Information Security Policy

Date Adopted: April 2021
Date Reviewed: November 2022
Author/owner: Board of Trustees (Operations, Audit and Risk Committee)
Review: Triennial

NB. 'Trustees' means the Directors referred to in the Trust's Articles of Association

History of most recent policy changes

Version	Date	Page	Change	Origin of Change e.g. TU request, Change in legislation
V1.0	April 2021		New MAT Policy implemented	
	April 2022		Reviewed to reference the TLP Cyber Security, CCTV, Staff Acceptable Use of ICT and Data Protection policies, and to reflect changes to the use of USB storage devices.	
	October 2022		Terminology updated to reflect TLP's new governance structure; review frequency updated	

Contents

Information Security

The Tarka Learning Partnership is committed to a policy of protecting the rights and privacy of individuals (including students, staff and others) in accordance with the Data Protection Act 2018. The Trust gathers and processes personal information about its staff, students, and other individuals to comply with obligations as a charitable company limited by guarantee that is responsible for academies.

The Trust has a responsibility to safeguard individuals from the possibility of information and systems misuse or infringement of personal privacy as well as to protect its reputation. The Information Security Policy outlines the Trust's organisational security processes and standards. The policy is based upon the sixth principle of the UK General Data Protection Regulation (UK GDPR) which states that organisations must protect the personal data, which it processes, against unauthorised loss by implementing appropriate technical and organisational measures. This policy has been written using the security framework recommended by Information Security Standard (ISO): 270001. This policy expands on the Trust's Data Protection Policy.

This policy provides the overall framework to ensure that everyone plays their part in protecting student and staff information. This policy shall be seen as additional to all other Trust policies relating to information disclosure, data protection and personal conduct. This policy should be used in conjunction with the Trust's Cyber Security Policy which sets out detailed guidance and expectations for protection of the Trust against cybercrime and cyber security.

Scope

This policy applies equally to everyone who reads or processes Trust information, including: All staff, whether permanent, temporary or casual; all representatives; all volunteers; third party contractors and consultants; and partners and suppliers.

The policy applies to all forms of information, including but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or electronic means such as email, fax or file transfer;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

The Trust's Cyber Security Policy covers protection of the devices we use, and the services we access online, from theft or damage and preventing unauthorised access to personal data stored on these devices and in the cloud.

The Trust's Staff Acceptable Use of ICT Policy covers detail on staff use of Trust and school computers, IT systems and wireless networks, as well as use of personal devices in school, to ensure responsible and secure use of electronic information systems.

Breaches of policy

Actions or neglect leading to a breach of this policy may result in disciplinary action. Breaches of this policy by a user who is not a direct employee of the Trust may result in action being taken against the user and/or their employer. In certain circumstances it may be necessary to refer breaches to the police and/or the Information Commissioner's Office (ICO) to consider whether criminal proceedings should be instigated.

Roles and responsibilities

All Information Users

- Comply with this policy and related processes, procedures and guidelines;
- Comply with legal, statutory, regulatory and contractual obligations related to information;
- Be familiar with the operation and security requirements of the information and computer systems, to minimise the possibility of harm to confidentiality, integrity and availability;
- Observe the utmost care when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the Trust without proper authorisation;

- Report immediately to the Head Teacher (or otherwise, in accordance with the Whistle Blowing Policy) all suspected violations of this and all other security policies; system intrusions; and any other security incident or weakness which might jeopardise the Academies information or information systems;
- Read and act on any communications and training regarding information security, seeking clarification if these are not understood;
- Play an active role in protecting information in day-to-day work;
- Must not attempt to access information to which they do not have authority.

IT Services

- Be the custodian of electronic information in its care by implementing and administering technical security controls as appropriate;
- Assist in identifying technical information security risks and appropriate technical security controls;
- Assist Tarka Learning Partnership to ensure all software is licensed and remove unlicensed software;
- Provide contingency arrangements for information systems;
- Provide appropriate protection from malicious software;
- Monitor and report breaches of this policy including unauthorised attempts to access information or systems;
- Provide technical support to enable compliance with this policy.

Agreements and contracts with external business partners and suppliers shall, where relevant, include the requirement to adhere to this policy.

Operating within the law

Information shall be used legally at all times, complying with UK and European law. All users, including employees, and agents of the school might be held personally responsible for any breach of the law.

All personal information processed electronically or held in a structured manual filing system shall be processed in accordance with the General Data Protection Regulation 2018. Utmost care shall be taken when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the Academy without proper authorisation.

Personal, confidential or sensitive information shall be protected appropriately at all times and in particular when removed from school premises either physically on paper or electronic storage devices, or when transmitted electronically outside the school.

Personal, confidential or sensitive information should not be included in the text of e-mails to be sent outside the school, or in files attached to them, unless these are securely encrypted or sent by secure network links.

Any request for information under the Freedom of Information Act 2000 shall be handled in accordance with the law and processed in line with the Trust's Freedom of Information Policy.

Information shall not be used in any way that might be seen as defamatory, libellous, insulting or offensive by others. Electronic and non-electronic communications shall not contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity. Note: It is accepted that in some professional situations such information is required for business reasons.

Information, including text, still and moving pictures, photographs, maps, diagrams, music and sound recording shall not be saved, processed or used in breach of copyright.

Protecting the availability of information

Business continuity plans shall include all aspects of the school's infrastructure, which are required to maintain the continuity of all critical business processes and support services. This shall include, but not be limited to, manual filing systems, information systems and communication.

Maintaining the integrity of information

Users are not permitted to modify electronic or manual information storage or processing systems.

Users shall use only the officially provided or approved facilities and systems to access school information.

Users shall not interfere with the configuration of any computing device without approval.

All devices that are subject to the threat of malicious software shall have anti-virus scanning software installed and regularly updated.

USB storage devices are not permitted for use with Trust computing devices.

Access Control

The schools will maintain control over access to the personal data that it processes.

All information about the security arrangements for school computer and network systems and structured manual filing systems is confidential to the school and shall not be released to people who are not authorised to receive that information.

So far as is reasonably practicable only authorised persons will be admitted to rooms that contain servers or provide access to data.

Equipment and paper files must not be left on view in any public setting.

Manual Filing Systems

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 Head Teacher 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 six months or whenever a member of staff leaves the organisation, whichever is sooner.

Electronic Systems

Documents or files containing personal identifiable information should be saved onto a shared network, with appropriate security protection. Access to electronic systems will be controlled through a system of user authentication. A two-tier authentication system will be implemented across all electronic systems. The two tiers will be username and unique password. Passwords should not be written down and/or left on display or be easily accessible.

Individuals will be given access to electronic filing systems if required to carry out legitimate functions. Individuals must not download or store files for use beyond their employment at the school.

Schools should ensure that default download settings, such as Google Takeout, are switched off.

Individuals will be required to change their password on a regular basis and usernames will be suspended either when an individual is on long term absence or when an individual leaves employment of the school. Individuals shall keep personal passwords confidential at all times and not share them with other members of staff under any circumstances.

Access to computer equipment should be restricted by closing windows and doors when the room / office is

not in use. Computer screens should be always be locked (Ctrl, Alt and Del) if being left switched on and unattended.

Mobile devices (e.g. laptops, mobile phones and memory sticks) must be encrypted for all sensitive, personal or confidential data.

Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons or members of the public.

Access will be afforded on a "need to do" basis, and access of leavers removed promptly.

Software and Systems Audit Logs
All school-owned IT equipment, including software, should be recorded and security marked. Users must not make, distribute or use unlicensed software or data on site.

The school will ensure that all major software and systems have inbuilt audit logs so that the school can ensure it can monitor what employees and 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
The school does not allow employees to access the personal data of family members or close friends. Employees should declare, upon employment, whether they are aware of any family members or friends who are registered at the Trust.

The school will then keep paper files in a separate filing cabinet (with access restricted to minimal employees) and where possible any electronic files will be locked down so that the declaring employee cannot access that data.

Employees who knowingly do not declare family and friends registered at the **Trust** may face disciplinary proceedings and may be charged with an offence under Section 170 of the Data Protection Act 2018.

External Access
On occasions the school will need to allow individuals who are not employees of the Trust 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 Trust. The Head Teacher 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 Head Teacher's nominated person.

An access log, detailing who has been given access to what systems and who authorised the access, will be maintained by the school.

Physical Security

The school will maintain high standards of Physical Security to prevent unauthorised access to personal data. The following controls will be maintained by the school:

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 school 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 Head Teacher, who may delegate to a member of their team, 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 to the school will be required to sign in a visitor's book and state their name, organisation, car registration (if applicable) and nature of business. 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 employee supervision.

Environmental Security

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

Back Ups
The individual schools will back up their electronic data and systems on a regular basis. If these backups are kept off site by an external provider, this arrangement will be governed by a data processing agreement. Should the school's electronic systems be compromised by an environmental or natural hazard, then the school will be able to reinstate the data from the backup with minimal destruction.

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

Systems Security

As well as physical security the school also protects against hazards to its IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect the school's ability to operate and could potentially endanger the lives of its Pupils.

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

Software Download Restrictions
All schools within the Trust use a Firewall that features anti-malware protection, HTTPS inspection, anonymous proxy detection & blocking, intrusion detection & prevention and web-filtering.

Schools shall only use licensed software on its computers, servers and all other devices. The school shall provide sufficient legally acquired software to meet all legitimate and agreed needs in a timely fashion.

Phishing Emails
In order to avoid the school'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 Trust if they are unsure about the validity of an email. For further guidance, including reporting phishing emails, please see the Trust's Cyber Security Policy.

Firewalls and Anti-Virus Software
The school will ensure that the firewalls and anti-virus software is installed on electronic devices and routers. The school will update the firewalls and anti-virus software when updates are made available and when advised to do so by IT. The school will review its firewalls and anti-virus software on an annual basis and decide if they are still fit for purpose.

Appropriate security patches will be applied to all devices that are subject to the threat of security vulnerabilities. For detailed guidance on device and network security, please see the Trust's Cyber Security Policy.

Shared Drives
The school 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 shared drive will only be accessible to employees responsible for HR matters. Head Teacher, who may delegate to a member of their team, will be responsible for giving shared drive access rights to employees. Shared drives will still be subject to the school's retention schedule.

All data, whether paper or electronic, must be disposed of properly and in accordance with the Trust's Records Management and Retention schedule.

PCs and laptops must be disposed of securely, through the school's current approved supplier list.

If a PC or laptop is to be given to another user, personal data should first be removed from it (e.g. student databases, free Trust meal information, etc).

It is imperative that staff follow any guidelines issued when overwriting data. Sending information to a computer's recycle bin does not delete the data as such. It is therefore important to empty the recycle bin regularly.

Paper records containing personal data or confidential information must be shredded or placed within confidential waste bins for secure disposal.

Communications Security

The transmission of personal data is a key business need and, when operated securely is a benefit to the school and pupils alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. The Data Protection Act 2018 should be considered at all times when recording, sharing, deleting or withholding information.

The school has implemented the following transmission security controls to mitigate these risks:

- Sensitive information must not be shared unless the person is authorised to receive it.
- Any transfers of confidential information should be secure and the method risk assessed.
- For electronic information transfers encrypted software should be used (e.g. Egress).

Giving Personal Data by telephone
When information is requested by telephone it is important to:

- Ask the caller to confirm their name, job title, department and organisation and verify this by returning their call via their organisation's switchboard;
- Confirm the reason for the request;
- Be satisfied that disclosure of the requested information is justified;
- Place a record on the student / staff file noting the name of the person disclosing the information, the date and time of the disclosure, the reason for the disclosure, who authorised it (if applicable) and the recipient's details.

Sending Personal Data by post
When sending personal data, excluding special category data, by post, the school 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.

When sending personal or sensitive information by post:
- Check the name, department and address of the intended recipient;
- Use a robust envelope, clearly marked "PRIVATE & CONFIDENTIAL To be opened by the addressee only";
- Information to a service or department within the Local Authority should be sent using the internal post system;
- If the public post system is to be used a return address must be recorded on the outside of the envelope, and recorded delivery should be used if the information is considered to be highly sensitive.

When sending personal or sensitive information by fax, the sender must:
- Check that there is a designated person who will collect the fax;
- Telephone the recipient to advise that a confidential fax is being sent to them, confirm the fax number and request a receipt;
- Check that the recipient fax machine is sited in a secure room and is not used by more than one department;
- Ensure that a cover sheet is included with the fax and shows the name of the recipient and the following wording: *"The information contained in this fax is STRICTLY PRIVATE & CONFIDENTIAL and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error please notify the sender immediately. Thank you."*

Sending Special Category Data by post
When sending special category data by post the school will use Royal Mail's 1st Class Recorded 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. 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 school will only send personal data and special category data by email if using a secure email transmission portal such as Egress.

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.

Exceptional Circumstances
In exceptional circumstances the school 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.

Using the BCC function
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 school employees will utilise the Blind Copy (BCC) function.

Surveillance Security
The school may or may not operate CCTV at its premises. Schools operating CCTV will abide by the Trust's CCTV Policy.

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

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

Lockable Storage
If employees are working at home they will ensure that they have lockable storage to keep personal data and school equipment safe from loss or theft. If the employee does not have access to lockable storage then they may apply to the school for assistance in purchasing such storage, at the discretion of the Head Teacher. Employees must not keep personal data or school equipment unsupervised at home for extended periods of time (for example when the employee goes on holiday).

Employees must not keep personal data or school 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 school 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 school's IT provider.

Encrypted Devices and Email Accounts
Employees will only use school issued encrypted devices to work on Personal Data. Employees will not use personal devices for accessing, storing, or creating personal data. This is because personal devices do not possess the same level of security as a school issued device.

Employees will not use personal email accounts to access or transmit personal data. Employees must only use school issued, or Trust authorised, email accounts.

Data Removal and Return
Employees will only take personal data away from the school 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 school premises either for re-filing or for safe destruction. Employees will not destroy data away from the premises as safe destruction cannot be guaranteed.

Monitoring

Use of electronic and non-electronic information and the use of information systems shall be monitored for the following reasons:

- To ensure adherence to this policy;
- To detect and investigate unauthorised use of information;
- To maintain the effectiveness, integrity and security of the computer network;
- To ensure that the law is not being contravened; to protect the services provided by the Trust to the public; and to protect the integrity and reputation of the Trust.

All monitoring shall be:

- Fair and proportionate to the risks of harm to the Trust's information and reputation;
- Undertaken so as to intrude on users' privacy only as much as is necessary;
- Carried out similarly regardless of whether the user is Trust-based or working remotely; and
- Carried out in accordance with legislative requirements.

Access to any records of usage will be stringently controlled.

Reporting information security breaches

In the event of loss or theft of computer equipment the Head Teacher must be informed at the earliest opportunity.

Security issues should be raised with the Head Teacher in the first instance. If this is not appropriate reference should be made to the Whistleblowing Policy.

Reports may be made by phone, face to face, or in writing.

Policy review

This policy shall be reviewed every three years. All users shall be informed of changes to this policy which affect them.

Declaration

I accept that I have a responsibility to safeguard Tarka Learning Partnership information and equipment by abiding by the conditions of use defined in this Information Security Policy.

I understand that misuse of electronic and other communications may lead to consequences, which could be harmful to individuals, the Trust or other organisations. I understand that for certain types of misuse, I may be open to criminal prosecution under the Obscene Publications Act, the Computer Misuse Act or the Data Protection Act.

I understand that in order to ensure that the Information Security Policy is properly followed, and to maintain the effectiveness, integrity and security of the network, the use of electronic communications will be monitored.

Name: ……

Signed: ……

Date: ……