INFORMATION SECURITY POLICY

for adoption by all CDAT schools

This policy is informed by the Christian values which are the basis for all of CDAT's work and any actions taken under this policy will reflect this.

'Blessed are those who act justly, who always do what is right'

Psalm 106:3

Approved by	Date	Review Schedule	Date of next review
Audit and Risk Committee	December 2025	Every two years	December 2027

Contents

1. Introduction and Scope

The Information Security policy outlines the Chester Diocesan Academies Trust's (CDAT) organisational security processes and standards. The policy is based on the sixth principle of the UK GDPR which states organisations must protect personal data against unauthorised loss by implementing appropriate technical and organisational measures.

To ensure we meet our legal obligations, personal data should be protected by the security model known as the 'CIA' triad. These are three key elements of information security:

- **Confidentiality** – only authorised people should have access to information.
- **Integrity** – information should be accurate and trustworthy.
- **Availability** – authorised people should have access to the information and systems they need to carry out their job.

This policy and its appendices apply to our entire workforce. This includes employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the school. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

The Information Security policy applies to all personal data, regardless of whether it is in paper or electronic format. It should be read alongside the other policies within our information governance policy framework, including data protection, records management, and acceptable use of systems.

2. Roles and Responsibilities

Senior Information Risk Owner (SIRO)
The SIRO is responsible for overseeing the implementation of this policy and ensuring that effective information security practices are in place across the organisation. The SIRO is also responsible for risk management and will ensure that staff are appropriately trained in information security, supported by the SPOC and IAOs. In our organisation, this role lies with the CEO (Trust) and Headteacher (school).

Single Point of Contact (SPOC)
The SPOC will support the SIRO in day-to-day operational management. This includes providing guidance on information security practices and promoting compliance with this policy to protect personal data in line with the CIA triad. In our organisation, this role lies with the Director of Operations (Trust) and School Business Manager or nearest equivalent (school).

Information Asset Owner (IAO)
IAOs will be responsible for the security and maintenance of their assigned information assets and for ensuring that other staff members use the information safely and responsibly.

All staff
All staff, including governors or trustees, contractors, agents and representatives, volunteers, and temporary staff working for or on our behalf, will be responsible for information security in accordance with this policy.

3. Access Control

We will maintain control over access to the personal data that we process. These controls will differ depending on the format of the data and the status of the individual accessing the data. We will maintain an audit log detailing which individuals have access to which systems (both electronic and manual). This log will be maintained by the CDAT Director of Operations.

Manual Filing Systems
Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files that contain personal data will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use.

Keys to storage units will be stored securely. The school Headteacher or, for the CDAT central team the Director of Operations, will be responsible for giving individuals access to the safe place. Access will only be given to individuals who require it to carry out legitimate business functions. Where a PIN is used, the password will be changed every three months or whenever a member of staff leaves the organisation, whichever is sooner.

Electronic Systems
Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to carry out legitimate functions.

Individuals will be required to regularly change their password and usernames will be suspended either when an individual is on long-term absence or when an individual leaves our employment.

Individuals should ensure they use different passwords for different systems to ensure if one system is compromised, that does not lead to other systems being accessed. Users should never leave a live session unattended while logged in.

Password managers
Where possible, password management software will be used to store passwords securely. This practice helps to prevent insecure workarounds such as adopting insecure passwords that are easier to remember, re-using passwords, or making minor variations to previous passwords.

Software and Systems Audit Logs
We will ensure that all major software and systems have inbuilt audit logs, wherever possible, so that we can ensure it can monitor what users have accessed and what changes may have been made. Although this is not a preventative measure it does ensure that the integrity of the data can be assured and also deters individuals from accessing records without authorisation.

Data Shielding
We do not allow our workforce to access the personal data of family members or close friends. Users should declare upon employment whether they are aware of any family members or friends who are registered with us.

When such an interest is raised, we will review access controls for relevant paper and electronic files to ensure that only appropriate access is granted.

Users who knowingly do not declare family and friends registered with us may face disciplinary proceedings and may be charged with an offence under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

External Access
On occasions we will need to allow individuals who are not part of our workforce to have access to systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in, or because of a partnership arrangement with another educational establishment. The CDAT Director of Operations or if unavailable an appropriately senior member of staff, is required to authorise all instances of third parties having access to systems.

We will maintain a record on our IAR detailing what access has been given to whom and the authorising individual.

4. Physical Security

We will maintain high standards of physical security to prevent unauthorised access to personal data. We will maintain the following controls:

Clear Desk Policy
Individuals will not leave personal data on desks, or any other working areas, unattended and will use the lockable storage units provided to secure personal data when not in use.

Portable storage devices
We will not permit the use of portable storage devices such as USB memory sticks and external hard drives to store or transfer pupil, staff, or business-related information.

Alarm System
We will maintain a security alarm system in our premises so that, when the premises are not occupied, an adequate level of security is still in operation.

Building Access
External doors to the premises will be locked when the premises are not occupied. Only authorised individuals will be key holders for the building premises. School Headteachers will be responsible for authorising key distribution and will maintain a log of key holders.

Internal Access
Internal areas that are off limits to pupils and parents will be kept locked and only accessed through PIN or keys. PINs will be changed every six months or whenever a member of staff leaves the organisation. Keys will be kept in a secure location and a log of any keys issued to staff maintained. Access equipment will be collected and deactivated when a staff member leaves or is away from work for over three months.

Visitor Control
Visitors will be required to sign in and state their name, organisation, car registration (if applicable) and nature of business. They may also be asked to provide information to help provide support in the event of an emergency. This may be either in paper or electronic format. Visitors will be escorted throughout the school and will not be allowed to access restricted areas without appropriate supervision.

Secure Disposal
We will ensure that all personal data is securely disposed of in line with our Records Management Policy and retention schedule. Hard copy information will be securely destroyed by shredder or a confidential waste provider. Electronically held information will be deleted automatically with retention periods built into the system wherever possible. Otherwise, manual review and deletion will take place at least annually.

Redundant computer equipment will be disposed of in accordance with the Waste Electrical and Electronic Equipment (WEEE) Regulations and through secure and auditable means. Where personal devices are being disposed of, the user must ensure that they have complied with this policy. School-related data should be removed and stored appropriately within the appropriate systems before disposal.

5. Environmental Security

As well as maintaining high standards of physical security to protect against unauthorised access to personal data, we must also protect data against environmental and natural hazards such as power loss, fire, and floods.

It is accepted that these hazards may be beyond our control, but we will implement the following mitigating controls:

Back Ups
We will regularly back up our electronic data and systems and carry out tests to ensure that they restore correctly. These backups will be held in a different location to the main server or held off-site by an external provider. This arrangement will be governed by a data processing agreement. Should our electronic systems be compromised by an environmental or natural hazard then we will be able to reinstate the data from the backup with minimal destruction.

Fire-proof Cabinets
We will aim to only purchase lockable data storage cabinets that can withstand exposure to fires for a short period of time. This will protect paper records held in the cabinets from any minor fires that break out on the building premises.

Fire Doors
Areas of the premises which contain paper records or core electronic equipment such as server boxes, will be fitted with fire doors so that data contained within those areas will be protected, for a period of time, against any fires that break out on the premises. Fire doors must not be propped open unless automatic door releases are installed.

Fire Alarm System
We will maintain a fire alarm system at our premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

6. Systems and Cyber Security

We will protect against hazards to our IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect our ability to operate and could potentially endanger the safety of our pupils and workforce.

We will implement security controls to mitigate risks to our digital devices and online locations, such as the cloud. All use of personal devices to access our network or systems must be authorised. We will ensure that, at minimum, the device has up-to-date security systems and encrypted storage, and that all software patches are installed as soon as they are released. The user will ensure these criteria are met for their personal devices, seeking specialist advice if required.

Software Download Restrictions
Users must request authorisation from our IT provider before downloading software onto our IT systems. Our IT provider will vet software to confirm its security certificate and ensure the

software is not malicious. Our IT provider will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

Firewalls and Anti-Virus Software

We will ensure that the firewalls and anti-virus software is installed on electronic devices and routers. We will update the firewalls and anti-virus software when updates are made available and when advised to do so by our IT provider. We will review our firewalls and anti-virus software on an annual basis and decide if they are still fit for purpose. We will ensure that updates and patches are applied when they are available to ensure any security weaknesses are addressed as soon as they are known.

Shared Drives

We maintain a shared drive on our servers. Whilst users are encouraged not to store personal data on the shared drive it is recognised that on occasion there will be a genuine business requirement to do so.

The shared drive will have restricted areas that only authorised users can access. School Headteachers will be responsible for giving shared drive access rights to users. Information held within the shared drives will still be subject to our retention schedule.

Cloud storage

We will liaise with our IT provider before utilising cloud storage. We will only use providers who can meet our security needs and demonstrate assurance with the National Cyber Security Centre (NCSC) Cloud Security Principles.

Malicious software and fraud

To avoid our systems being compromised fraudulently by email, users will consider the source of emails before clicking on any links or opening attachments. Users will check with our IT provider if they are unsure about the validity of an email, and must immediately inform our IT provider if they have clicked on a suspicious link.

We will ensure staff receive adequate training to identify phishing, spear phishing, whaling emails, and other malicious threats. Staff identified as at higher risk of being targets for this type of fraud will receive regular training to combat the risk of social engineering and other types of fraud.

7. Communications Security

The transmission of personal data is a key business need and, when operated securely is a benefit to us and pupils alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. We have implemented the following transmission security controls to mitigate these risks:

Sending personal data by post

When sending personal data, excluding special category data, by post, we will use Royal Mail's standard postal service. Individuals will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

Sending special category data by post

When sending special category data by post we will use Royal Mail's 1st Class Recorded postal service. Individuals will double check addresses before sending and will ensure that

the sending envelope does not contain any data which is not intended for the data subject. If the envelope contains information that is thought to be particularly sensitive, individuals are advised to have the envelope double checked by a colleague.

Sending personal data by email

We will only email personal and special category data using secure email transmission methods, such as end-to-end encryption and encryption protocols. Individuals will double-check the recipient's email address to ensure that the email is being sent to the intended individual(s). The use of autocomplete for recipient email addresses will be discouraged.

Secure data transfer services must be used when sending emails to a large number of recipients, such as a mailshot, or when it would not be appropriate for recipients to know each other's email addresses. The Blind Carbon Copy (BCC) function will be used where no alternative option exists.

Staff must not use personal email accounts to access or transmit pupil, staff, or business data. Only business-issued email accounts should be used.

Exceptional Circumstances

In exceptional circumstances we may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive that the usual transmission methods would not be considered secure, or because the volume of the data that needs to be transmitted is too big for usual transmission methods.

8. Remote Working

Personal devices

Any electronic device not provided by us and used to access or process personal or business data will be classed as a personal device. The use of personal devices must be authorised and meet the requirements set out in this policy.

Personal devices must be limited to the individual user and not a shared resource, e.g., a family device. Users must only access the information they are entitled to in order to fulfil their role. To prevent unauthorised access, devices must include appropriate security and access controls, such as password and/or PIN protection.

Pupil, staff, or business data must not be downloaded and saved onto personal devices. Such data must remain within the defined systems to ensure it remains secure, available to all authorised personnel, and managed within our systems for its full lifecycle, including secure destruction in line with our retention schedule. Printing of any personal data on home printers is strictly forbidden.

Security and confidentiality

Users must ensure that electronic equipment or paper documents containing personal data are kept secure and never left unsupervised. Any paper documents requiring disposal must be securely destroyed using a cross-cut shredder or returned to our premises for confidential waste disposal.

Individuals must not work in areas where others may view, hear, or copy personal data. Users must always be mindful of their surroundings and ensure measures are in place to prevent loss or unauthorised access to information.

When remote working, only trusted Wi-Fi connections will be used, with appropriate anti-virus and firewalls installed to safeguard against malicious intrusion. Unsecured network connections, including public Wi-Fi or hot spots, must not be used, and devices must be configured to prevent automatic connection to unknown networks.

Users will be mindful of any applications (apps) installed on personal devices that could be used to access pupil, staff, or business data. The user must seek reassurance that any risks associated with apps monitoring the device's use are being effectively managed.

Authorised access
Access to business systems and cloud storage on personal devices is only permitted where authorised. Access should not be attempted when a user leaves employment or the working relationship ceases. Attempts to do so will be treated as a data breach and investigated as such. Under Section 170 of the Data Protection Act 2018, knowingly accessing data you are not entitled to is a criminal offence.

Any exemptions to the above access can only be authorised by the SIRO and will only be given where there is a clear business need and following a full risk assessment.

9. Data Breaches

A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of or access to personal data. The severity of breaches can vary from minor to very severe, however all breaches will be treated seriously. Appropriate measures will be in place to ensure continuous improvement of information security practice, reducing the risk of minor breaches or near-miss incidents from turning into high-risk breaches.

Where a data breach is likely to result in a high risk to the rights and freedoms of the data subject(s), Article 33 of the UK GDPR requires data controllers to report these to the Information Commissioner's Office (ICO), and sometimes the affected data subject(s), within 72 hours of discovery.

All actual and suspected breaches of security or confidentiality, including near misses, will be recorded and investigated in accordance with the Data Breach Procedure set out in Appendix One.

10. Business Continuity

We will have a risk-based business continuity and/or disaster recovery plan to enable us to continue critical business in the event of an information security incident. This plan will include the process to follow, emergency contacts, and business-critical priorities. We will ensure staff are aware of these arrangements and can access the plan easily.

We will ensure that we have a Critical Incident Plan in place to ensure a process is documented for what to do, who to call and what the priorities are in the event of a disaster.

We have a process in place for testing, assessing and evaluating the effectiveness of the measures we have in place. This may include vulnerability scanning and penetration testing.

We will obtain appropriate insurance which includes cyber security cover, to ensure we can cover the costs of a serious cyber event.

Appendix One – Data Breach Procedure

Introduction

To enable us to report serious incidents to the ICO within 72 hours it is vital that we have a robust system in place to manage, contain, and report such incidents.

This procedure has been written to govern our management of data breaches.

Roles and Responsibilities

Single Point of Contact (SPOC) – At school level this is the School Business Manager; at Trust level this is the CDAT Director of Operations.
Senior Information Risk Owner (SIRO) – CDAT Chief Executive Officer
Information Asset Owner (IAO) – as detailed in the Information Asset Register.
Data Protection Officer (DPO) – Veritau.

Immediate Actions (within 24 hours)

If any member of the workforce is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to their line manager and the Single Point of Contact (SPOC) within 24 hours. If the SPOC is not at work at the time of the notification, their nominated deputy would need to start the investigation process.

If the breach has the potential to have serious or wide-reaching detriment to data subjects, then the Data Protection Officer must be contacted within this 24-hour period.

If appropriate, the SPOC or the individual who discovered the breach will make every effort to retrieve the information and ensure recipients do not retain a copy of the disclosed data. This may involve asking email recipients to delete from their inboxes and recycle bins or collecting paper records in person. Measures to retrieve disclosed information will be dependent on the level of risk. Written confirmation should be sought from the recipient to confirm that the information is no longer held.

Assigning Investigation (within 48 hours)

The SPOC or nominated officer will begin to complete a data breach form and assess the data protection risks using a risk matrix to determine the severity rating. If the breach is assessed to be moderate or above, the SPOC will inform the SIRO.

The DPO should be sent a copy of the data breach form and the risk matrix to ensure the breach has been assessed appropriately and to recommend further measures to mitigate or reduce the risk.

Reporting to the ICO/Data Subjects (within 72 hours)

Where the breach is assessed as high or very high risk, it should be reported to the ICO within 72 hours.

The SIRO, in conjunction with the relevant manager, SPOC, IAO and DPO will decide whether the incident needs to be reported to the ICO, and whether any data subjects need to be informed. The relevant member of staff/IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

The decision to notify data subjects will depend on the level of risk and any detriment or harm that could result from the disclosure. We will also consider what is in the best interests of the data subjects when making the decision. The SPOC will be responsible for liaising with data subjects where it has been deemed appropriate to inform them.

Investigating and Concluding Incidents

The SPOC will ensure that all investigations have been completed, all potential information risks have been identified, and remedial actions have been implemented. Where necessary, the SIRO should review the completed data breach form and action plan to ensure the breach was handled appropriately and actions completed.

When the DPO has investigated a data breach, the SIRO must sign off the investigation report and ensure recommendations are implemented.

The SIRO will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.

All actual data breaches and near-misses must be recorded on a data breach log, along with the risk rating, actions taken, and investigation outcome. Any lessons learned should be shared and used to improve working practices.

DPO contact details:

Schools Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA

schoolsDPO@veritau.co.uk // 01904 554025