouts

All CHS physical sites are protected by door security systems which prevent non-CHS employees from having access to the computer systems. In buildings where non-CHS employees may be present all computers are kept in locked areas. The CHS system servers at Endurance House are kept in a secure room to which only CHS ICT staff have access.

CHS computer screens are locked after a period of inactivity to prevent unattended devices being accessed by unauthorised persons.

Individuals issued with hand-held or portable electronic devices must take proper care of the equipment and ensure its security at all times. This equipment remains the property of CHS Group and may be withdrawn if there is any evidence that it has been misused or not kept securely.

5.0 Data support and operations

5.1 Regulation of general systems mechanisms

All CHS computers used by staff are set automatically to install security updates. This is to prevent malicious or unauthorised access to the devices through vulnerabilities in the software. CHS servers are regularly patched with updates, once the updates have been tested with the CHS applications using the server. This is to ensure that untested updates will not prevent core applications from running.

Servers cannot be accessed by non-ICT members of staff. This ensures that malicious code cannot be installed on servers. It also protects against accidental damage to data or applications.

The level of security patches on servers is regularly reviewed. ICT staff stay aware of current threats and will mitigate against them and inform management and staff when appropriate. CHS Group regularly undertakes security reviews including penetration testing, security system reviews, phishing tests, and user awareness communication.

5.2 Breach policy

Any breach, or potential breach of CHS data or ICT systems is to be dealt with in line with the CHS Data Breach Guidance. This is referenced in the related documents in the section below.

5.3 Use of Non-CHS Group devices and working locations

CHS recommends that employees and workers only use CHS-supplied equipment and hardware. However it recognises this may not always be effective or manageable.

Therefore, CHS systems and applications can be accessed from most devices, but there are some important rules to follow:

- always use the remote access methods provided by CHS to access the information or application. If in any doubt, employees should contact the ICT service desk;
- do not copy any CHS data or information on to any non CHS system, for example: USB drive, optical media, the storage on your phone or laptop, personal email. Do not copy any CHS data on to any non-CHS Internet storage, such as Dropbox;
- ensure your personal devices have up-to-date security patches and anti-virus software installed. If in any doubt, please contact the ICT service desk;
- do not use public access devices to access CHS data or applications, such as those in libraries or Internet cafes;
- when working at non-CHS locations (including working from home) be aware that your screen may be viewable and your conversations audible. Take care not to disclose any confidential data or personal information.

5.4 Data backup

ICT has in place back-up applications and facilities, including but not limited to:

- Veeam backup software, which backs up individual files and also fully recoverable copies of each server;
- Windows Shadow Replication;
- Storage on Microsoft Azure at Microsoft hosted sites;
- Backup of files and shadow copy restore are tested at least weekly and, in some cases, almost daily;
- Disaster recovery suite at partner organization, including tamper-proof backup location, which has a full recovery test at least annually. This test involves key staff at CHS to test the recovered systems;
- CHS undertakes an annual Business Continuity Audit.

5.5 Virus and intrusion protection

Mimecast. All email at CHS comes in and goes out via Mimecast, which is the industry-leading email scanning and security service providing a high level of protection for incoming and outgoing emails and attachments.

Fortinet. Our high availability Fortinet servers control the connections both to the Internet, and to our many sites. The Fortinet firewalls control security access to CHS internal systems creating a

Virtual Private Network between sites, so that all data that crosses the Internet has a high level of encryption and cannot be read. Fortinet also prevents access to known malicious websites.

Sophos Endpoint. Sophos is present on all CHS devices. Endpoint is a centralised and constantly updated Virus Control System which informs ICT administrators of stopped viruses and threats, as well as preventing physical access to systems via USB drives and optical media.

Sophos Intercept X. Intercept X looks at the way that software behaves, shutting down any connection attempting unusual behaviour, and preventing damage from malware and other potentially malicious software.

Office 365. CHS uses Microsoft hosted Office 365. Email systems are hosted by Microsoft and are high availability, have Microsoft Disaster Recovery, and Microsoft Advanced Threat Protection.

Access Control. The level of access given to staff when they log in does not have high enough privileges to be able to install applications (including malware) on to the CHS servers, meaning that even if a staff computer becomes infected it would be difficult for it to infect others, especially servers.

Automatic updates. Staff computers are controlled by Microsoft update services and security vulnerabilities are automatically patched, making it more difficult for malicious software to infect CHS devices.

Remember: no ICT system will ever stop 100% of threats. Most security and data breaches still rely on email to find a way into companies. Users of CHS email should therefore:

- think carefully before opening any email attachment or following links in any email;
- never open an unexpected email attachment, or from an unknown sender;
- check carefully a sender's email address, for example for any misspellings;
- not be rushed into responding to any unexpected email. Hackers often try to instill a sense of urgency- they may try to impersonate someone in authority at CHS or elsewhere. For useful information, check out the National Cyber Security Centre guidance, https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams.

5.6 Printing confidential information

Do not print confidential or personal information unless absolutely necessary. CHS operates a clear-desk policy. Documents containing confidential or personal information must never be left unattended unless they are securely locked away. These documents should be securely destroyed or placed in the blue paper bins for an external contractor to destroy as soon as possible. If you are using confidential or personal information in hard copy documents, please consider an alternative method of accessing the information: speak to your line manager or the ICT Department.

5.7 Movement of data

All CHS personal data shared outside CHS needs to be covered by data sharing agreements or contractual clauses relating to data sharing, which will define the purpose for sharing the data, and the responsibilities and duties of each data controller, the method of data sharing, and any permissions required. Any new sharing of CHS Group personal data must be approved by CMT via the Data Protection Officer. See the CHS Data Protection policy for more information.

Sharing data includes emailing information or documents. Think carefully before sharing any information or documents: is there a data sharing agreement in place? Is there a more secure way of sharing the information, e.g. via a secure SharePoint link? Is the recipient of the email correct? If in doubt, speak to your line manager, the ICT Department, or Data Protection Officer.

5.8 Co-operation with Subject Access Requests

Any individual whose personal data is held by CHS Group has the right to make a Subject Access Request for a copy of their personal information held by CHS (see our Data Protection Policy). We may therefore need to access your CHS devices to retrieve any data that is held on it about the individual who has requested their personal information. This may include allowing a nominated member of staff to access ICT and hand-held devices and conduct a search to find any information about the individual that is held on the devices, including work mobile phones.

5.9 Shared access to Outlook & One-Drive Accounts

CHS Outlook accounts should only be used for work-related matters. Any personal work-related communications and information should be filed separately in a folder marked "personal" to ensure that this information is clearly identifiable if CHS requires access to an employee's Outlook and/or One-drive for business continuity purposes. This usually applies to former colleagues who have left CHS, and the manager has good reason to believe that business critical information is held on the former employee's Outlook or other electronic files. Such requests must be made via the ICT helpdesk, and approval must be obtained by the Director of Corporate Services or HR Manager in advance.

In exceptional circumstances, managers may request access to a colleague's Outlook account and/or OneDrive, to ascertain if business communication is stored there. Such requests are usually made when someone is absent from work due to long term sickness or maternity. These requests must be made via the ICT helpdesk, detailing the information required, and ICT will consult the Director of Corporate Services/HR Manager to consider whether access should be granted for a limited period, or whether alternative action could be taken to achieve the same outcome.

6.0 Communication & Training

6.1 Data awareness

This policy will be issued to individuals when they first join or first need access to ICT systems. Thereafter, updates will be provided on Synergy with a notification via Viva Engage. Managers are

expected to ensure agency or temporary workers are made aware of their responsibilities on starting.

CHS staff are required to read the ICT & Information Security Policy as part of their induction process and confirm to HR that they have done so. The Assistant Director of ICT and Facilities Management and the Data Protection Advisor meet with each new member of staff face-to-face as part of the induction process, to cover the contents of the policy, required training, and the risks associated with this policy.

All CHS members of staff undertake mandatory GDPR training to ensure they are aware of:

- the importance of confidentiality;
- the use, collection, and deletion of data at CHS Group;
- how to respond to a data breach or suspected breach;
- use of data in email and other communication applications.

GDPR induction training is mandatory for all new employees. Ongoing resources, support and briefing are provided by the Data Protection team. CHS completes an Annual GDPR Compliance Self-Assessment, including a survey of managers.

All CHS members of staff undertake mandatory Cyber Security training to ensure that they are aware of:

- their responsibility to protect CHS data;
- likely risks presented by email and phishing attempts;
- how to spot hacking attempts and non-genuine emails;
- how to deal with any suspected attempts to access CHS systems;
- the importance of correct password and physical security.

CHS undertakes an annual Cyber Security Audit.

CHS regularly undertakes both penetration testing and phishing tests to check data security and shares the results at all levels from Board to team meetings to raise awareness and educate staff. Staff who are repeatedly fooled by phishing tests are required to repeat their cyber security training.

CHS ICT staff undertake a higher level of training to understand the security levels in place to protect CHS data and systems and the backup systems in place.

Additional training modules are circulated to all staff as part of CHS Mimecast security system to address specific risks or significant new threats as required.

7.0 Legislation

The use of ICT is covered by several items of legislation. Some of these are detailed below.

Data Protection Act 2018 (DPA 2018), the EU General Data Protection Regulations (GDPR), and the Data (Use and Access) Act 2025.

These articles of legislation govern the use of personal data. This covers any information that can be used to identify living individuals, ranging from names and addresses (e.g. customer lists) to more sensitive personal information (e.g. health records). Employees must ensure that when personal data is being processed this is in accordance with the principles of data protection legislation (see our Data Protection Policy for further guidance). Failure to comply with data protection legislation can attract penalties ranging from fines to criminal sanctions.

Computer Misuse Act 1990

The Computer Misuse Act 1990 makes computer hacking a serious criminal offence. Computer hacking includes unauthorised access to computer systems, even when you have authorised access to another part of the system, unauthorised modification of computer material, and unauthorised access with intent to commit further offences. If you suspect that any system is being accessed without authorisation you should notify the ICT Team immediately.

Regulation of Investigatory Powers Act 2000

Under the Regulation of Investigatory Powers Act 2000 ("RIPA"), interception of communications without lawful authority is an offence. 'Communications' will include email and web-access systems, if they are connected to a public telecommunications network. If you suspect that any system is being accessed without authorisation you should notify the ICT Team immediately.

Lawful Business Practice Regulations

Under the Lawful Business Practice Regulations ("LBPR"), employers can monitor communications on a private network, either with the consent of all parties to communications, or if the monitoring is for one of the reasons set out in the LBPR.

These include monitoring or keeping a record of communications

i. in order to:

- establish the existence of facts, or
- ascertain compliance with regulatory or self-regulatory practices or procedures applicable to the organisation, or
- ascertain or demonstrate the standards which are achieved or ought to be achieved by those using the system in the course of their duties;

ii. in the interests of national security;

iii. for the purpose of prevention and/or detection of crime;

iv. detecting unauthorised use of the (phone/internet/email etc.) systems;

v. monitoring the performance standards of staff.

CHS must make "all reasonable efforts" to inform employees if monitoring is taking place. If the reason for monitoring falls under the items listed above, then CHS reserves the right to monitor communication without prior notification subject to the completion of a data protection impact assessment to ensure that the monitoring is necessary and proportionate. The communication of this policy in itself constitutes reasonable effort towards informing employees of the CHS's policy in the circumstances described, of monitoring without prior notification.

Human Rights Act 1998 (HRA)

The HRA incorporates the European Convention on Human Rights into UK law. Article 8 of the Convention provides a general right to privacy.

Copyright Law

- Copyright, Designs and Patents Act 1988
- The Copyright and Related Rights Regulations 2003 SI No: 2498
- Directive 2001/29/EC

Employees must observe all signs of Copyright reservation " © " or the words "copyright reserved". If there is any doubt as to the law relating to Copyright, then information can be found here: http://www.cla.co.uk/

9.0 Compliance with this Policy

As part of its ongoing obligations under data protection legislation, CHS will monitor data protection compliance in general, and compliance with this policy specifically, via data protection impact assessments, to ensure that such monitoring is necessary and proportionate. It is in our CHS' legitimate interests to ensure that any policy is being complied with, and to obtain assurance that the organisation is complying with its legal obligations under data protection legislation.

Compliance monitoring will be limited to business-related devices and applications and can include SharePoint, One-Drive files, Outlook accounts, internet use, social media, communication apps, and work-related accounts including Facebook, MS Teams etc.

The information obtained through monitoring may be shared internally, including with members of the HR team, line managers and any other managers who require access to the data in the performance of their role. Information will only normally be shared in this way if the organisation has reasonable grounds to believe that this policy has not been followed. Information gathered through monitoring will only be retained long enough for issues to come to light and for any investigation to be conducted.

If a breach of this policy is suspected, the organisation will investigate the matter under its Disciplinary Policy and Procedure. If any breaches are confirmed, this could lead to disciplinary action up to and including summary dismissal, as well as potential prosecution if the law has been broken. If you have any doubts as to whether your use of ICT may be considered inappropriate it is prudent to be overcautious. If in doubt, please contact the ICT department for advice.

CHS Group does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, CHS Group reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

10.0 Related Documentation

- Personal Data Breach - Incident Response Plan
- Personal Data Breach Internal Process
- Guidance Sheet (3) – Personal Data Breach Reporting
- Leavers Procedure
- New Starter – Full Login Account
- New Starter – Basic email account
- CHS Data Protection Policy