

	The Gregg Schools Trust Proprietor of The Gregg School	Document Owner: DSL
	E-Safety Policy	Updated: March 2026
Document Type: Regulatory Policy		
Reviewed and ratified by: Education and Safeguarding Committee		Date of Approval: 28 th April 2026
Review frequency: 1 year <i>(or as necessary in line with updates or incidents)</i>		Date of next Review: April 2027 <i>(or as necessary in line with updates or incidents)</i>

The Gregg Schools Trust ("The Trust") is the parent company of The Gregg Schools, and for the purposes of the Independent Schools Standards Regulations (ISSRs) is identified as the Proprietor.

From the date of this policy until 31st August 2026, the Trust operated two schools:

- The Gregg Preparatory School in Winn Road, Southampton - a co-educational day school and pre-school for 4 to 11 year olds.
- The Gregg School at Townhill Park House, Townhill Park, Southampton - a co-educational day school for 11 to 16 year olds. This school is situated in buildings and grounds owned by the Trust.

From 1st September 2026, the two schools will merge onto the Townhill Park House site and the Winn Road building will close. As such, a material change will take place.

The Gregg School ('the School') will become an all-through school, providing high quality education for students aged 4 to 16 years.

This policy and procedure is applicable to all members of staff at both schools through until 31 August 2026, and continues to be applicable to all staff at the all-through school from 01 September 2026.

1. Policy Statement

The requirements of this policy apply to all the groups referred to in the policy and listed below in respect of all ICT resources and equipment within the school, and those available to staff working remotely or at home.

Safeguarding is central to the work of the school. The school uses technology and the Internet extensively to enrich learning and school operations. Online safeguarding ("E-Safety") is a dynamic area; this policy sets out how we identify, assess and mitigate risks, empowering the whole school community to stay safe when using digital technology, on-site and off-site.

The policy applies to all users (staff, governors, volunteers, contractors, students and visitors) and covers all IT resources including devices, networks, software and online services (e.g. Firefly, Office 365/Teams, MIS, email, school websites, and social media). This combined policy also incorporates Acceptable Use Policies (AUP) and incident flowcharts as appendices and is reviewed at least annually or following significant incidents or DfE guidance updates.

Users - refers to staff, governors, adult work experience, apprentices and trainee teachers, school volunteers, students and any other person working in, or on behalf of, the school including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school (e.g. parent, guardian, carer).

School – any school business or activity conducted on or off the school site, (e.g. visits, conferences, school trips etc.)

Wider school community – students, all staff, governors, parents, volunteers.

For the purposes of this policy, IT resources and equipment include computer resources, use of school Internet access and email systems, software (including use of software such as Veracross, SIMS, Firefly and Office 365), school telephones and text systems, CCTV, cameras and recording equipment, school website, and any other electronic or communication equipment used in the course of the user's work.

Safeguarding is a serious matter. The school uses technology and the Internet extensively across all areas of the curriculum. Online safeguarding (which includes the prevention of on-line radicalisation of students) known as E-Safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an E-Safety incident, whichever is sooner.

The primary purpose of this policy is two-fold:

- i. To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- ii. To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for staff and parents to read on Firefly. Upon review, all members of staff will electronically sign to confirm they have read and understood both the E-Safety Policy and the Staff Acceptable Use Policy.

Senior school students will be directed to view the Students Acceptable Use Policy at the beginning of each school year via their planner.

Legal & Statutory Framework

This policy aligns with statutory guidance in Keeping Children Safe in Education (KCSIE) and related DfE advice, including the 2025 updates now in force, and references the Cyber Security Standards for Schools and Colleges, and DfE guidance on filtering/monitoring and safe use of generative AI. It sits alongside the Trust's Child Protection & Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, RSHE Policy, Data Protection/GDPR Policy and Staff Code of Conduct.

2. Roles & Responsibilities

2.1 The Gregg Schools Trust ('the Trust')

The Trust ensures:

- Effective policies, procedures and resources are in place;
- Reviews E-Safety at least annually and following incidents;
- Assures that filtering/monitoring standards and cyber security standards are met and that safeguarding leadership is effective.

2.2 Headteacher

The Headteacher holds overall responsibility for E-Safety. Day-to-day management is delegated to the E-Safety Officer and DSL. The DSL ensures appropriate training for all audiences (students, staff - including contractors, governors and parents), and that incidents are handled promptly and recorded.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned, up to date and appropriate to the recipient i.e. students, all staff (including contracted staff who work onsite), senior leadership team, governing body and parents
- The designated E-Safety Officer has had appropriate REGULAR CPD in order to undertake their day-to-day duties. External courses are recorded on CPD Genie; National Online Safety courses are recorded on their website tracking system.
- All E-Safety incidents are dealt with promptly and appropriately according to the requirements of this policy.

2.3 E-Safety Officer

The day-to-day duty of the E-Safety Officer is devolved to the Head of Computing supported by the DSL.

The above will:

- Keep up to date with the latest risks to children whilst using technology and familiarise him/herself with the latest research and available resources for school and home use;
- Review this policy regularly and bring any matters to the attention of the Headteacher;

- Advise the Headteacher and governors of all E-Safety matters;
- Engage with parents and the school community on E-Safety matters at school and/or at home;
- Liaise with other agencies as required;
- Retain a log of E-Safety incidents on the Management Information System (MIS) and the Monitoring Overview document (Staff Share > Pastoral);
- Ensure any technical E-Safety measures in school (e.g. Internet filtering software and behaviour management software) are fit for purpose;
- Make him/herself aware of any reporting function with technical E-Safety measures (i.e. internet filtering reporting function; Classroom Cloud tool violation log viewer by student and date/time) and liaise with the Headteacher/DSL/Governors to decide on what reports may be appropriate for viewing.

2.4 Managed Service

Infinity Education and onsite IT Manager, under the direction of the Head of Facilities, are responsible for ensuring that the IT technical infrastructure across the school is secure. This will include at a minimum:

- Anti-virus is fit-for-purpose, up-to-date and applied to all capable devices
- Windows updates are regularly monitored and devices updated as appropriate
- Any E-Safety technical solutions such as Internet filtering are operating correctly
- Filtering levels are applied appropriately and are appropriate for the age of all users, and that categories of use are discussed and agreed with the E-Safety Officer and Headteacher
- Passwords are applied correctly to all users regardless of age

2.5 All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the E-Safety Officer.
- The boundaries for use of ICT equipment and services in school, and/or personal equipment, are given in the Staff Acceptable Use Policy. Any deviation or misuse of ICT equipment or services will be reported to the Headteacher.
- Any E-Safety incident is reported to the appropriate E-Safety Officer or DSL, who logs the incident, or in his/her absence to the Headteacher.
- The reporting flowcharts contained within this E-Safety policy (Appendices 6 and 7) are fully understood.
- USB Storage Devices are banned for all users unless agreed under special circumstances with the IT Manager and E-Safety Officer.

2.6 All Students

The boundaries for use of ICT equipment and services in the school, and/or personal equipment, are given in the Student Acceptable Use Policy (AUP). Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Trust's Behaviour and Discipline Policy.

E-Safety is embedded into the curriculum. Students will be given the appropriate advice and guidance by staff and will be made aware how they can report areas of concern whilst at school or outside of school.

2.7 Parents and Carers

Parents play the most important role in the development of their children. Therefore, as far as possible, the school will ensure that parents have the skills and knowledge they need to ensure the safety of students outside the school environment. Through parents' evenings, school newsletters, safeguarding evenings and via our websites and social media accounts, the school will keep parents up to date with new and emerging E-Safety risks and will involve parents in strategies to ensure that students are empowered.

Parents are informed of their responsibilities on FIREFLY.

3. Technology

The school uses a range of devices including PC's, laptops and tablets. In order to safeguard students, and to prevent loss of personal data, we employ the following assistive technology.

Use of Artificial Intelligence (AI) Tools

Staff and students must follow Trust guidance on safe, ethical use of AI (e.g. generative tools). AI systems must be filtered/monitored where feasible, and never used to process sensitive personal data or to generate/propagate harmful content. Curriculum use must include discussion of AI reliability, bias and safety. Any AI service trials require risk assessment and approval by the E-Safety Officer/Headteacher.

3.1 Internet Filtering and Monitoring

The school uses Smoothwall software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites during school time. What is appropriate and inappropriate will be determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. Using the Classroom Cloud software, sensitive violation criteria have been imposed to log any inappropriate key word searched or websites. The E-Safety Officer and DSL are responsible for ensuring that filtering is appropriate and that any issues are brought to the attention of the Headteacher.

3.2 Encryption

All devices operated through the school that hold personal data are to be encrypted. No data as specified by the regulations is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach is to be brought to the attention of the Headteacher immediately. The Headteacher will take advice to ascertain whether a report needs to be made to the Information Commissioner's Office.

3.3 Passwords and Two Factor Authentication

All staff and students will be unable to access any device without a unique username and password. Students and staff are given training on security of their passwords. Every effort should be made by Staff to ensure their password remains secret and that it complies with the school parameters, meaning it contains at least eight characters, to include one uppercase letter, one lowercase letter, one number and one symbol.

Any school device that is used outside of the school network will require two factor authentication to sign in. This may be using a secondary email address, a mobile number or the Microsoft Authenticator app. This covers all of the school's IT systems including email and VPN.

3.4 Anti-Virus

All capable devices will have anti-virus software. This software will be updated regularly for new virus definitions. The E-Safety Officer working with the Managed Service will be responsible for ensuring this task is carried out and will report to the Headteacher if there are any concerns.

3.5 Mobile Phones *(See Appendix 9 also – Mobile Phone policy)*

Staff

Senior school

Personal mobile phones are not restricted, but should not be used for non-school related communication whilst supervising students unless part of your employment or in the case of an urgent or emergency situation. You are advised not to share your personal phone numbers when making contact with parents.

Prep school

Personal mobile phone use is restricted to non-contact time. Visitors are not permitted to use their mobile phones in front of children.

Use of personal mobile phone cameras to record pictures of the children on trips or undertaking learning activities is permitted, but photographs taken must be downloaded to the staff share or the cloud within twenty-four hours and deleted from personal phones.

Students

Senior school

Where a student does bring their phone to school, it should not be switched on during the school day and should be stored in their school bag.

Prep school

The school does not encourage children to bring mobile phones to school. The only exceptions are those students who travel via school minibus. Where a child does bring their phone to school, it is handed in to the office and is not switched on during the school day. The school cannot be held responsible for it.

3.6 Bring Your Own Device – BYOD

Senior school

Students are strongly encouraged to bring their own device to school to support their learning. However, a student does not have the right to use his or her own laptop, mobile phone or other electronic device unless they have a teacher's permission and/or the device has school monitoring and security software installed on it. Devices are not insured by the school or able to be repaired. BYOD must not be used for cheating.

Prep school

The use of children's own technology to provide educational material is only permitted when directed by a teacher.

For purposes of BYOD, "device" means privately owned wireless and/or portable electronic hand-held equipment that includes, but is not limited to, existing and emerging mobile communication systems and smart technologies, portable internet devices, Smart Phones,

hand held entertainment systems or portable information technology systems that can be used for word processing, image capture/recording, sound recording and information transmitting/receiving/storing etc.

Students and parents/guardians using any BYOD technology must adhere to this policy and, for senior school the Student AUP.

BYOD devices must not be used to cheat on assignments or tests, or for non-instructional purposes (such as making personal phone calls and text/instant messaging).

BYOD devices must not be used to record, transmit or post photographic images or video of a person, or persons on site during school activities and/or hours including whilst travelling on school minibuses, unless specifically instructed to by a member of staff and with the permission of the people involved.

BYOD devices may only be used to access the school secure environment during the school day.

3.7 Cloud Storage

Student cloud drives are monitored by the E-Safety Officer. Staff must not upload personal data to school cloud areas unless for legitimate school purposes and in line with GDPR.

4. Safe Use

4.1 Security

During lesson time, staff should ensure that teacher machines in classrooms are screen locked if they are left unattended for any period, especially when leaving a room. Any concerns about the security of the school's ICT systems should be raised immediately with the appropriate E-Safety Officer using Mantis or directly to the Managed Service.

4.2 Confidentiality

Staff must ensure that their use of the school's IT facilities is in accordance with GDPR 2018. This is particularly important when using data off site. Electronic data must only be accessed remotely through the school's Virtual Private Network (VPN). This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with. Care should be taken when sending information, that sensitive data is not included unless necessary.

4.3 Internet

Use of the Internet in school by students is encouraged where it is part of the curriculum. Internet use is granted to staff on the understanding that they have read this policy and the AUP.

All internet activity is subject to monitoring. You must not access, or attempt to access, any sites that may contain the following: child abuse, pornography, those that promote racial or religious hatred, promotion of illegal acts or any other information which may be illegal or

offensive to colleagues. Inadvertent access should be reported to the E-Safety Officer, who will log and deal with the incident.

4.4 Email

All staff will be provided with a school email address to enable them to perform their role effectively, and should be used to communicate with parents and students for any school related commitments. Staff are able to access email outside of school hours from mobile or fixed devices, and this email facility can be used to undertake school business outside of normal office hours. All staff are reminded that emails are subject to Freedom of Information requests. School email addresses should not be used for emails of a personal nature. Similarly use of personal email addresses for work purposes is not permitted.

Senior school

Students are permitted to use the school email system, and as such will be given their own email address. The email address will be prefixed by their cohort year of entry followed by the first 5 characters of their surname, then their first initial e.g. 15SmithT@thegreggschools.org. Students are given lessons about safe and sensible internet use.

Prep school

Students are given their own email address in order to access Google Classroom and Teams. They are not permitted to use the school email system for any other purpose unless directed to by a teacher. The email address will be prefixed by their cohort year of entry followed by their initials. Students are given lessons about safe and sensible internet use.

4.5 Photos and videos

The school provides digital cameras and other recording equipment for educational and school business use. When used off of the school site it is the responsibility of the member of staff to ensure that the equipment is kept secure and safe.

Wherever possible, the school prefers that staff use a school device for taking images of students. However, where this is not possible, staff may use their personal mobile phone for taking photos of students during school activities. It is the member of staff's responsibility to ensure that these are uploaded to the school system and deleted from their phone within 24 hours.

As part of the admission process for any student, their parents are given the opportunity to state that they do not give consent for images of their child to be taken/used by the school.

Senior school

At the senior school, parents' consent via an electronic reply slip which can be found in the New Starter paperwork found on Firefly.

Students also have the right to "opt-out" themselves when they reach the age of 13 via the GDPR Image consent form (to be found on Firefly).

Prep school

In the prep school, parents' consent via an Essential Information Form.

The list of children who have "opted-out" must be consulted before any image or video of any child is used publicly, particularly in newsletters or social media.

4.6 Social Networking and Media Sharing

There are many social networking services available and the school is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within the school and have been appropriately risk assessed. Should staff wish to use other social media, permission must first be sought via the relevant E-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Twitter – used by the school as a broadcast service (see below).
- Facebook – used by the school as a broadcast service (see below).
- Instagram - used by the school as a broadcast service (see below).
- YouTube - used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. **No persons will be “followed” or “friended”** on these services and as such no two-way communication will take place.

Staff using social networking for personal use should never undermine the school, its staff, the students or their parents.

In addition, the following is to be strictly adhered to:

- The list of students whose parents have “opted-out” (see 4.5) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are “comment enabled”, comments are to be set to “moderated”.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a license which allows for such use (i.e. creative commons).

4.7 Notice and take down policy

Should it come to the attention of the school that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

4.8 Incidents

Any E-Safety incident is to be brought to the immediate attention of the relevant E-Safety Officer or DSL, or in his/her absence the Headteacher. The E-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Any malware or suspected malware must be reported immediately to the relevant E-Safety Officer who will follow the Malware Incident Response Plan (Appendix 8).

4.9 Unacceptable use

School systems and resources must not be used under any circumstances for the following purposes:

- To communicate to anyone who is not authorised to receive information that is confidential to the school
- To deliberately present personal views or opinions as those of the school
- To knowingly access, view, download, post, e-mail or otherwise transmit pornography or sexually suggestive or harassing materials or messages
- To knowingly access, view, download, post, e-mail or otherwise transmit materials or messages that promote extreme religious beliefs
- To knowingly access, view, download, post, e-mail or otherwise transmit materials or messages that can be classed as discriminatory or that may cause offense
- To access, view, download, post, e-mail or otherwise transmit material that contains viruses
- To use the school's facilities to undertake gambling, trading or any other action for personal gain or political purposes
- To undertake any activity which has negative implications for the safeguarding of young people
- To undertake an activity that is for paid work or otherwise for third parties (for example, exam marking, private tutoring, etc) without the consent of the headteacher.

Any of the above activities (but not limited to) are likely to be regarded as gross misconduct, which may after proper investigation lead to dismissal.

4.10 Training and Curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology. This includes updated awareness of new and emerging issues. To support this, the school will have an annual program of training which is suitable to the audience (see Appendix 10).

E-Safety for students is embedded into the curriculum. Whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and potential risks as part of the student's learning.

As well as the program of training we will establish further training or lessons as necessary in response to any incidents.

The relevant E-Safety Officer is responsible for recommending a program of training and awareness for the school year to the Headteacher for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

4.11 Cyber Bullying

Cyberbullying includes things such as sending nasty text messages or emails, or setting up a hate group on a social networking site. The bullying may also happen 24/7 and the victim is often targeted when they are not at school.

What we do:

- Staff will be made aware of the reporting mechanisms on different sites and services so that they can support students who want to make a report.

- We will ensure that all staff understand that incidents of, or concerns about, cyber bullying should be reported to the E-safety Officer, the Designated Safeguarding Lead and the appropriate Head(s) of Year.
- Through our curriculum and assembly programmes, we will be proactive in discussing cyberbullying with students; how it occurs, why it occurs, and the consequences of such behaviour.
- Incidents of cyberbullying will be investigated and managed with reference to the Trust's Anti Bullying and Behaviour and Discipline Policies.

What advice we give to students:

Through our curriculum, the Respect program and assembly program we will encourage students to respect their friends' and peers' thoughts and feelings online, and to recognise that what is considered morally right and wrong offline must also be thought of in the same way online.

Students will be taught to:

- **Not reply** to cyber bullying (most bullying seeks a reaction from the victim)
- **Save the evidence** of any messages or similar they receive to show when making a report
- **Tell a trusted adult** as soon as possible if they or a peer are being bullied to minimise their own upset or worry.

Attendance & Absence Risks

Being absent or missing from education can indicate safeguarding risks including sexual/criminal exploitation and online harm. Monitoring and early help processes consider attendance patterns alongside online-safety concerns.

Monitoring, Audit & Review

The E-Safety Officer conducts regular audits of filtering/monitoring logs, incident records and training compliance; reports findings to SLT/Governors; and ensures actions are implemented. The school completes the DfE technology self-assessment annually, and Governors review this policy at least yearly or after incidents.

Policy Communication & Availability

This policy is published on Firefly and the school website for staff, students and parents, and signposted via induction and annual updates. Staff confirm they have read and understood the policy and AUPs.

Related Policies

Child Protection & Safeguarding Policy; Behaviour Policy; Anti-Bullying Policy; RSHE Policy; Data Protection/GDPR Policy; Staff Code of Conduct; Attendance Policy; Alternative Provision Guidance; Safer Recruitment Policy.

Appendix 1 – Staff Acceptable Use Policy

The Staff AUP is shared electronically on Firefly and signed electronically on there.

The Gregg Schools Trust Staff Acceptable Use Policy (AUP)

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the E-Safety Policy. Once you have read and understood both you must sign the policy signature sheet. If you refuse to sign this declaration, it is still expected that you operate in accordance with the policy.

Supervision of students using IT equipment – If staff require students to use IT equipment in their lessons, staff must have the teacher console for the monitoring software running on their teaching machine, to monitor them. For any devices that do not have the monitoring software installed on them, staff are expected to be vigilant as they supervise students.

Internet Access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues; any paid work for an organisation other than the school. Inadvertent access must be treated as an E-Safety incident and reported to the E-Safety officer.

Social networking – Is allowed in school in accordance with the E-Safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become “friends” with parents or students on personal social networks.

Use of Email – Staff are required not to use school email addresses for personal messages. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act. As per Internet Access, emails should not contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an E-Safety incident and reported to the E-Safety officer.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – In order to access sensitive data from outside of school, staff should use the VPN and not personal data storage devices.

Personal Use of School ICT including Cloud Storage - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use. You must not upload any personal data to the cloud storage areas.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - Use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by the E-Safety Officer.

Viruses and other malware - Any virus outbreaks are to be reported to the managed service company and E-Safety Officer as soon as it is practical to do so, along with the name of the virus (if known). The school will refer this to the managed service provider.

E-Safety – is the responsibility of everyone to everyone. As such you will promote positive E-Safety messages in all use of ICT whether you are with other members of staff or with students.

Appendix 2 – Senior School Student Acceptable Use Policy

The Senior school Student AUP is shared with students in their planner.

Use of Equipment:

School Device

- I will not install programs onto school equipment.
- I will take care to look after all computing equipment.
- I will not eat or drink near computing equipment.
- I will plug in the laptop when I return it to the caddy.
- I will report any defects in the school laptop to the teacher.

Personal Device

- I will ensure my device is charged for use each day.
- During the school day, I will use my device for school work only.
- I will not allow others to use my device or login details.
- **I understand** my personal device must run the school's required **monitoring/security software** to be used in school.

Use of internet and email:

- I will use the internet responsibly and for school activities only.
- I will not bully online (cyberbullying).
- I will report any websites with inappropriate content to a member of staff.
- I understand that if I use the internet irresponsibly, I will have that privilege removed.
- I will use the school email and other systems responsibly.
- I will only open emails if I know who has sent it to me.
- I will not open attachments from unknown sources.
- I will only connect to The Gregg School WI-FI whilst in school.

AI Tools

- I will not present the work of others or Artificial Intelligence as my own. If a teacher suspects AI has been used, they will use a suitable tool to check for plagiarism.
- If I decide to use Artificial Intelligence in my work, I will give it credit accordingly.
- I will avoid entering personal data or confidential information into AI tools.

Security and Privacy:

- I will not share my password with anyone.
- I will not attempt to bypass the school network's security systems or change settings.
- I will not attempt to access social media networks during the school day.
- I will not post anything online during the school day.
- I will not attempt to view, download or circulate inappropriate content.
- I am aware that my activities on school computing equipment are monitored.
- I am aware that if I am found to be using my personal device for anything other than school work, I will lose the privilege of using my own device.
- I understand that my internet usage will be monitored by the school's filtering and monitoring systems.

Consequences for Misuse

- **I understand** that misuse may result in:
 - Temporary or permanent **loss of access** to services or the network.
 - **Confiscation** of a device during the school day under school policy.
 - **Detentions** or other disciplinary measures.
 - **Parents/Carers** being informed.
 - Referral to the **DSL** or external authorities for serious incidents.
- **I understand** exam-related misconduct may be reported to awarding bodies.

Exam & Assessment Conditions

- **I will** follow all **exam rules** and instructions regarding devices and online platforms.
- **I will not** use devices or online tools during assessments unless **explicitly authorised**.

Acceptance

- **I confirm** that I have read, understand and agree to follow this Student Acceptable Use Policy.
- **I understand** that breaches of this policy have consequences and may affect my access to technology and learning.
- **I understand** this policy is published in my planner and may be updated; I will review updates when notified.

Appendix 3 – Prep School Student Acceptable Use Policy

The Prep school student AUP is shared with students via their parent Starter Pack on joining the school. Any updates or changes are sent out via email.

Student Acceptable Use Policy

- I will only use computing equipment when told to do so by my teacher
- I will only use activities that a teacher has told or allowed me to use
- I will look after all computing equipment carefully
- I will not eat or drink near computing equipment
- I will not share my password with anyone
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use the computing equipment.

Appendix 4 – Why We Filter and Monitor (Staff Version)

This document is available on the staff Firefly dashboard.

1. Purpose of This Guidance

This appendix explains **why the school filters and monitors digital activity**, how this supports our safeguarding duties, and what it means for staff, students, and parents.

Staff with questions or concerns are encouraged to speak with the **Headteacher** or the **Designated Safeguarding Lead (DSL)**.

2. Why the School Filters Internet Activity

The school filters internet access for two principal reasons:

a) Safeguarding and Safety

Filtering is designed to ensure that:

- Students, and where applicable adults, are not exposed to **illegal**, **harmful**, or **inappropriate** online content.
- Access to websites is restricted by **category** and **age group**, in line with statutory expectations.
- Harmful content is blocked whether students seek it intentionally or encounter it unintentionally through search results or misleading links.

b) Duty of Care and Legal Protection

Filtering demonstrates that the school has taken **reasonable steps** to protect students from online risks.

It reduces safeguarding risk and helps fulfil our responsibilities under:

- **Keeping Children Safe in Education (KCSIE)**
- **DfE Filtering and Monitoring Standards (2023)**
- The Trust's **Safeguarding and Child Protection Policy**

3. Why the School Monitors Digital Activity

Monitoring provides **assurance**, visibility, and protection. It is not designed for general surveillance.

Monitoring enables the school to:

- Identify, as far as possible, whether any **inappropriate**, **unsafe**, or **illegal** online activity has occurred.
- Respond promptly to concerns relating to **wellbeing**, **safeguarding risks**, mental health indicators, or potential harm.
- Provide an evidence trail where disciplinary or safeguarding action is required.
- Ensure that students and staff are using digital systems **appropriately**, **professionally**, and **safely**.

Monitoring is **proportionate**, **targeted** and focused on safeguarding rather than personal scrutiny.

4. Privacy and Lawful Basis

Every individual has the right to privacy. However, when using school systems or devices for school purposes, the expectation of privacy is **reduced** in order to fulfil statutory safeguarding duties.

Monitoring is conducted under the lawful bases of:

- **Public Task** – the school acting in the public interest to safeguard children
- **Legal Obligation** – compliance with safeguarding legislation (KCSIE)
- **Vital Interests** – where monitoring may protect a child or adult from serious harm
- **Legitimate Interests** – maintaining secure and safe digital systems

Consent is not required for filtering or monitoring. What *is* required is **transparency**, which the school actively provides.

5. Personal and School Devices (BYOD and School-Owned Equipment)

Monitoring may apply to:

- **School-owned devices**, at all times
- **Personally owned devices**, when:
 - used on the school network
 - used on school premises for school-related activity
 - required to run school-approved safeguarding or monitoring software (BYOD conditions)

Any monitoring of personal devices is limited strictly to **school-related activity** and is never used to examine private personal content unrelated to school.

6. Communication with Students and Parents

Students

At the start of each academic year (Autumn Term), students will be informed:

- that online activity may be monitored
- why monitoring is necessary
- how it protects their safety
- how they can ask questions or raise concerns

This forms part of their digital safety education.

Parents and Carers

Each academic year, parents will receive a communication explaining:

- that students' internet activity may be monitored
- how this supports safeguarding
- how the monitoring process is explained to students
- how concerns can be raised via the pastoral or safeguarding team

Parents and students will be asked to **acknowledge** (not give consent to) their understanding of the Acceptable Use Policy and the school's approach to filtering and monitoring.

7. Summary

Filtering and monitoring are essential parts of the Trust's safeguarding provision. They:

- protect young people from online harm
- enable early identification of risks
- help maintain a safe learning environment
- ensure compliance with statutory standards
- support staff in fulfilling their safeguarding responsibilities

Staff should feel confident in discussing this with students and parents and are encouraged to seek clarification where needed.

Appendix 5 - Training and Curriculum Plans

Training and Curriculum plans

Senior School

E-Safety Schemes of work

The table below identifies the topics covered in the Key Stage 3 E-Safety schemes of work during computing lessons.

Year 7	Year 8	Year 9
Digital Life 101	My Media	Trillion Dollar Footprint
Strategic Searching	A Creator's Responsibilities	Identifying High Quality Sites
Scams and Schemes	Safe Online Talk	Reality of Digital Drama
Cyberbullying Be Upstanding	Which Me Should I Be?	Cyberbullying - Crossing the line
A Creator's Rights	Gender Stereotypes Online	Rework, Reuse, Remix

Students receive additional lessons around Safer Internet Day each year.

Students in Key Stage also complete 3 lessons on the topic of Online Sexual Harassment as part of a project working with the charity ChildNet and there are enrichment activities on E-Safety via the Respect program.

In PSD lessons, students cover the following topics:

Year 7	Year 8	Year 9
Media Literacy and Digital Resilience	Bullying, Abuse and Discrimination	Respectful Relationships including consent.
		Crime, Extremism and Online Risk
		Social Influences

In Key stage 4, students receive lessons on the following topics in their PSD lessons as well as through the program of assemblies.

Years 10 and 11
Cyberbullying
Risky Online Relationships including online pressures
Rights, remixes and Respect
Digital Footprint
Sexting
Online Fraud and Scams

E-Safety for Parents

The E-Safety Officer or DSL will run training session(s) for parents on how they can support safe e-use by their child. This will be either online or in person. Parents are also encouraged to complete the National Online Safety modules for parents.

E-Safety for Staff

All staff will be trained on the requirements of this policy annually as part of their annual safeguarding update training. Staff also complete the National Online Safety training course for teachers/support staff.

Prep School

The Prep school use Twinkl resources for their Computing lessons including e-Safety.

This covers the following topics/lessons in Key Stage 1:

Reception
Staying Safe on the internet (Buddy the Dog's story/discussion cards)
What do we use the internet for?
Staying SMART online

F1

Safe Image searching
Staying SMART Online
My personal information
What is email?
Keeping safe online

F2

Digital Footprint
Identifying dangers online
Being Kind Online
Cyber Snakes & Ladders - website searching

Y3/Y4

Cyberbullying
Search engines
Plagiarism
Sharing information
Acceptable/unacceptable behaviour
Reporting concerns.

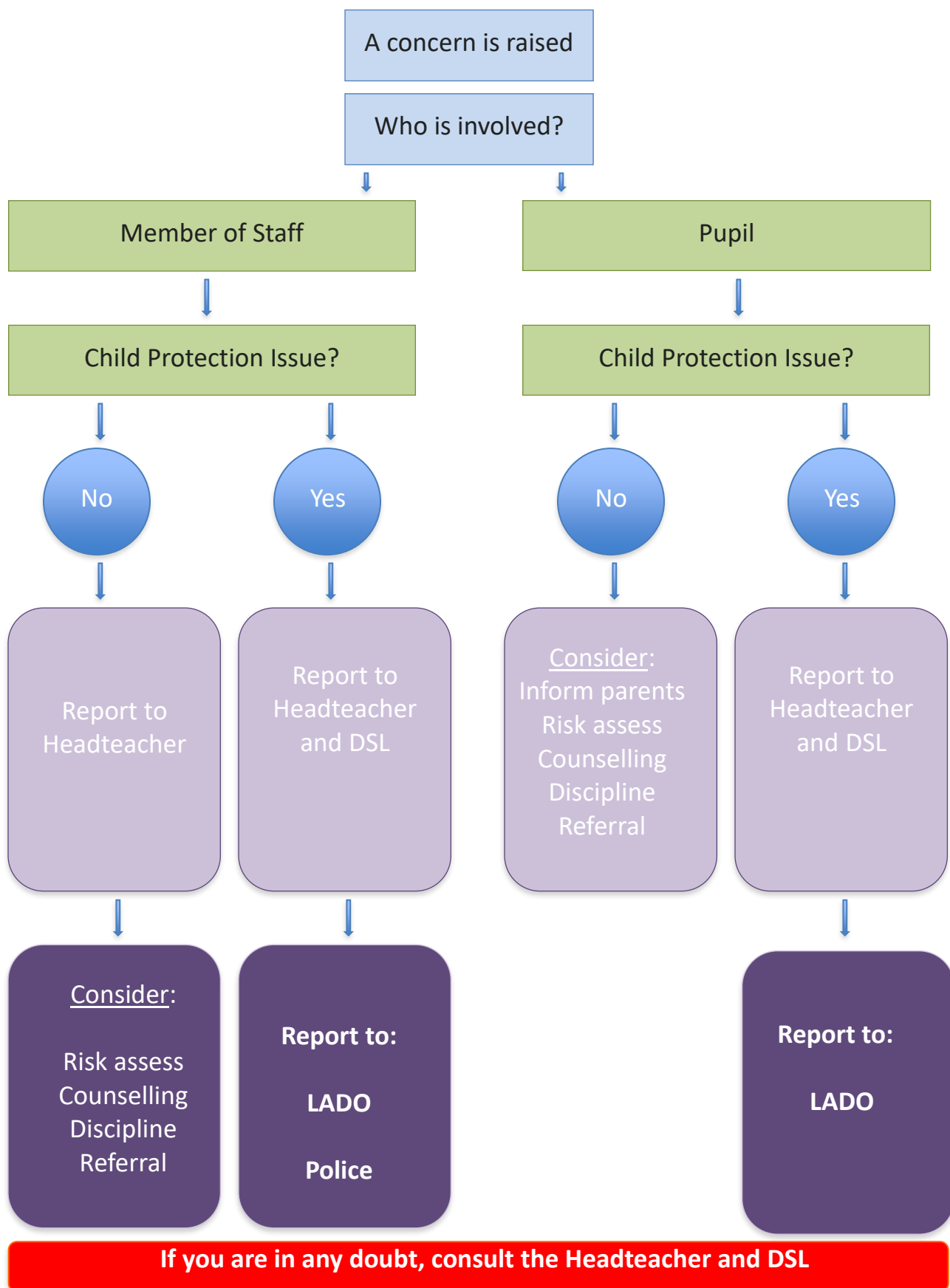
Y5/6

Cyberbullying (including comparisons with in-person bullying and strategies for dealing with it)
Identifying secure and insecure websites (e.g. recognising the lock symbol and checking for site security)
Online relationships and the safe sharing of personal information
Media awareness, including how gender stereotypes are presented online
Applying online safety rules using the SMART acronym

Students receive additional lessons and assemblies around Safer Internet Day each year.

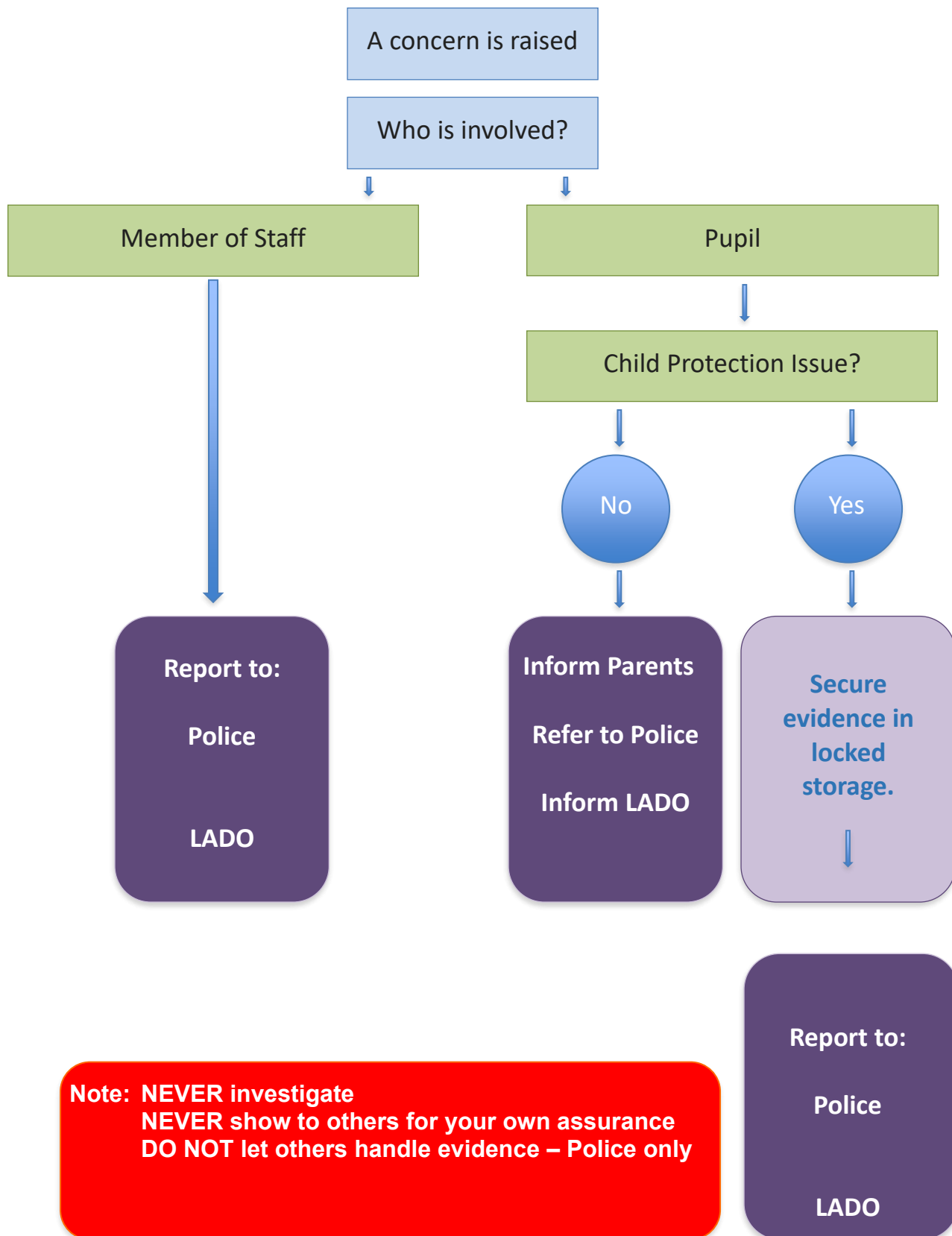
Appendix 6 – Inappropriate Activity Flowchart

Inappropriate Activity Flowchart



Appendix 7 – Illegal Activity Flowchart

Illegal Activity Flowchart



Appendix 8 – Malware Incident Response Plan

Malware Incident Response Plan

1. Immediately disconnect the infected computers, laptops or tablets from all network connections, whether wired, wireless or mobile phone based and phone CSE (01993 886688).
In a very serious case, consider whether turning off the Wi-Fi, disabling any core network connections (including switches), and disconnecting from the internet might be necessary.
2. Reset credentials including passwords (especially for administrator and other system accounts).
3. Safely wipe the infected devices and reinstall the OS.
4. Infinity Education will verify that the backup is free from any malware as well as connect devices to a clean network in order to download, install and update the OS and all other software.
5. Infinity Education will install, update, and run antivirus software.
6. When instructed to by Infinity Education, we will then reconnect to your network.
7. Monitor network traffic and run antivirus scans to identify if any infection remains.



THE GREGG SCHOOL

Mobile Phone & Smart Device Policy (Students & Staff)

This policy will be kept under regular review and updated in line with DfE recommendations and changes in legislation.

1. Policy Statement

The Gregg School is committed to ensuring a **calm, safe and focused learning environment**. To support this, and in line with the latest DfE guidance, **mobile phones and smart devices are prohibited throughout the school day for all students**.

This policy applies to:

- Mobile phones
 - Smart watches with communication or recording abilities
 - Wireless earbuds/headphones
 - Any device capable of messaging, recording, or online communication, which are not required for completing classwork
-

2. Purpose of this Policy

This policy ensures:

- A distraction-free environment for teaching and learning
 - Reduced incidents of bullying, online harm and social distraction
 - Alignment with legal duties on behaviour, safeguarding, searching, and reasonable adjustments
 - Clarity for students, staff and parents regarding expectations and consequences
-

3. Student Mobile Phone Rules

3.1 Prohibition During the Entire School Day

Students **must not use or access** mobile phones from 8.30 to 4 pm (5pm if staying after school) and including the following:

- Before and during morning registration
- During lessons
- During transitions between lessons
- During breaktime and lunchtime
- During assemblies
- During extra-curricular sessions during the school day
- Immediately after school while on school grounds

3.2 Travelling to and from School

Senior school students may carry a phone for safety while travelling but phones must be turned OFF upon entering school and school grounds. Phones must remain powered off and securely stored in a school bag until students leave school and school grounds at the end of the day.

Prep school students are not encouraged to bring mobile phones to school. The only exceptions are those students who travel via school minibus. In this situation the phone is handed to the driver when the student embarks, and the driver hands it in to the office upon arrival at school. The phone is then returned to the student at the drop off point that evening by the driver. The school cannot be held responsible for the phone.

3.3 Trips and Visits

- Senior school students may bring mobile phones on trips and visits. Devices must be kept powered off and securely stored in a school bag and may only be used with the explicit permission of the lead teacher. For visits that include an overnight stay, students are required to hand in their mobile phones to staff for safekeeping during the night.

3.4 Sanctions for Breach of the Mobile Phone Policy for Senior School students

- All mobile devices must remain switched off and securely stored in a school bag for the duration of the school day. Any breach of this requirement—including a device sounding or vibrating while in a school bag—will result in the following sanctions: a 6-debit detention will be issued, the device will be confiscated by the member of staff involved.
- The teacher issuing the 6-debit detention will add this to Mantis as per normal procedure.
- The member of staff who issues the sanction must take the device to Reception. The device will be securely stored in a locked drawer until it is collected at the end of the day.
- If this is period 5 or 6, teacher to issue the 6-debit detention, but to give the mobile back to the student at the end of the lesson.
- If a student accrues **more** than two 6-debit detentions in one half-term, the student will have their mobile confiscated for **the school day** for the rest of the half term. This will be locked in the reception drawer.

4. Staff Rules for Mobile Phone Use

To model expected behaviour and ensure policy consistency:

4.1 Personal Mobile Phone Use

Senior school staff must:

- **Not use personal phones in front of pupils** during the school day except in emergencies
- Keep phones on silent and out of sight in teaching areas
- Staff **must not use personal devices in ways that compromise safeguarding**

Prep school staff:

- **No personal phone use around children**
- No photos/videos taken on personal devices
- Devices stored away and used only in controlled situations

4.2 Professional Use of Devices

Senior staff **may** use phones or school-issued devices for:

- Multi-factor authentication (school systems)
- Emergency safeguarding communication
- A clearly defined educational or business purpose that necessitates the use of this technology (agreed with SLT)

4.3 Photography/Video

- Only school-provided devices/cameras may be used for taking photographs or videos of children, adhering to The Gregg School Safeguarding Policy
- **Visitors/Parents:** Visitors are forbidden from using mobile phones on the premises, with policies enforced by staff.

4.4 Enforcement Responsibilities

All staff must:

- Enforce the mobile phone policy consistently and without exceptions
- Challenge students who breach the policy and follow the sanctions outlined above
- Confiscate devices according to procedure
- Report repeated breaches to Tutors / Heads of Year

5. Sanctions for Student Misuse

Sanctions for breaching the policy align with the school's existing Behaviour & Discipline Policy.

5.1 Safeguarding Considerations

If misuse suggests a risk of harm (e.g. bullying, harassment, online risks):

- DSL must be informed immediately
- Safeguarding procedures followed in line with *Keeping Children Safe in Education* (DfE)

6. Confiscation & Searching

Staff are legally protected when confiscating a phone used in breach of policy, provided they act reasonably. The phone can be collected by the student at the end of the day. Searching for a phone or device should be conducted by a member of the pastoral or SLT teams.

7. Reasonable Adjustments & Exceptions

In line with the Equality Act 2010 and SEND/medical statutory guidance, exceptions may be made for:

- Students with disabilities
- Students with medical conditions requiring phone-linked monitoring (e.g. diabetes CGM)
- Young carers
- Specific safeguarding needs

Adjustments must:

- Be approved by HOY or SLT
 - Specify exact times and locations where the device may be accessed
 - Be reviewed regularly
-

8. Expectations for Parents

Parents must:

- Support the school's mobile phone-free environment
- Contact the school office—not their child—during the day
- Discuss risks of mobile misuse with their child
- Raise concerns promptly with staff

Parents' support is emphasised within DfE guidance.

9. Education & Online Safety

Through the PSHE, RSE, Computing curriculum and assemblies, students will continue to be taught:

- Online risks, bullying and privacy
 - Psychological impact of constant connectivity
 - Benefits of reduced phone use
 - Healthy digital habits
-

10. Review of Policy

This policy will be reviewed:

- Annually (in line with Behaviour Policy)
- After significant changes to DfE guidance
- Following any safeguarding recommendations