High Tunstall College of Science

Inspire | Support | Achieve

Information Security Policy

Revised	-	December 2025
Stakeholder Consulted	-	Staffing, Staff Welfare and Finance Committee
Review Date	-	December 2027
Responsibility for Review	-	Senior Teacher – Achievement and Standards/Compliance Officer

V1.0

Contents

Appendices

1. Introduction and Scope

The Information Security Policy outlines the college's organisational security processes and standards. The policy is based upon the sixth principle of the GDPR which states organisations must protect the personal data, which it processes, 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, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the college. 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.

This policy should be read in conjunction with the following college policies:

- Student Technology Acceptable Use Policy
- Staff Technology Acceptable Use Policy
- Information Security Incident Reporting Policy
- Data Protection Policy
- Surveillance and CCTV Policy
- Remote Access Policy
- Remote Learning and Online Communication Acceptable Use Policy

2. [Updated] Access Control

The college will maintain control over access to the personal data that it processes. These controls will differ depending on the format of the data and the status of the individual accessing the data. This will be maintained by the ICT Technicians and Headteacher's PA.

Staff will be informed that caution should be exercised while accessing personal data if an unauthorised person is in the same room. If a member of staff needs to leave their device unattended, the device should be locked. Where staff are using a personal device, they will be advised that a similar function should be implemented.

The college has implemented multi factor authentication (MFA) when accessing systems using office 365. This will be required when accessing systems off college site.

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.

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. From October 2022, the college will implement multi factor authentication (MFA) when accessing systems using office 365. This will be required when accessing systems off college site. A two-tier authentication system will be implemented across all other electronic systems. The two tiers will be username and unique password.

Individuals will be required to change their password every 90 days and usernames will be suspended when an individual leaves employment of the college.

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

The college will ensure, where possible, that all software and systems have inbuilt audit logs so that the college 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.

[Updated] External Access

On occasions the college will need to allow individuals, who are not employees of the college, to have access to data 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 Headteacher (Sponsor) is required to authorise all instances of third parties having access to systems. If the above individual is not available to authorise access, then access can also be authorised by the Deputy Headteachers (Sponsors).

[New] Trainee teachers will be provided with access to college systems via the Senior Teacher (Teaching & Learning) and the Headteachers (PA).

Once access needed has expired (after reason for access has expired) this should be removed immediately by the ICT team after consultation with the Sponsor.

3. Physical Security

The college will maintain high standards of physical security to prevent unauthorised access to personal data. The following controls will be maintained by the college:

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

The college will maintain a security alarm system at its 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 employees will be key holders for the building premises. The Site Manager will be responsible for authorising key and fob distribution and will maintain a log of key/fob holders.

Internal Access

Internal areas, which are off limits to students and parents, will be kept locked and only accessed through key fobs and keys. Keys will be kept in a secure location and a log of any keys issued to staff maintained.

Visitor Control

Visitors to the college will be required to sign in and state their name, organisation, car registration (if applicable) and nature of business. Visitors will be escorted throughout the college and will not be allowed to access restricted areas without employee 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 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.

4. Environmental Security

As well as maintaining high standards of physical security, to protect against unauthorised access to personal data, the college 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 the control of college but the college will implement the following mitigating controls:

Back Ups

The college will back up their electronic data and systems every weeknight**.** These backups will be kept off site by an external provider. This arrangement will be governed by a data processing agreement. Should the college's electronic systems be compromised by an environmental or natural hazard then the college will be able to reinstate the data from the backup with minimal destruction.

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

The college will maintain a fire alarm system at its premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

5. Systems and Cyber Security

The college will protect against hazards to the IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect the college's ability to operate and could potentially endanger the safety of our students and staff.

The college will implement the following systems security controls in order to mitigate risks to electronic systems:

Software Download Restrictions

Employees must request authorisation from the ICT Technicians before downloading software on to the college's IT systems. The ICT Technicians will vet software to confirm its security certificate and ensure the software is not malicious. The ICT Technicians will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

Firewalls and Anti-Virus Software

The college will ensure that firewalls and anti-virus software is installed on electronic devices and routers. The college will update the firewalls and anti-virus software when updates are made available through One-IT. The college will review its firewalls and anti-virus software on an annual basis and decide if they are still fit for purpose. The IT Technician 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

The college maintains a shared drive on its servers. Whilst employees 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 employees can access. For example, a HR folder in the staff drive will only be accessible to employees responsible for HR matters. The Headteacher will be responsible for authorising shared drive access rights to employees. Shared drives will still be subject to the college's retention schedule.

Phishing Emails

In order to avoid the college's computer systems from being compromised through phishing emails - employees 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. Employees will check with the ICT Technicians if they are unsure about the validity of an email and must immediately inform the ICT Technicians if they have clicked on a suspicious link. The college will ensure staff have received adequate training to be able to recognise such emails.

Malware Prevention

The college understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

The ICT Technicians will ensure that all college devices have secure malware protection and undergo regular malware scans. The ICT Technicians will update malware protection on a regular basis to ensure it is up-to-date and can react to changing threats.

Secure configuration

An inventory will be kept of all IT hardware and software currently in use at the college, including mobile phones and other personal devices provided by the college. This will be stored in the ICT Support Office and will be kept up-to-date.

Any changes to the IT hardware or software will be documented using the inventory, and will be authorised by the ICT Technicians before use.

All systems will be audited on a semi-annually basis to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security.

Funds permitting any software that is out-of-date or reaches its 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products such that any security issues will not be rectified.

All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed every 90 days to prevent access to facilities which could compromise network security.

The college believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users.

Cloud Computing

The college uses Microsoft Office 365 OneDrive and Atomwide MyUSO for cloud storage, care must be taken to ensure that any personal data stored in the cloud is not downloaded to unencrypted personal devices. Personal data should not be stored on other forms of cloud storage as the data must be stored securely and held in the European Economic Area.

6. Communications Security

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

Secure transfer

All personal data sent to the Local Authority electronically will be sent via the secure site Anycomms.

Personal data sent to other schools will be sent securely through school2schools. For other organisations other than the local authority or schools, the college will ensure that files containing personal data will be encrypted and the password will be provided separately. Alternatively, these can also be sent securely via MyUSO.

Sending Personal Data by post

When sending personal data by post the college will use Royal Mail's standard postal service. Employees 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

Employees 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 then employees are advised to have the envelope double checked by a colleague.

Sending Personal Data and Special Category Data by email

The college will only send personal data including special category data by email if using a secure email transmission portal such as anycomms, school2school transfer or MYUSO.

Employees 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 (that are external to the college, such as parents), 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.

When sending internal emails through the organisation all emails containing personal data should state the word "secure" in the subject. This will encrypt the email.

Exceptional Circumstances

In exceptional circumstance the college may wish to hand deliver to ensure safe transmission of personal data. This could be because the personal data is so sensitive that 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.

7. Surveillance Security

The college operates CCTV software and e-monitoring at its premises.

Due to the sensitivity of information that could be collected as a result of this operation, the college has a separate policy which governs the use of CCTV and surveillance. This policy has been written in accordance with the ICO's Surveillance Code of Practice.

8. Remote Working

It is understood that on some occasion employees of the college will need to work at home or away from the college premises. If this is the case then the employees will adhere to the following controls:

Staff will encrypt devices such as USB sticks which include personal data. If any portable devices are lost, this will prevent unauthorised access to personal data.

Staff and governors who use their personal laptop/computer to access college confidential information must ensure the device has the latest operating system patches and fixes installed along with up-to-date anti-virus/firewall software.

Staff who use college-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off college premises.

Further information regarding remote working can be found in our Remote Access Policy and our Remote Learning and Online Communication Acceptable Use Policy.

Lockable Storage

If employees are working at home, they will ensure that they have lockable storage to keep personal data and college equipment safe from loss or theft.

Employees must not keep personal data or college equipment unsupervised at home for extended periods of time (for example when the employee goes on holiday).

Employees must not keep personal data or college equipment in cars if unsupervised.

Private Working Area

Employees must not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport).

Employees should also take care to ensure that other household members do not have access to personal data and do not use college equipment for their own personal use.

Trusted Wi-Fi Connections

Employees will only connect their devices to trusted Wi-Fi connections and will not use 'free public Wi-Fi' or 'Guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion.

When using home Wi-Fi networks employees should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt employees should seek assistance from the ICT Technicians.

Encrypted Devices and Email Accounts

Employees will only use encrypted devices to work on Personal Data. Employees will not use personal email accounts to access or transmit personal data. Employees must only use college issued email accounts.

Data Removal and Return

Employees will only take personal data away from the college premises if this is required for a genuine business need. Employees will take care to limit the amount of data taken away from the premises.

Employees will ensure that all data is returned to the college premises either for re-filing or for safe destruction. Employees will not destroy data away from the premises as safe destruction cannot be guaranteed.

9. 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.

10. 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.

11. Monitoring & review

This policy will be reviewed on a biennial (2) yearly basis or sooner if circumstances and requirements change by the Senior Teacher – Achievement and Standards (SIRO) together with the Compliance Officer (SPOC).

The next review is December 2027.

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

- Senior Information Risk Owner (SIRO) – The Senior Teacher – Achievement and Standards
- Single Point of Contact (SPOC) – Compliance 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 individual who discovered the breach, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

Assigning Investigation (within 48 hours)

Once received, the SPOC will assess the data protection risks and determine the severity rating using the Risk Matrix. An Investigation Report should also be completed.

The SPOC will notify the Senior Information Risk Owner (SIRO) and the relevant Information Asset Owner (IAO) that the breach has taken place. The SPOC will recommend immediate actions that need to take place to contain the incident.

The IAO will assign an officer to investigate any near misses, very low, low and moderate incidents. High or very high incidents will be investigated by the SPOC or SIRO, with assistance from the Data Protection Officer (DPO).

Reporting to the ICO/Data Subjects (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.

Investigating and Concluding Incidents

The SPOC will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.

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

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

All incidences should be recorded on our Data Breach Log, along with the outcome of the investigation.

DPO contact details:

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

schoolsDPO@veritau.co.uk // 01904 554025