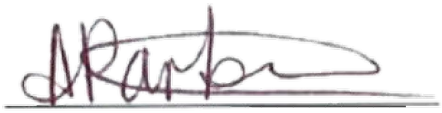
Cyber Security Policy

Version 1

Policy confirmed by the Governing Body of Grace Mary Primary School on:

Date: 3rd December 2025

Signature: 

(Chair of Governors)

Signature: 

(Head Teacher)

Intent

Grace Mary Primary School's Cyber Security Policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. The more we rely on technology to collect, store and manage information, the more vulnerable we become, to severe security breaches. Human errors, hacker attacks, and system malfunctions could cause great financial damage and may jeopardise our school's reputation. For this reason, we have implemented several security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy and also refer all employees to other school policies.

Scope

This policy applies to all our employees, contractors, volunteers, and anyone who has permanent or temporary access to our systems and hardware.

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Information concerning staff, students, parents, and governors.
- Unpublished financial information and contractual data.

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches. Protect personal and schooldevices. When employees use their digital devices to access the school's emails or accounts, they introduce security risks to our data. We advise our employees to keep both their personal and school-issued devices secure.

They should do the following on school-issued devices and their personal devices if using these for work purposes:

- Keep all devices password protected (even if you only use your laptop for work, for example, this may be synched to your phone or tablet).
- Ensure antivirus software is kept up to date.
- Ensure they do not leave their devices exposed or unattended (if you leave the device unattended, at home or school, all devices need to be locked/put to sleep).
- Install security updates of browsers and systems regularly. This includes ensuring your school-issued device is restarted regularly to ensure updates from our IT provider (Network IT) are completed.
- Log into school accounts and systems through secure and private networks only (Wi-Fi and VPN networks included).

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new staff receive school-issued equipment they should review the school's Acceptable Use of ICT Policy, as it will contain key information relating to the safe and secure use of this equipment.

Keep emails safe
Emails often host phishing attacks, scams, or malicious software (e.g., trojans and worms.)

To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g., "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g., offering prizes, advice.)
- Check the email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or giveaways (e.g., grammar mistakes, capital letters, an excessive number of exclamation marks.)
- When accessing emails when not connected to the school WI-FI
- (such as at home, or on personal devices), staff have two-factor authentication set up.
- All emails that are used to conduct opr support GMPS business MUST be sent using @gracemary.sandwell.sch.uk address. Non work emails must not be used to conduct official business.

If an employee isn't sure that an email they received is safe, they should contact 'Network IT' Team and DO NOT open it if possible.

Manage passwords properly
Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret.

Passwords for emails and computer log-ins are set by 'Network IT' and include randomised letters and numbers, which cannot be easily guessed.

For this reason, we advise our employees to:

- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential.
- Not keep combinations of identifiable information together. For example, do not keep their email address and password together or

do not keep their passwords at the back of school lanyards.
- Exchange credentials only when necessary. When exchanging them in person is not possible, employees should use the phone instead of email, and only if they recognise the person they are talking to.
- Passwords for the computer log-ins, must be changed annually.

Transfer data securely
Transferring data introduces a security risk

Employees must:
- Avoid transferring sensitive data (e.g., pupil/family information, employee records) to other devices or accounts unless necessary. When a mass transfer of such data is needed, we request employees seek the support of Network IT for help.
- Share confidential data over the school's network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Report scams, privacy breaches, and hacking attempts. Our IT technicians, Network IT needs to know about scams, breaches, and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails, or phishing attempts as soon as possible to our specialists. Our IT technicians will investigate promptly, resolve the issue, and contact the school if necessary. We encourage our employees to reach out to them with any questions or concerns. (A ticket must be raised immediately not wait until they are on site and inform the Business Manager)

Additional MUST DO measures
To reduce the likelihood of security breaches, we also instruct our employees to:
- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to SIOBHAN OLIARNYK (Business Manager) and NETWORK IT. complete form (Appendix 2 & 3)
- Report a perceived threat or possible security weakness in school's systems
- Downloading of software is disabled on staff and pupil accounts without the use of an elevated user account which is entered by NETWORK IT.
- Avoid accessing suspicious websites. We also expect our employees to comply with our 'Acceptable Use of ICT' and associated policies.
- Log out of emails every time a session is finished.

- Not use apps on phones such as Mail or Outlook to access work emails UNLESS YOU HAVE HAD PERMISSION
- Install firewalls, anti-malware software, and access authentication systems.
- Investigate security breaches thoroughly.
- Follow this policy's provisions as other employees do.

As an additional measure, NETWORK IT have added a detector
This monitoring solution will help to detect and provide regular reports of any suspicious cyber activity targeting the school IP address and any attempts to access unauthorised websites. Any reports will be shared with the Headteacher by Network IT.

Remote working
When working remotely, staff must follow this policy's instructions as well.

Since they will be accessing our school's information and systems from a distance, they are obliged to follow all data encryption, protection standards, and settings, and ensure their private network is secure.

Response to cyber attack
If staff perceive a threat or possible security weakness/breach, they must contact Siobhan Oliarnyk and Network IT. Within our SLA with Network IT, we may raise concerns with them over the weekend if security had been compromised.
Network IT's solution to any incident would be:
1. Assess the impact of the incident – has it targeted servers, file shares as well as workstations and isolate them from the network.
2. Recover your server from the latest available backup.
3. Use the server/ bootable media to wipe and reinstall impacted workstations with a fresh installation of Windows and key applications.
4. Ensure users can log on to access their files and the internet.
5. Monitor the network activity for the next week to ensure the incident has been remediated.

5. Disciplinary Action - We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action. Deliberate and serious breaches of this policy may lead to the school taking disciplinary measures in accordance with the school's disciplinary policy and procedure (Appendix 1: misuse)

All the school's phone, web-based, locally hosted systems and email-related resources are provided for business purposes. Therefore, the school maintains the right to monitor all internet and local network

traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

However, see the Safeguarding section below.
Examples of deliberate or serious breaches of this policy and examples of misuse are, but are not limited to:

- Knowingly disclose login information to an unauthorised third party
- Inappropriate disclosure of personal data
- Knowingly installing software on school devices that hasn't been approved by Network IT or Headteacher which leads to a breach.
- Allowing the use of school devices by unauthorised third parties.
- Using school devices for anything other than work-related matters.
- Storing data on insecure media such as removable media that leads to a breach.

Everyone should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and data. We can all contribute to this by being vigilant and keeping cyber security at the top of our minds.

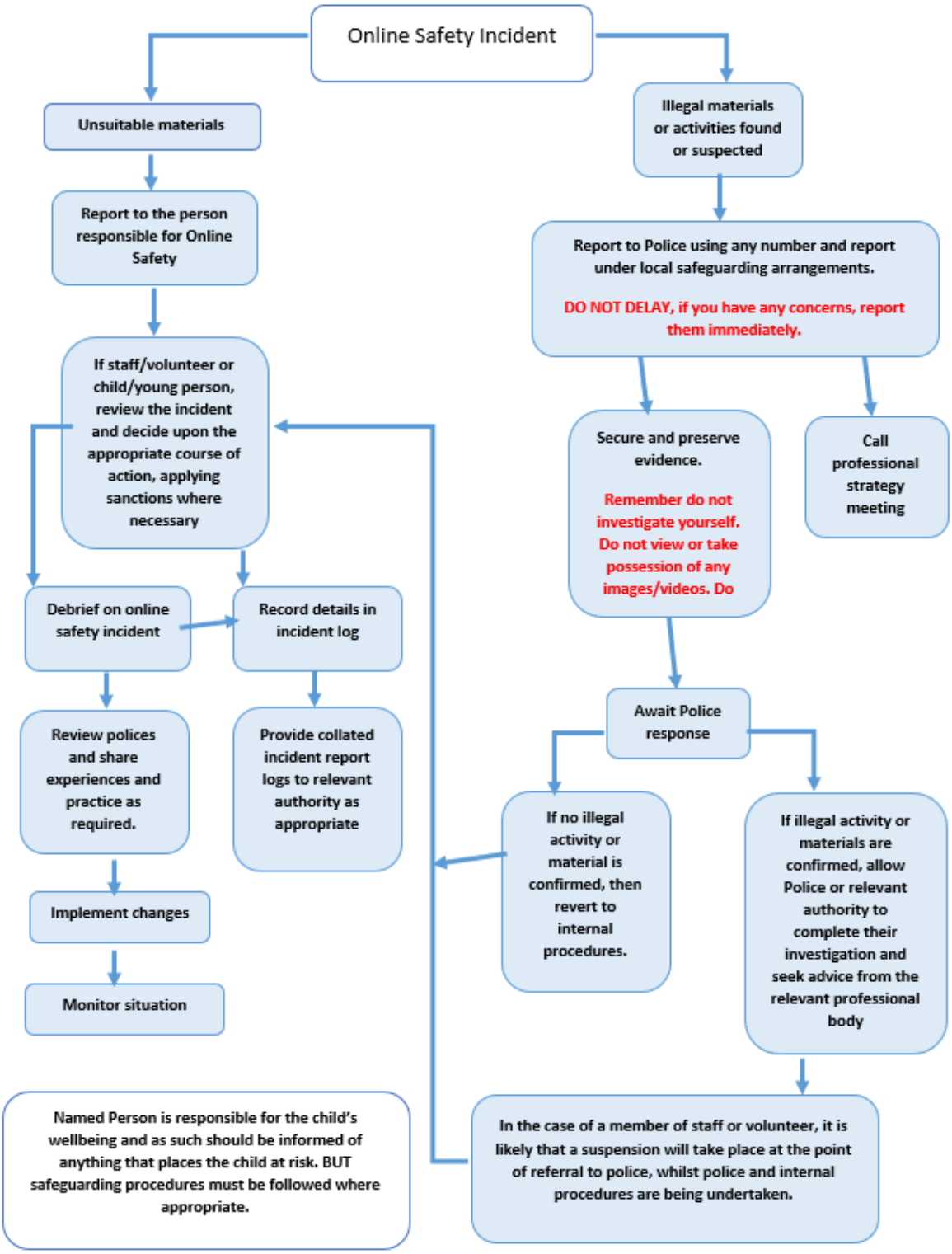
Safeguarding
Schools have a statutory duty to monitor their digital environment to identify any potential threats to pupils' welfare and well-being. We have appropriate filtering and monitoring in place which runs on all school-owned devices and is continuously monitored for safeguarding risks. If pupils and staff use a school-owned device outside of school, the device will continue to be monitored when it is both online and offline. If an incident arises,

Conclusion
Cyber security is a collective responsibility. By adhering to this policy, the school can protect its digital resources, maintain the integrity of personal data, and create a safe and secure environment conducive to learning and growth. Let us all commit to fostering a culture of vigilance and responsibility in our digital interactions.

Further Reading
- NSCS Cyber Essentials Framework - Cyber Essentials - NCSC.GOV.UK
- NCSC Cyber Security for schools - Cyber Security for Schools - NCSC.GOV.UK
- DfE Cyber Security Standards - Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK
- LGfL Elevate Cyber Security Toolkit - Elevate Cyber Security Toolkit | LGFL

Appendix 1

Responding to incidents of misuse – flow chart



Appendix 2

Record of reviewing devices/internet sites (responding to incidents of misuse)- to be attached as a file on CPOMs

Group: .....
Date: .....
Reason for investigation: .....

.....

.....

.....

Details of first reviewing person
Name: .....
Position: .....
Signature: .....

Details of second reviewing person
Name: .....
Position: .....
Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

`Appendix 3

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		