SCHOOL POLICY

Cyber Security Policy

Reviewed by:	Resources Committee.
Signed (Governing Body):	
Date:	April 2025
Next Review due:	April 2026

Produced by Turton School

Contents:

Statement of intent

Turton School is committed to maintaining the confidentiality, integrity and availability of its information and ensuring that the details of the finances, operations and individuals within the school are only accessible to the appropriate individuals. It is, therefore, important to implement appropriate levels of access, uphold high standards of security, take suitable precautions, and have systems and procedures in place that support this.

The school recognises, however, that breaches in security can occur, with most breaches caused by human error. The school will ensure all staff are aware of how to minimise this risk. In addition, because most information is stored online or on electronic devices that can be vulnerable to cyber-attacks, the school will ensure there are procedures in place to prevent attacks occurring. To minimise both risks, it is necessary to have a contingency plan containing a procedure to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

1. LEGAL FRAMEWORK

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- National Cyber Security Centre (N.D.) 'Cyber Essentials'
- ICO (2022) 'Guide to the General Data Protection Regulation (GDPR)'
- (DfE) (2023) 'Meeting digital and technology standards in schools and colleges'

This policy operates in conjunction with the following school policies:

- Online Safety Policy
- Data Protection Policy
- Disciplinary Policy and Procedure
- Behaviour Policy
- Social Media Policy
- Remote Education Policy
- IT Disaster Recovery Plan

2. TYPES OF SECURITY BREACH AND CAUSES

Unauthorised use without damage to data – involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it. This includes unauthorised people within the school, e.g. schools where pupils access systems that staff have left open and/or logged in, or where staff access data beyond their authorisation, as can occur in schools where all staff are given admin-level access for ease.

Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access. This is also known as data theft. The data may be forwarded or deleted altogether.

Damage to physical systems – involves damage to the hardware in the school's ICT system, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

Unauthorised damage to data – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused by the actions of individuals, and may be accidental, malicious or the result of negligence:

- Accidental breaches can occur as a result of human error or insufficient training for staff, so they are unaware of the procedures to follow
- Malicious breaches can occur as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data

Breaches caused by negligence can occur as a result of a staff member knowingly disregarding school policies and procedures or allowing pupils to access data without authorisation and/or supervision.

Breaches in security may also be caused by system issues, which could involve incorrect installation, configuration problems or operational errors:

- The incorrect installation of antivirus software and/or use of outdated software can make the school software more vulnerable to a virus
- Incorrect firewall settings being applied, e.g. unrestricted access to the school network, can allow unauthorised individuals to access the school system
- Operational errors, such as confusion between back-up copies of data, can cause the most recent data to be overwritten
- Staff role changes causing configuration errors.

3. ROLES AND RESPONSIBILITIES

The governing board will be responsible for:

- Ensuring the school has appropriate cyber-security measures in place.
- Ensuring the school has an appropriate approach to managing data breaches in place.
- Supporting the headteacher and other relevant staff in the delivery of this policy.
- Ensuring the school meets the relevant cyber-security standards.
- Ensuring at least one member of the board completes basic cyber-security training.

The headteacher will be responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Ensuring appropriate user access procedures are in place.
- Responding to alerts for access to inappropriate content in line with the Online Safety Policy.
- Organising training for staff members in conjunction with the DPO.
- Appointing an IT disaster recovery team (head teacher, deputy head, business manager, IT manager and IT technician) who is responsible for implementing the school's procedures in the event of a cyber-security incident.

The DPO will be responsible for:

- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use.
- Leading on the school's response to incidents of data security breaches.
- Assessing the risks to the school in the event of a cyber-security breach.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.
- Working with the ICT manager and headteacher after a data security breach to determine where weaknesses lie and improve security measures.

- Organising training for staff members on data security, network security and preventing breaches.
- Monitoring and reviewing the effectiveness of this policy, alongside the headteacher, and communicating any changes to staff members.

The ICT manager will be responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the school.
- Ensuring any obsolete software is removed from the school systems.
- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Installing, monitoring and reviewing filtering systems for the school network.
- Setting up user privileges in line with recommendations from the headteacher.
- Removing any inactive users from the school system and ensuring that this is always up-to-date.
- Installing appropriate security software on staff members' personal devices where the headteacher has permitted for them to be used for work purposes.
- Performing a back-up of all electronic data held by the school, ensuring detailed records of findings are kept.
- Ensuring all school-owned devices have secure malware protection and are regularly updated.
- Recording any alerts for access to inappropriate content and notifying the headteacher.

The DSL will be responsible for:

- Assessing whether there is a safeguarding aspect to any cyber-security incident and considering whether any referrals need to be made.

All staff members will be responsible for:

- Understanding their responsibilities in regard to this policy.
- Undertaking the appropriate training.
- Ensuring they are aware of when new updates become available and how to safely install them.

4. SECURE CONFIGURATION

An inventory will be kept of all ICT hardware and software currently in use at the school, including mobile phones and other personal devices provided by the school. The inventory will be stored as a spreadsheet on teams will be audited on a termly basis to ensure it is up-to-date. Any changes to the ICT hardware or software will be documented using the inventory and will be authorised by the ICT technician before use.

All systems will be audited on a termly basis by the ICT technician 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, and will be recorded in the inventory. Any obsolete software will be removed from systems.

All hardware, software and operating systems will require passwords from individual users. The school 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. Passwords will need to adhere to a specific character length and not be obvious or easy to guess, in line with the school's policy on passwords.

The school will refer to the five security controls outlined in the National Cyber Security Centre's (NCSC's) 'Cyber Essentials'. These are:

- **Firewalls** – Firewalls function as a barrier between internal networks and the internet. They will be installed on any device that can access the internet, particularly where staff are using public or otherwise insecure Wi-Fi.
- **Secure configuration** – The default configurations on devices and software are often as open as possible to ensure ease of use, but they also provide more access points for unauthorised users. The school will disable or remove any unnecessary functions and change default passwords to reduce the risk of a security breach.
- **Access control** – The more people have access to data, the larger the chance of a security breach. The school will ensure that access is given on a 'need-to-know' basis to help protect data. All accounts will be protected with strong passwords, and where necessary, two-factor authorisation.
- **Malware protection** – The school will protect itself from malware by installing antivirus and anti-malware software, and using techniques such as whitelisting (a cyber-security strategy under which a user can only take actions on their computer that an administrator has explicitly allowed in advance) and sandboxes (an isolated virtual machine in which potentially unsafe software code can execute without affecting network resources or local applications).
- **Patch management** – The school will install software updates as soon as they are available to minimise the time frame in which vulnerabilities can be exploited. If the manufacturer stops offering support for the software, the school will replace it with a more up-to-date alternative.

The ICT manager will:

- Protect all devices, where possible, on every network with a correctly configured boundary, or software firewall, or a device that performs the same function.
- Change the default administrator password, or disable remote access on each firewall.
- Protect access to the firewall's administrative interface with a specified IP-allow list combined with a managed password, or prevent access from the internet entirely.
- Keep firewall firmware up to date.
- Check monitoring logs to help detect suspicious activity.
- Block inbound unauthenticated connections by default.
- Review reasons why particular inbound traffic has been permitted through the firewall often, change the rules when access is no longer needed.
- Enable a software firewall for devices used on untrusted networks, like public wi-fi.

5. NETWORK SECURITY

In line with the UK GDPR, the school will appropriately test, assess, and evaluate any security measures put in place on a yearly basis to ensure these measures remain effective.
The school will employ firewalls in order to prevent unauthorised access to the systems.

Localised firewall deployment
The school's firewall will be deployed as a localised deployment, which means the broadband service connects to a firewall that is located on an appliance or system on the school premises, as either discrete technology or a component of another system.

As the school's firewall is managed on the premises, it is the responsibility of the ICT technician to effectively manage the firewall. The ICT technician will ensure that:

- The firewall is checked monthly for any changes and/or updates, and that these are recorded using the inventory.
- Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.
- The firewall is also checked monthly to ensure that a high level of security is maintained, and there is effective protection from external threats.

Any compromise of security through the firewall is recorded and is reported to the DPO. The ICT technician will react appropriately to security threats to find new ways of managing the firewall.

The school will be aware that security standards may change over time with changing cyber threats, and that the security of every device on its network is reviewed regularly.

The school will agree with the ICT technician a system for recording and reviewing decisions made about network security features.

To ensure that the network is as secure as possible, the school will:

- Keep a register, list, or diagram of all the network devices.
- Avoid leaving network devices in unlocked or unattended locations.
- Remove or disable unused user accounts, including guest and unused administrator accounts.
- Change default device passwords.
- Require authentication for users to access sensitive school data or network data.
- Remove or disable all unnecessary software according to your organisational need.
- Disable any auto-run features that allow file execution.
- Set up filtering and monitoring services to work with the network's security features enabled.
- Immediately change passwords which have been compromised or suspected of compromise.
- Protect against a brute-force attack on any account by having an increasing delay between unsuccessful password attempts.

Unlicensed hardware or software will never be used by the school.

All unpatched or unsupported hardware or software will be replaced by the ICT technician. Where it is not possible to replace these devices, they will have their access to the internet removed so that scanning tools cannot find weaknesses.

6. MALWARE PREVENTION

The school 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 technician will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements. The ICT technician will update malware protection on a daily basis to ensure it is up-to-date and can react to changing threats. Malware protection will also be updated in the event of any attacks to the school's hardware and software.

Staff will follow procedures for filtering and monitoring to keep pupils safe as set out in the Online Safety Policy. The school's filtering provider will be:

- A member of Internet Watch Foundation (IWF)
- Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- Effective at blocking access to illegal content

The filtering system will be able to identify known technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them, and provide alerts when any web content has been blocked

Filtering of websites will ensure that access to websites with known malware are blocked immediately.

The school will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users. The ICT technician will review the mail security technology on a **termly** basis to ensure it is kept up-to-date and effective.

Where apps are installed, the ICT technician will keep up-to-date with any updates, ensuring staff are informed of when updates are ready and how to install them.

The school will use anti-malware software that:

- Is set up to scan files upon access, when downloaded, opened, or accessed from a network folder.
- Scans web pages as they are accessed.
- Prevents access to potentially malicious websites, unless risk-assessed, authorised and documented against a specific business requirement.

7. USER PRIVILEGES AND PASSWORDS

The school understands that controlling what users have access to is important for promoting network security and data protection. User privileges will be differentiated, e.g., pupils will have different access to data and the network than members of staff, whose access will also be role-based.

The headteacher will clearly define what users have access to and will communicate this to the ICT manager, ensuring that a written record is kept. The ICT manager will ensure that user accounts are set up to allow users access to the facilities required, in line with the headteacher's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

All users will be required to change their passwords if they become known to other individuals, in line with the 'Secure configuration' section of this policy. Pupils are responsible for remembering their passwords; however, the ICT technician will be able to reset them if necessary. Multi-factor authentication (multiple different methods of verifying the user's identity) should be used wherever possible.

A multi-user account will be created for visitors to the school and access will be filtered as per the headteacher's instructions. Usernames and passwords for this account will be changed on a termly basis and will be provided as required.
The school will implement a user account creation, approval and removal process which is part of the school joining and leaving protocols.

User accounts and access privileges will be appropriately controlled, and only authorised individuals will have an account which enables them to access, alter, disclose or delete personal data. Users will have a separate account for routine business if their main account:

- Is an administrative account.
- Enables the execution of software that makes significant system or security changes.
- Can make changes to the operating system.
- Can create new accounts.
- Can change the privileges of existing accounts.

The school will consider using multi-factor authentication, particularly for accounts that have access to sensitive or personal data.

8. MONITORING USAGE

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff. The school will inform all pupils and staff that their usage will be monitored, as well as how it is being monitored and why, in accordance with the school's Online Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the ICT manager. Alerts will also be sent for unauthorised and accidental access. Alerts will identify the user, the activity that prompted the alert, and the information or service the user was attempting to access.

The ICT manager will report this to the DPO. The DPO will then inform the headteacher as appropriate.

The ICT manager will ensure that websites are filtered for inappropriate and malicious content.

All data gathered by monitoring usage will be kept for easy access when required. This data may be used as a method of evidence for supporting a not-yet-discovered breach of

network security. In addition, the data may be used to ensure the school is protected and all software is up-to-date.

9. REMOVABLE MEDIA CONTROLS

The school understands that pupils and staff may need to access the school network from outside the school premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

The ICT manager will ensure all school-owned devices for personal use, such as laptops, phones and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

Before distributing any school-owned devices, the ICT manager will ensure that manufacturers' default passwords have been changed. A set password will be chosen, and the staff member will be prompted to change the password once using the device.
When using laptops, tablets and other portable devices, the headteacher will determine the limitations for access to the network, as described in the 'Network security' section of this policy.

Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off the school premises. Staff will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any school-owned laptops, tablets or other devices, or when accessing school networks.

All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls
.
The Wi-Fi network at the school will be password protected and will only be given out as required. Pupils in years 7 to 11 are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless agreed prior to usage. A separate Wi-Fi network will be established for visitors at the school to limit their access to school networks and any other applications which it is not necessary for them to access.

10. HOME WORKING AND REMOTE LEARNING

Staff and pupils will adhere to data protection legislation and the school's related policies when working remotely.

Staff will receive annual training regarding what to do if a data protection issue arises from any home working or remote learning.

Wherever possible, personal data will not be taken home by staff members for the purposes of home working, due to the risk of data being lost or the occurrence of a data breach.

Staff and pupils may be required to use their own devices for the duration of the remote working or learning period. Any user on a personal device will need to access the school system through a proxy, e.g. VPN. Using a shared personal or household device for school purposes should be avoided where possible; however, the school understands that this may not always be possible.

Staff and pupils are not permitted to let their family members or friends use any school equipment, in order to protect the confidentiality of any personal data held on the device. Any staff member found to have shared personal data without authorisation will be

disciplined in line with the Disciplinary Policy and Procedure. This may also result in a data breach that the school would need to record and potentially report to the ICO.

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. School devices will automatically lock after fifteen minutes of inactivity to avoid an unauthorised person gaining access to the device.

To ensure reasonable precautions are taken when managing data, staff will avoid:

- Keeping personal data on unencrypted hard drives.
- Sending work emails to and from personal email addresses.
- Leaving logged-in devices and files unattended.
- Using shared home devices where other household members can access personal data.
- Using an unsecured Wi-Fi network.

Staff working from home will be encouraged and enabled to go paperless, where possible, as paper files cannot be protected digitally and may be misplaced. If sensitive data is taken off the school premises to allow staff to work from home, it will be transported in a secure manner. The school's procedures for taking data off the school premises will apply to both paper-based and electronic data.

Pupils cannot alter the passwords or encryptions protecting school documents and systems put in place by the school. Pupils cannot alter or disable any security measures that are installed on school devices, e.g. firewalls, malware prevention or anti-virus software. Pupils cannot share any confidential and/or personal information made accessible to them, e.g. VPN passwords, with anyone who is not authorised to view that information.

Pupils that do not use school devices or software in accordance with this policy will be disciplined in line with the Behavioural Policy.

Any devices that are used by staff and pupils for remote working and learning will be assessed by the ICT technician prior to being taken to the home setting, using the following checks:

- System security check – the security of the network and information systems
- Data security check – the security of the data held within the systems
- Online security check – the security of any online service or system, e.g. the school website

The ICT technician will provide staff and pupils with details and instructions for accessing the school network that they will be using throughout the duration of the remote working and learning period.

In the event that a staff member or pupil decides to leave the school permanently, all data in any form will be returned on or before their last day.

11. BACKING UP DATA

The ICT manager performs a back-up of all electronic data held by the school on a termly basis, and the date of the back-up is recorded using a log. Each back-up is retained for three months before being deleted. The ICT manager performs an incremental back-up on a weekly basis of any data that has changed since the previous back-up.

The ICT manager will ensure that there are at least three backup copies of important data, a copy on the server, a copy on the backup server and tapes kept in a fire proof safe.
The number of devices with access to back up data will be kept to an absolute minimum.

The school will follow the NCSC's guidance on backing up data where necessary, including:

- Identifying what essential data needs to be backed up.
- Storing backed-up data in a separate location to the original data.
- Ensuring that backing up data is regularly practised.

The school will keep under review where servers can be replaced with cloud solutions, including accessing files, documents and shared folders. Where cloud solutions are used, the school will confirm its ICT provider ensures that data is portable and allows for:

- Secure encrypted transfer.
- Data export to an open standard or commonly used format.
- Data links through secure, documented application programming interfaces (APIs).
- A timely process for data transfer in an open standard or neutral format if the school ends the contract.
- Easy and secure access from a range of devices.

12. AVOIDING PHISHING ATTACKS

The ICT manager will configure all staff accounts using the principle of 'least privilege' – staff members are only provided with as much rights as are required to perform their jobs. Designated individuals who have access to the master user account will avoid browsing the web or checking emails whilst using this account.

Staff will use the following warning signs when considering whether a communication may be unusual:

- Is it from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is it addressed to a 'valued customer', 'friend' or 'colleague'?
- Does it contain a veiled threat that asks the staff member to act urgently?
- Is it from a senior member of the school asking for a payment?
- Is it from a supplier advising of a change in bank account details for payment?
- Does it sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.
- Is it from a generic email address, such as Gmail or Hotmail?

The ICT manager will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam, applied in accordance with the 'Malware prevention' section of this policy.

13. USER TRAINING AND AWARENESS

The DPO and headteacher will arrange training for pupils and staff on an annual basis to ensure they are aware of how to use the network appropriately. This will cover identifying irregular methods of communication in order to help staff members spot requests that are out of the ordinary.

Staff with access to the school's IT network will be required to undertake basic cyber-security training upon induction which is refreshed every year. At least one member of the governing board will also take part in this training. The training will focus on the following:

- Phishing
- Password security
- Social engineering
- The dangers of removable storage media

All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Behavioural Policy and the Disciplinary Policy and Procedure.

14. CYBER-SECURITY INCIDENTS

All cyber-security incidents will be managed in line with the school's IT Disaster Recovery Plan.