Cyber Security Policy

Date	Review Date	Coordinator
Nov 2023	Sept 2026	Sarah Nichols-Weaver

We believe this policy should be a working document that is fit for purpose, represents the school ethos, enables consistency and quality across the school and is related to the following legislation:

- Equality Act 2010
- Data Protection Act 2018
- General Data Protection Regulations 2018

The following documentation is also related to this policy:

- Cyber security in schools (National Cyber Security Centre)
- Equality Act 2010: Advice for Schools (DfE)
- Race Disparity Audit - Summary Findings from the Ethnicity Facts and Figures Website (Cabinet Office)
- Data Protection: a toolkit for schools (DfE)
- Preparing for the General Data Protection Regulation (GDPR) - Information Commissioner's Office

We are aware that 'cyber security is about protecting the devices we all use and the services we access online, both at home and at work, from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices.' (Cyber security in schools (National Cyber Security Centre))

We realise that online criminals, hackers, malicious insiders, schools and mistakes made by school personnel are behind cyber attacks.

We understand cyber risk means 'any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems'.

We have a duty to keep our systems, people and data secure and safe from harm as schools face the same cyber security threats as other organisations. All school systems hold information on school personnel and pupils such as medical history, home addresses, phone numbers and bank details. We understand that if a virus penetrates our system then all our information is at risk and could be encrypted, stolen, sold or used by criminals.

We acknowledge the advice from the Information Commissioner that schools must be vigilant about information security and has warned that unauthorised access to personal information would be harmful to pupils, school personnel and parents. We realise we are also exposed to other risks relating to online security such as exposure to sexually explicit, racist, violent and extremist material; inappropriate contact from people who may wish to abuse, exploit or bully them; and pupils who may engage in harmful online behaviour.

We have a duty to have in place 'an effective approach to online safety' in order to 'protect and educate the whole school community in their use of technology and establish mechanisms to identify, to intervene in and to escalate any incident where appropriate.'

We understand that the most serious cyber threats that we may be at risk from are:

- **Ransomware** which is a form of malicious software that attempts to encrypt data then extort a ransom to release an unlock code. Ransomware is usually delivered by malicious emails.

- **Phishing** which is an attempt to gain sensitive information while posing as a trustworthy contact.

- **Data leakage** from the use of smart phones and tablets when used for the backup and the transportation of data has become a target for data thieves.

- **Hacking** by data thieves gaining access to IT systems by the use of social engineering and by tricking school personnel into revealing names and passwords.

- **Insider threat** from school personnel or by contractors leaking data accidently or maliciously.

We have a duty to ensure school personnel will:

- never ignore software updates;
- always lock their devices when they are not being used;
- download apps and software from official app stores;
- not share accounts with others;
- not be afraid to challenge policies and procedures that make their job difficult;
- question that if it looks strange then get a second opinion

We believe we work hard to ensure that we protect our valuable data from cyber risk by having in place excellent technology, well-developed processes, procedures, training for school personnel and by educating pupils.

We wish to work closely with keyworkers and to hear their views and opinions as we acknowledge and support Article 12 of the United Nations Convention on the Rights of the Child that children should be encouraged to form and to express their views.

We as a school community have a commitment to promote equality. Therefore, an equality impact assessment has been undertaken and we believe this policy is in line with the Equality Act 2010.

We all have a responsibility to ensure equality permeates in to all aspects of school life and that everyone is treated equally irrespective of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation. We want everyone connected with this school to feel safe, secure, valued and of equal worth.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy.

Aims

- To strengthen and unify the safety and security of all data held within the school by having in place an effective approach to online safety.
- To ensure the protection of all personal and sensitive data for which we hold responsibility as the Data Controller.
- To ensure compliance with all relevant legislation connected to this policy.
- To work with other schools and the local authority to share good practice in order to improve this policy.

Responsibility for the Policy and Procedure

Role of the Governing Body

The Governing Body has:

- in accordance with the GDPR appointed a Data Protection Officer who has expert knowledge of data protection law and practices;
- delegated powers and responsibilities to the Headteacher to ensure all school personnel and stakeholders are aware of and comply with this policy;
- responsibility for ensuring:

    - ☐ full compliance with all statutory responsibilities;
    - ☐ the school complies with all equalities legislation;
    - ☐ funding is in place to support this policy;
    - ☐ this policy and all policies are maintained and updated regularly;
    - ☐ all policies are made available to parents;
    - ☐ the nomination of a designated Equalities governor to ensure that appropriate action will be taken to deal with all prejudice related incidents or incidents which are a breach of this policy;

        - determining this policy with the Governing Body;
        - discussing improvements to this policy during the school year;

- organising surveys to gauge the thoughts of all pupils;
- reviewing the effectiveness of this policy with the Governing Body

☐ Trustees to:

- visit the school regularly;
- work closely with the Headteacher and the Data Protection Officer;
- ensure this policy and other linked policies are up to date;
- ensure that everyone connected with the school is aware of this policy;
- attend training related to this policy;
- report to the Governing Body every term;
- annually report to the Governing Body on the success and development of this policy

☐ the effective implementation, monitoring and evaluation of this policy

Role of the Headteacher

The Headteacher will:

- work in conjunction with the Data Protection Officer to ensure all school personnel, pupils and parents are aware of and comply with this policy;
- ensure risk assessments are:

  ☐ in place and cover all aspects of this policy;
  ☐ accurate and suitable;
  ☐ reviewed annually;
  ☐ easily available for all school personnel

- have in place an effective approach to deal with cyber security and online safety approaches:

  ☐ **Personnel**
  - Data Protection Officer in place
  - Designated Safeguarding Lead in place
  - Cyber security discussed regularly at governing body meetings and with the SLT

  ☐ **Cyber Threats and Online Security**
  - Firewalls and internet gateways in place and monitored and tested daily/weekly
  - Cyber security controls in place to deal with cyber threats such as:

    Ransomware
    - School personnel trained to be wary of unsolicited emails that require a prompt response.
    - Malware protection software installed and maintained.
    - All applications are kept up to date.
    - Data backup procedures are in place in order to allow recovery from an unencrypted file.

    Phishing
    - School personnel trained to be suspicious of unexpected emails.
    - Anti-malware software in place.
    - Spam filters in place and regularly checked.

    Data leakage
    - All mobile devices have pass code locks.
    - Encryption software in place.
    - Ensure mobile devices can be remotely wiped by ensuring GPS is turned on at all times.
    - Ensure mobile devices are secure at all times.

    Insider threat
    - School personnel:

- trained to be alert to issues and to minimise careless mistakes;
- allowed minimum access to IT system in order to undertake their role;
- controlled use of USB pen drive, portable hard drives and media players

☐ **Content Filtering**
- Content filtering in place and regularly updated

☐ **Access Controls**
- Minimum access privileges for users in place
- Records kept of user access privileges

☐ **Third Party Providers**
- Third party platform providers thoroughly vetted to ensure their security and safety are as strict as the school

☐ **Hardware and Software**
- All hardware and software authorised and documented before use
- Approved users can only make changes to devices
- Software updates and security patches implemented when release by manufacturers

☐ **Online Safety Education**
- Pupils taught about online safety as part of safeguarding for schools
- Pupils taught about the acceptable use of smart phones on and off the school premises
- School personnel aware of the risks regarding acceptable and secure use of systems

☐ **Security of Hardware**
- Hard drives, internet routers, services and other devices securely stored

- work closely with the link governor;
- provide leadership and vision in respect of equality;
- make effective use of relevant research and information to improve this policy;
- provide guidance, support and training to all staff;
- make effective use of relevant research and information to improve this policy;
- monitor the effectiveness of this policy by speaking with pupils, school personnel, parents and governors;
- annually report to the Governing Body on the success and development of this policy

Role of the Data Protection Officer

The Data Protection Officer will:

- work with the Headteacher to ensure an effective approach to deal with cyber security and online safety is in place and is constantly monitored and reviewed;
- have expert knowledge of data protection law and practices;
- manage internal data protection activities;
- ensure risk and impact assessments are conducted in accordance with ICO guidance;
- report data breaches within 72 hours;
- have in place a Critical Incident Plan to deal with any data breach:

  ☐ System temporarily shut down
  ☐ Bank and credit card companies informed
  ☐ Action Fraud informed
  ☐ Change passwords
  ☐ Inform all stakeholders
  ☐ IT consultant employed to assess the extent of the breach
  ☐ Incident documented for possible enquiry

- ensure individuals have greater control over their personal data;

- ensure the secure disposal of redundant data and IT hardware holding data in compliance with ICO guidance;
- train school personnel;
- keep up to date documentation of all data protection activities;
- work closely with the Headteacher and nominated governor;
- periodically report to the Headteacher and to the Governing Body;
- annually report to the Governing Body on the success and development of this policy

Role of School Personnel

School personnel will:

- comply with all aspects of this policy;
- attend awareness training regarding online safety and cyber threats;
- be aware that in order to prevent unauthorised users accessing devices or networks will:

  - ☐ have a different password for each account or service;
  - ☐ store passwords securely away from their device(s);
  - ☐ use a two factor authentication on sensitive accounts;
  - ☐ always lock their account when they step away or stop using their device

- not include the following when choosing a password:

  - ☐ Partner's name
  - ☐ Child's name
  - ☐ Pet's name
  - ☐ Place of birth
  - ☐ Favourite holiday
  - ☐ Something related to a sports team
  - ☐ A list of numbers or words like 'password' or 'qwerty'

- be aware of 'phishing' emails and will be aware of the following clues that a phishing email might include:

  - ☐ Does it contain poor quality images or logos?
  - ☐ Are there spelling or grammatical errors?
  - ☐ Does it address you as 'dear friend' rather by name?
  - ☐ Is it asking you to act urgently?
  - ☐ Does it refer to a previous message you don't remember seeing?

- only USBs or pen drives that have been provided by the school;
- ensure the USB is password protected;
- keep work information safe when working from home by:

  - ☐ using up to date anti-virus software;
  - ☐ downloading all software updates as soon as they are offered;
  - ☐ ensuring all devices have passwords;
  - ☐ changing any default passwords on devices or software including home wi-fi;
  - ☐ switching on two-factor authentication for sensitive accounts

(Cyber security in schools (National Cyber Security Centre))

- be aware of all other linked policies.

Role of Pupils

Pupils will be:

- aware of and comply with this policy;

- taught about:

  - ☐ online safety as part of safeguarding for schools;
  - ☐ the acceptable use of smart phones on and off the school premises;
  - ☐ the risks regarding acceptable and secure use of systems

Role of Parents/Carers

Parents/carers will

- be aware of and comply with this policy;
- work in partnership with the school;
- be invited to attend awareness training about online safety as part of safeguarding for schools.

Raising Awareness of this Policy

We will raise awareness of this policy via:

- School Handbook/Prospectus;
- School website;
- Staff Handbook;
- Meetings with parents such as introductory, transition, parent-teacher consultations and periodic curriculum workshops;
- School events;
- Meetings with school personnel;
- Written communications with home such as weekly newsletters and of end of half term newsletters;
- Annual report to parents;
- Headteacher reports to the Trustee Body;
- Information displays in the main school entrance;
- Text messages
- Email

Training

We:

- have in place appropriate training for this policy that is undertaken by a registered training provider that covers:

  - ☐ All aspects of this policy
  - ☐ General Data Protection Regulation
  - ☐ Data Protection Act 1998
  - ☐ Freedom of Information 2000
  - ☐ Access to Personal Records
  - ☐ E-safety
  - ☐ Safeguarding and Child Protection
  - ☐ Equality
  - ☐ Inclusion

- ensure the content of all training is correct, delivered well and engages staff as we believe that the more engaging training is, the better the outcomes that we need to measure;
- can provide data that evidences staff understanding by using a simple short multiple-choice test through one of the following applications such as Google Forms, Microsoft Forms, Kahoot or SurveyMonkey;
- have in place evidence for all staff:

  - ☐ that highlights the knowledge gaps in the training;
  - ☐ that shows how those knowledge gaps were corrected

Equality Impact Assessment

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation.

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil and it helps to promote equality at this school.

Race Disparity Audit

We acknowledge the findings of the Race Disparity Audit that clearly shows how people of different ethnicities are treated across the public services of health, education, employment and the criminal justice system.

The educational section of the audit that covers: differences by region; attainment and economic disadvantage; exclusions and abuse; and destinations, has a significant importance for the strategic planning of this school.

Monitoring the Implementation and Effectiveness of the Policy

The practical application of this policy will be reviewed annually or when the need arises by the coordinator, the Headteacher and the nominated governor.

A statement of the policy's effectiveness and the necessary recommendations for improvement will be presented to the Governing Body for further discussion and endorsement.

Linked Policies

- Acceptable Internet Use Agreement
- Curriculum
- Data Protection and the General Data Protection Regulation
- Equality
- E-Safety
- Internet Social Networking Websites
- Mobile Phone Safety and Acceptable Use
- Safeguarding and Child Protection
- School Crisis Management
- School Disaster Recovery

See Appendices Documents section on Policies for Schools Website

- Frequency of Policy Monitoring
- Monitoring Implementation and Policy Effectiveness Action Plan
- Initial Equality Impact Assessment
- Policy Evaluation
- Policy Approval Form

We believe this school policy:

- is an essential part of the school;
- supports staff in managing certain situations;
- forms an important framework that will ensure consistency in applying values and principles throughout the establishment;
- provides guidance, consistency, accountability, efficiency, and clarity on how the school operates;
- provides a roadmap for day-to-day operations;
- ensures compliance with laws and regulations, gives guidance for decision-making, and streamlining internal processes;
- is designed to influence and determine all major decisions, actions and all activities taking place within the boundaries set by them;
- stems from the school's vision and objectives which are formed in strategic management meetings