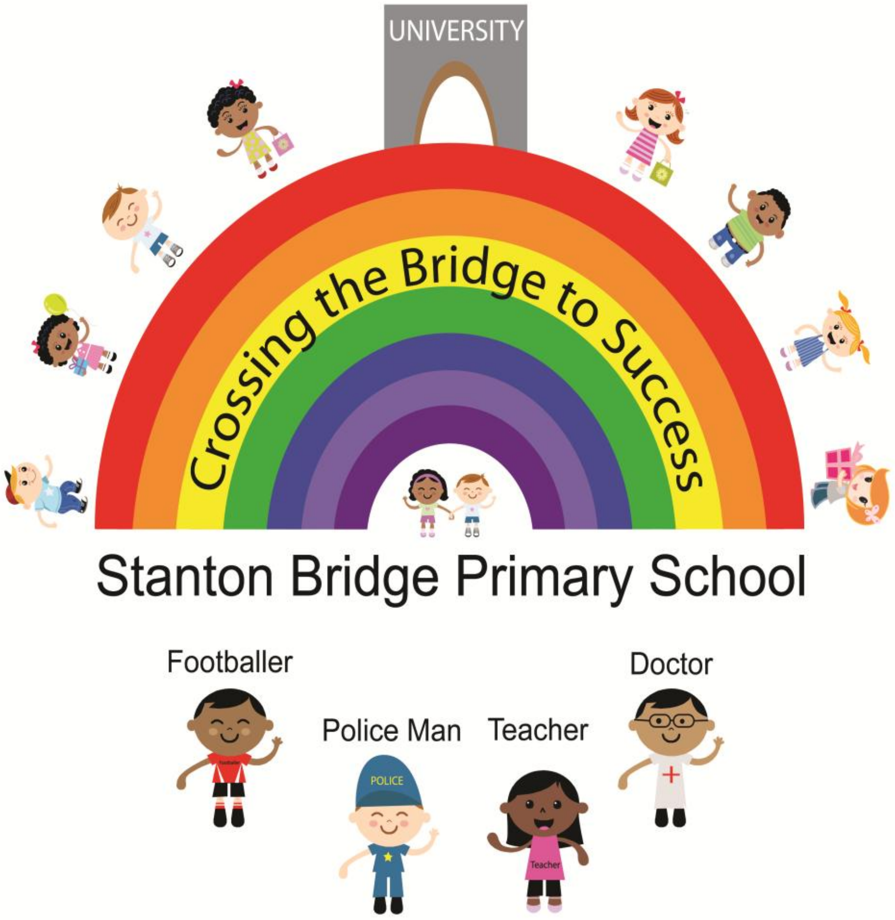

Cyber Security Policy

Stanton Bridge Primary School

Adopted: April 2025

Cyber Security Policy

Stanton Bridge Primary School recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our **Behaviour Policy.**

Purpose and Scope

The purpose of this document is to establish systems and controls to protect the School from cyber criminals and associated cyber security risks, as well as to set out an action plan should the School fall victim to cyber-crime.

This policy is relevant to all staff and anyone else that may use school IT system sucah s Governors or Visitors.

What is Cyber-Crime?

any criminal activity that utilizes computers, networks, or digital devices, including hacking, phishing, identity theft, ransomware, viruses, phishing, malware and data breaches.

Rise in school cybercrime attacks sparks NCA education drive

Reference: https://www.nationalcrimeagency.gov.uk/news/rise-in-school-cyber-crime-attacks-sparks-nca-education-drive

Data from the National Crime Agency's National Cyber Crime Unit (NCCU) shows there was a 107 per cent increase in reports from the police cyber prevent network of students as young as nine deploying DDoS (distributed denial of service) attacks from 2019 to 2020.

Types of Cybercrime or Cyberattack

Understanding the most common types of cybercrime is key to fighting it, the most prevalent ones:

- **Fishing Scams:** it is one of the most common types of cyberattack, these scams involve fake emails or messages designed to trick victims into giving up personal or corporate information.
- **Identity theft:** it's when cybercriminals get your personal information such as transactional data to make unauthorised transactions or enable other fraudulent activities.
- **Ransomware attacks:** they are a type of malicious software that exploit computer networks to encrypt victims' files and block access until a ransom is paid. *This type of cybercrime can lead to data breaches* where victims pay the

ransom to get access back to their files or systems.it is usually distributed through phishing emails or drive-by downloading. Once inside a computer system, the malicious software spreads its arms, encrypts files, and demands a ransom, often in the form of cryptocurrency, in exchange for the decryption key.

- **Distributed Denial of Service (DDOS) Attacks**: they are severe cyberattacks where a multitude of compromised systems flood a single target with excessive traffic, effectively causing a service outage for regular users. These incidents utilize vast networks of hijacked computers.

Cybercrime can lead to a wide range of consequences:

- ❖ Financial losses
- ❖ Reputational damage
- ❖ Data breaches
- ❖ Identity theft
- ❖ Loss of life in extreme cases
- ❖ Impacting individuals, businesses, and society as a whole.

The following consequences of cyber-crime which could affect:

Financial Loss:

It can lead to direct financial losses, such as stolen money from credit cards or bank accounts, the global cost of all forms of online crime is estimated to be in excess of £300 billion. Therefore, we have to protect our data, otherwise, we may be fined up to £17.5 million or 4% of the total worldwide annual turnover if we fail to protect our data. Cyberattacks can result in direct financial losses:

- Lost revenue due to downtime
- Cost of implementing new security measures
- Cost of recovery from a data breach

Data Protection and Privacy:

Confidential information and all forms of personal data should be kept secured from unauthorised access and misuse, it is considered one of the most essential requirements for our school.

Identity Theft:

Data protection focuses on safeguarding personal information from cyberattack because criminals can steal personal information to open fraudulent accounts, make unauthorised purchases.

Reputational Damage:

A cyber security incident can have a major impact on our school reputation, particularly if it involves:

- The loss of confidential information
- Personal data
- Reported in the media

Data or Privacy Breaches:

Cybercriminals can steal and gain access to sensitive personal information for students or staff, leading to privacy violations and potential embarrassment or harm.

Disruption of School Operations:

Cyberattacks can disrupt our school operations, leading to downtime, lost productivity, and reduced efficiency.

Legal and Regulatory Consequences:

School has various regulatory duties which we could unintentionally breach through falling victim to cyberattacks (loss of personal data), can lead to legal and regulatory penalties, such as fines from the Information Commissioners Office (ICO) or claims for damages by the individuals concerned.

Increased Security Costs:

Schools may need to invest in additional security measures to protect against cyberattacks, leading to increased costs.

Cloud Security Challenges:

Schools that rely on cloud services are vulnerable to cyberattacks that target cloud infrastructure, leading to data breaches.

Cyber-Attack Prevention Methodology

To prevent cyberattack in our school, we focus on cybersecurity training for staff and students, implementing strong digital safeguards, and staying informed about emerging threats.

Essential Guidance to help protect our school data and systems

The DfE Cyber Security Standards

it aims to protect school's sensitive data from threats and ensure we are prepared, meeting legal requirements, and reduce the risk of cyber-attacks.

Key areas in these standards:

- **Security controls**: it includes anything specifically designed to prevent any attacks on school's sensitive information, students and staff data, therefore, schools should have basic security measures like firewalls, strong passwords, cloud security, incident response plans and antivirus software to keep hackers out.

- **Governance:** Governance integrates with school's operations and prevents the interruption of activities due to cyber threats or attacks. Features of cybersecurity governance include:

  - Regular policy reviews and risk assessment
  - Decision-making hierarchies
  - Defined risks related to business objectives
  - Mitigation plans and strategies
  - Oversight processes and procedures

- **Data protection:** Schools must have strict rules in place to control who can access student and staff information.

- **Patching and updates**: Keeping your software up to date is crucial. Regular patches and updates fix known vulnerabilities and help prevent attacks.

- **Incident management plan**: Schools need to be prepared in case something goes wrong and set a plan that will help school to react quickly to minimise damage from cyberattack or breach, such as:

  - School should have structured approach to detect and identify any cyberattack
  - Prioritize it
  - Categorize and analyse cyberattack to include investigating the breach, which cover:
    - Confirming what happened
    - What data has been affected
    - Data was protected or not and sensitivity of the data should be confirmed
    - Consequences of the attack identified.

- Notification: need to decide whether the cyberattack needs to be reported to regulators such as ICO and National Crime Agency and/or colleagues or parents.
- Evaluation & Respond to containment and recovering from security incidents, by recover any data lost and consider any improvements that can be made to minimizing damage.
- Incident closure

Stanton Bridge Primary School Technology Solutions

Governors

Governors are responsible for the approval of the online safety policy, which is part of Cyber Security Policy and for reviewing the effectiveness of the policy by reviewing e-safety incidents and monitoring reports. Online safety falls within the remit of the governor responsible for Safeguarding. The role of the online safety governor will include:

- Ensure an online safety policy is in place, reviewed every year and is available to all stakeholders
- Ensure that there is an online safety leader who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive.
- Ensure that procedures for the safe use of ICT and the Internet are in place and adhered to
- Hold the headteacher and staff accountable for online safety.

Headteacher and SLT

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online safety leader. Any complaint about staff misuse must be referred to the online safety leader at the school or, in the case of a serious complaint, to the headteacher.

- Ensure access to induction and training in online safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SLT.
- Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured.
- Work in partnership with the DFE and the Internet Service Provider and school Technician and Computer Manager to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- The Senior Leadership Team will receive monitoring reports from the online safety manager and IT Technician.

Online safety coordinator:

- Leads Online Safety meetings.
- Work in partnership with the DFE and the Internet Service Provider and school IT Technician to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of e-safety incidents and creates a log of incidents to inform future online safety developments with the IT Technician.

- Reports to Senior Leadership Team.
- Liaise with the nominated member of the governing body & headteacher to provide an annual report on online safety.

The School have put in place a number of systems and controls to mitigate the risk of falling victim to cyberattack. These include technology solutions as well as controls and guidance for staff.

Controls and Guidance for Staff & Students

Even with the best technical protections in place, staff and students need to be aware of the tactics cyber criminals use to target schools, therefore, staff training is very important to prevent human error remains one of the biggest risks to cybersecurity in schools.

Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHCEE lessons where personal safety, responsibility, and/or development are being discussed.

Cybersecurity Training for Staff and Students:

Provide regular training for all staff and students on recognizing phishing attempts, secure their email accounts.

Cyber Awareness Culture:

Embed cybersecurity awareness into the school culture, making it a daily practice rather than a one-time event, starting with basic online safety principles for students.

Guidance for Parent

Encourage parents to be involved in their children's online safety, providing them with resources and guidance, which is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish.

Online Safety Policy Link:
chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.stantonbridge.coventry.sch.uk/ckfinder/userfiles/files/Policies/Online-Safety-Policy.pdf

Technology Solutions

The School have implemented the following technical measures to protect against cyber-crime:

❖ School Email Accounts using Microsoft Office 365 - PASSWORD

Email attacks in cybersecurity involve malicious activities using email as a primary vector to compromise systems, steal data, or disrupt activities, with phishing being a common tactic.

The school uses email (Microsoft Office 365) internally for staff and is an essential part of school communication, it is also used to enhance the curriculum by:

- Initiating contact and projects with other schools nationally and internationally
- Providing immediate feedback on work, and requests for support where it is needed.
- The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

Microsoft Office 365 Password Policy

At least 8 number of characters that a password for a user account should contain

Passwords may not contain the user's samAccountName (Account Name) value or entire displayName (Full Name value).

Passwords must meet the following minimum complexity requirements:

The password contains characters from three of the following categories

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters (special characters): (~!@#$%^&*_-+=|\(){}[]:;"'<>,.?/) Currency symbols such as the Euro or British Pound are not counted as special characters for this policy setting.
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
- Complexity requirements are enforced when passwords are changed or created.

Password Expiry Rules:

- Password expire after 90 days
- User receive notification 14days prior password expire date of 90 days

for Staff

School has set password policy is a set of rules designed to enhance computer security by encouraging staff to employ strong passwords and use them properly. staff have been made aware of the following when using email in school:

- You Should Not Share Your Passwords.
- Staff should ONLY use official school-provided email accounts to communicate with parents or carers.
- To contact other professionals for work purposes, this is important for confidentiality.
- Personal email should not be accessed during school hours or share with parents or carers.
- Staff must tell the Computing lead or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- keep passwords secret.
- never reuse a password.
- never allow any other person to access the school's systems using your login details.
- not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or the School IT systems.
- only access work systems using computers or phones that the School owns.
- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using School computer, iPad or phone.
- not install software onto your School computer. All software requests should be made to Miss Amani.
- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to Mrs. Emma Good as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our Data Breach Policy.

Multi-Factor Authentication (MFA):

School has added MFA to staff emails as an extra layer of security by requiring more than just a password, a user would log in with their password and then complete a second verification step. This second factor could be:

- o A code sent to a mobile device (via SMS or an authentication app like Google Authenticator or Microsoft Authenticator).

for Students

Pupils will be educated through the computing curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

School Computer Account for Staff and Students

School has implemented policies for creating strong, unique passwords and restrict access to sensitive data and systems based on roles and responsibilities.

❖ Regular Software Updates:

ICT Support team always ensure all software and operating systems are kept up-to-date with the latest security patches and updates. Deleting or disabling unused/unnecessary software.

❖ Antivirus Software Trellix

Our school use Trellix Endpoint Security antivirus software, it is an endpoint protection platform (EPP) that provides multi-layered endpoint protection, including antivirus, firewall, and exploit prevention, and uses machine learning for threat detection and response. It is designed to protect data and stop advanced threats across on-prem, cloud, and disconnected environments.

Benefits:

- Improved Threat Detection: Machine learning and advanced threat detection capabilities help identify and respond to even the most sophisticated threats.
- Enhanced Security Posture: The multi-layered approach and proactive security measures strengthen school's overall security posture.
- Simplified Management: Centralized management and automation streamline security operations, making it easier for security teams to manage and respond to threats.
- Increased Efficiency: The platform's efficiency and effectiveness allow security teams to resolve threats faster with fewer resources.
- Peace of Mind: Trellix Endpoint Security provides peace of mind by protecting users, increasing productivity, and creating a secure computing environment.

❖ Firewalls Software:

A firewall helps monitor traffic and block suspicious activity.
Coventry City Council's ICT & Digital Service manages the firewall for our school, including the Smoothwall web filtering service, and offers both filtered and unfiltered internet access options.

❖ Web Filtering:

The Smoothwall web filtering service is used across local authorities and is set up based on BECTA recommendations, as well as considering existing filtering options within schools.

- **Stanton Bridge Primary School's internet filtering controlled by Coventry City Council**
  - Teachers: controlled via Coventry Proxy Covlea (Address: proxy.covlea.net – Port: 8080)
  - Students: controlled via Coventry Proxy Covlea, (Address: proxy.covlea.net – Port: 8080)
  - Both teachers and students group membership are controlled through Domain Controllers: SVR-SBP-DC01 (10.253.216.32) & SVR-SBP-DC02 (10.253.216.33) Active Directory.

- **Requests for Blocking/Unblocking:**

  Requests to block or unblock websites can only be made to ICT Service Desk via the usual route for raising issues. To raise a Service request. Email schoolsictrequest@coventry.gov.uk.

- **Making use of ICT and the Internet in school**

  The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.
  School monitoring system used to supplement the filtering system

- **Learning to Evaluate Internet Content**

  With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught to:

  - Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
  - Use age-appropriate tools to search for information online
  - Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

  The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the school's IT Technician and then the online safety manager. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

❖ Education Protect by Impero

Stanton Bridge uses Impero Education Pro filtering system, it is an online safety software is compliant with the UK Safer Internet Centre's `appropriate monitoring' provider checklist. Also it protects students with state-of-the-art online safety technology, in line with Ofsted and ISI. Designed in response to UK Government requirements, such as the Prevent duty and the Department for Education's Keeping Children Safe in Education guidance (KCSiE), Impero Education Pro's state-of-the-art safeguarding software helps schools to fulfil their legal duty of care around internet safety and safeguarding. This best practice approach to safeguarding in schools, including active monitoring and logging incident captures to provide contextual insight, helps schools to identify potential risk, respond before an incident escalates, and educate students about responsible internet behaviour. The school has provided enhanced user-level filtering through the use of the Impero filtering programme. In reality, there is no filtering system can guarantee 100% protection against access to unsuitable sites. Therefore, Stanton Bridge Primary School use Impero software to monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement.

❖ Computing subject leader / Technical Staff:

The Computing Subject leader is responsible for ensuring:

- That the schools technical infrastructure is secure and is not open to misuse or malicious attack.

- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the headteacher; online safety coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies.

❖ Staff and Students User Account Folder (School Network)

- Staff and students account folders are existing in FS01, deleting unnecessary user folder.
- Staff and students accounts are created in DC01, deleting or disabling unused/unnecessary user accounts.

❖ Data encryption

Regularly back up important data to prevent loss in case of a cyber incident.
Data encryption is a security method that transforms data into an unreadable format (ciphertext) using a secret key, allowing only authorized users with the key to decrypt and access the original information (plaintext).

- **Host Virtual Server Back**

  - Secure data backup
  - Encryption 3 external hard drives using BitLocker, it can't be read by anyone without the proper password.
  - using strong passwords; and disabling auto-run features.

- **Encrypt Email Attachments**

  School use software like 7-Zip or WinZip to compress and encrypt a file, then attach the encrypted file to your email.
  Password will be sent in a separate email because it is a security practice to reduce the risk of an attacker obtaining both the password and the associated information (like a link or file) at once, making it harder for them to access sensitive data.

- **Hold School Data Online**

  Most cloud providers like Microsoft do offer encryption services for data stored in their systems.

❖ Backup and Recovery Solutions

We have regular backups of our Virtual Servers. Which include both on-site and cloud data.
If a ransomware attack hits, having a backup means we won't lose important information. Plus, it helps us get back up and running quickly.

- **External Hard Drive Backup**

  Host server should be backed up regularly to 3 external hard drive:

- **Cloud Backup**
  School use Safe Data Storage online cloud to backup the following virtual hosts:

- App
- FS01
- FS02
- Admin Server

Back up the following Virtual Servers on the Curriculum Server

Server	Folders Backup
SVR-SBP-FS01	o Staff o Students
SVR-SBP-FS02	o Club o Hall o Pupils o Resources o SLT o Staff o Tech o Visitor
SVR-SBP-APP	o Install Point o Shared Software o Network Programs

❖ Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online.

Pupils are not allowed to access social media sites in school, there are various restrictions through the web filtering on the use of these sites in school that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the computing curriculum and PSHCEE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Teachers will use a safe search engine such as Primary School ICT (http://primaryschoolict.com)
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

For more information on the school's Cyber Security Policy contact Mrs. Emma Good.

Signed by

__________________________ **Chair of Trustees** **Date**: ....

__________________________ **Headteacher** **Date**: ....

This policy will be reviewed annually