HumberEducationTrust
Where everybody counts, every moment matters.

# Information Security Policy

| | |
|---|---|
| **Approved by:** | Finance & General Purposes Committee |
| **Created:** | Summer 2021 |
| **Amended:** | Summer 2023, Summer 2025 |
| **New review date:** | Summer 2027 |

**Contents**

**Introduction and Scope** ..... **3**
**Roles and Responsibilities** ..... **3**
**Access Control** ..... **4**
**Physical Security** ..... **5**
**Environmental Security** ..... **6**
**Systems and Cyber Security** ..... **6**
**Communications Security** ..... **8**
**Remote Working** ..... **8**
**Data Breaches** ..... **9**
**Business Continuity** ..... **10**
**Appendix One – Data Breach Procedure** ..... **11**

## Introduction and Scope

The Information Security Policy outlines Humber Education Trust's organisational security processes and standards. It is based on the sixth principle of the UK GDPR, which states that 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, including its appendices, applies to our entire workforce. This includes employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for or on our behalf. Individuals found to knowingly or recklessly infringe this policy may face disciplinary action.

The Information Security Policy applies to all personal data, whether paper or electronic. It should be read alongside the other policies within our information governance policy framework.

## Roles and Responsibilities

Overall responsibility for ensuring that we meet the statutory requirements of any legislation lies with the Board of Governors or Trustees. The following roles will have day-to-day responsibility for information security management and providing the necessary assurance to the Board.

### Senior Information Risk Owner (SIRO)

The SIRO (CFOO) 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 (School Business Managers) and IAOs (Headteachers).

### 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 School Business Managers.

### 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.

**Access Control**

We maintain control over access to the personal data that we process. These controls will differ depending on the format of the data and the role of the individual accessing the information. We maintain a record detailing which individuals have routine access to which information systems in our IAR.

**Manual filing systems**
Access to manual filing systems (i.e., non-electronic systems) will be controlled by a key or PIN management system. When not in use, all files containing personal data will be locked away in lockable storage units, such as a filing cabinet or a document safe.

Keys to storage units will be held securely and managed by the SPOC. Access will only be given to staff members who require it to carry out legitimate business functions. Where in use, PINs will be changed annually or whenever a staff member with access 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 perform legitimate functions. Wherever possible, multi-factor authentication will be implemented across all critical electronic systems.

Individuals will be required to comply with our password standards. Accounts will be suspended when a staff member is on long-term absence and deleted when the staff member leaves our employment.

Individuals will use different passwords for different systems to ensure that if one system is compromised, it does not lead to access to other systems. 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 ensure that all critical software and systems have built-in audit logs wherever possible so that they can monitor what users have accessed and what changes have been made. Although this is not a preventative measure, it supports the integrity of the data and acts as a deterrent for individuals seeking to access records without authorisation.

**Data shielding**
We will not allow our workforce to access the personal data of family members or close friends wherever possible. Users should declare whether they know any family members or friends registered with us upon employment. When such an interest is raised, We review access controls for relevant paper and electronic files to ensure that only appropriate access is granted.

Users who knowingly fail to declare family and friends registered with us may face disciplinary proceedings and be charged with an offence under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

**External access**
Occasionally, we may need to allow individuals outside our workforce access to our systems. This could be for audit purposes, to fulfil an inspection, when using agency staff, or because of a partnership arrangement with another educational establishment. The SIRO or SPOC, or if unavailable, an appropriately senior staff member, will authorise instances of third parties having access to systems.

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

**Physical Security**

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

**Clear desk policy**
Staff members will not leave personal data unattended on desks or workspaces. Lockable storage units will be used 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.

**Building access**
External doors to the premises will be locked when the building is not occupied. Only authorised individuals will be key holders for the building. The SPOC will be responsible for authorising key distribution and will maintain a log of key holders.

**Internal access**
Internal areas off limits to pupils and visitors will be appropriately secured and only accessible by access card, fob, PIN, or key. Access equipment will be collected and deactivated when a staff member leaves or is away from work for over three months. PINs, where in use, will be changed every six months or whenever a staff member leaves the organisation. Keys will be kept in a secure location, and the SPOC will maintain a log of any keys issued to staff.

**Visitor control**
Visitors must sign in and state their name, organisation, car registration (if applicable), who they are visiting, and the nature of business. They may also be asked to provide information to help us provide support in an emergency event. Visitor access will be documented via paper or an

electronic visitor management system. Visitors will be escorted throughout the site and will not access restricted areas without appropriate supervision.

**Secure disposal**
We ensure that all personal data is securely disposed of per our Records Management Policy and retention schedule. Hard copy information will be securely destroyed by a cross-shredder or a confidential waste provider. Electronically held information will be deleted automatically, with retention periods built into systems, wherever possible. Otherwise, manual review and deletion will take place annually at a minimum.

Redundant computer equipment will be securely wiped and disposed of following the Waste Electrical and Electronic Equipment (WEEE) Regulations. 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.

**Environmental Security**

We must maintain high standards of physical security to protect personal data against unauthorised access and environmental and natural hazards such as power loss, fire, and floods. It is accepted that these hazards may be beyond our control, but we implement the following mitigating controls:

**Back-ups**
We regularly back up our electronic data and systems and conduct tests to ensure they can be restored correctly. These backups are cloud based and held with Redstor (managed by North Yorkshire Digital). A data processing agreement will govern this arrangement. Should an environmental or natural hazard compromise our electronic systems, we be able to reinstate the data from the backup with minimal disruption or data loss.

**Fire-proof cabinets**
We provide lockable data storage cabinets that can withstand short fire exposure. This will protect any business-critical paper records held in cabinets from minor fires on the building premises.

**Security alarm systems**
We ensure that appropriate security systems are in place to alert individuals in the event of a fire or intruder. Extra measures, such as fire doors, will be implemented in areas where paper records or critical electronic equipment are held to provide extra security in an emergency event.

Emergency contact details will be in place and shared with the necessary services to ensure we can be contacted out of hours in the event of alarm system triggers.

**Systems and Cyber Security**

We 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 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 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**
We restrict users from downloading third-party apps and software onto our devices. Users must request authorisation from our IT provider, who will vet the software to confirm that it does not pose a security risk. A list of trusted software will be retained.

**Firewalls and anti-virus software**
We ensure that firewall infrastructure is deployed and anti-virus software is installed on electronic devices and routers. We also update security releases as soon as possible to address any weaknesses. We review our firewall setup and anti-virus software annually to assess if they remain fit for purpose.

**Shared storage**
We maintain minimal shared storage on servers with restricted areas only authorised users can access. The SPOC will be responsible for providing users with access. Information held within shared storage will remain subject to our retention schedule. The core means of storage across the trust is cloud based, backed up to Redstor and with Starlink support in case of broadband failure.

**Cloud storage**
We liaise with our IT provider before utilising cloud storage. We 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 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.

## Communications Security

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

### Sending personal data by post

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

### Sending special category data by post

We restrict sending special category data by post wherever possible. Where necessary, we use a signed-for postal service to track delivery. Individuals will double-check addresses before sending and ensure that the sending envelope does not contain data not intended for the data subject. If the information is particularly sensitive, a colleague will double-check the contents.

### Sending personal data by email

We 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 the 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 large for usual transmission methods.

## 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.

**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.

**Business Continuity**

We 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 ensure staff are aware of these arrangements and can access the plan easily.

We have a process for testing, assessing, and evaluating the effectiveness of our information security measures.

We obtain appropriate insurance (Risk Protection Arrangement - RPA) , including cybersecurity coverage, to cover the costs of a serious cyber event. We also ensure that all staff complete cybersecurity training in accordance with the insurance policy requirements. We ensure that we meet the standards expected for the National Cyber Security Centre (NCSC) and the RPA.

**Appendix One – Data Breach Procedure**

**Immediate actions (within 24 hours)**

If any member of the workforce becomes aware of an actual data breach or an information security event (a 'near-miss'), they must report it to the Single Point of Contact (SPOC) within 24 hours. If the SPOC is unavailable, the SIRO or nominated deputy must start the investigation process.

If the breach has the potential to be serious or cause wide-reaching detriment to data subjects, then the Data Protection Officer must also 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 an 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 and/or 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 liaison with the SPOC and DPO, will agree on whether the incident will be reported to the ICO and whether any data subjects should be informed. The DPO will prepare the ICO report and, once approved by the SIRO, submit it and liaise with the ICO until the matter is concluded.

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 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.

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.