The Whitby Secondary Partnership

Information Security Policy

Document History	
Created or reviewed:	May 2023
Reviewing officer:	Executive Head Teacher/Heads of School/SLT
Review frequency:	Every two years or when new guidance/legislation is published
Review date:	May 2024

Signed by the Chairs of Governors:

S Crossland

C Zanelli

Contents

Introduction and Scope

The Information Security policy outlines the Whitby Secondary Partnership's 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.

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 ICT Network Manager.

Manual Filing Systems

Access to manual filing systems (ie, 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 Site Manager/Caretakers 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 PIN 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. Two factor authentication will be implemented across all external critical electronic systems.

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.

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 [SA2]

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.

We will then keep paper files in a separate location (with access restricted to minimal employees) and where possible any electronic files will be locked down so that the declaring user cannot access that data.

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 ICT Network Manager 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 an access log, detailing who has been given access to what systems and who authorised the access.

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.

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. The Site Manager 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.

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.

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.

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 the following security controls in order to mitigate risks to electronic systems:

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 onto 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. The Network Manager 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.

Phishing Emails

In order to avoid our computer systems from being compromised through phishing emails, users are encouraged not to click on links that have been sent to them in emails when the source of that email is unverified. Employees will also take care when clicking on links from trusted sources in case those email accounts have been compromised. 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 have received adequate training to be able to recognise such emails.

Biometric Data

The school takes finger print data and stores this as a barcode in order to link students to their lunch account in order to avoid students having cash in the school. In processing this data, the school follows the government's 'Protection of biometric data of children in schools and colleges, July 2022' policy to ensure that this information is used lawfully and for the sole purpose of cashless catering.

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 send personal data and special category data by email if using a secure email transmission portal.

Individuals will always double check the recipient's email address to ensure that the email is being sent to the intended individual(s). Use of autocomplete should be strongly discouraged.

When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses then we will utilise the Blind Copy (BCC) function.

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.

Data Breaches

Article 33 of the UK GDPR requires data controllers to report breaches of personal data to the Information Commissioner's Officer; and sometimes the affected data subject(s), within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of the data subject(s).

All actual and suspected breaches of security or confidentiality are to be reported in accordance with the Data Breach Procedure set out in Appendix One of this document.

Business Continuity

We will ensure that we have a business continuity plan in place to ensure we can continue normal business in the event of a security incident.

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 includes 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.