	The Gregg Schools Trust Proprietor of The Gregg School and The Gregg Preparatory School	Document Owner E-Safety Officer
		Document Type: Policy
	The Gregg School **E-Safety Policy**	Issue Date: Feb 2024
		Revision: Version 8

Applies to: The Gregg School ☒ The Gregg Preparatory School ☒

Critical ISI Policy? YES ☒ NO ☐	ISI Paragraph Reference:
Version approved by:	Date of Approval:

Date of last Review: Feb 2023	Review frequency: 1 year/s (1/2/3)	Date of next Review: Feb 2025

1. Policy Statement

1.1 The requirements of this policy apply to all of 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.

Users - refers to staff, governing body, 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.

1.2 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 SIMS, Firefly and Office 365), school telephones and text systems, cameras and recording equipment, school website, and any other electronic or communication equipment used in the course of the user's work.

1.3 Safeguarding is a serious matter. At The Gregg Schools Trust we use 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 twofold:

a. To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.

b. 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.

1.4 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 the Firefly Dashboard.

2. Roles & Responsibilities

2.1 The Gregg Schools Trust

The Trust is accountable for ensuring that our school has effective policies and procedures in place; as such they will review this policy regularly and in response to any E-Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the School; and to ensure E-Safety incidents were appropriately dealt with and that the policy was effective in managing those incidents

2.2 Headteachers

Reporting to the Trust, the Headteachers have overall responsibility for E-Safety within the schools. The day-to-day management of this will be delegated to the E-Safety Officer, who will liaise with the appropriate Designated Safeguarding Lead (DSL).

The Headteachers will ensure that:

a. E-Safety training throughout the school is planned, up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, governing body and parents
b. 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.

c. 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 E-Safety Officer at the Senior School is devolved to the Assistant Headteacher responsible for IT, supported by the DSLs. At the Prep School it is devolved to the DSL in liaison with the E-Safety Officer and Deputy Facilities Manager at the Senior School.

The above will:

a. Keep up to date with the latest risks to children whilst using technology and familiarize him/herself with the latest research and available resources for school and home use
b. Review this policy regularly and bring any matters to the attention of the Headteacher
c. Advise the Headteacher and governors all E-Safety matters
d. Engage with parents and the school community on E-Safety matters at school and/or at home
e. Liaise with other agencies as required
f. Retain a log of E-Safety incidents on SIMS and the Monitoring Overview document (Staff Share > Pastoral) at the Senior School and on SchoolPod at the Prep School
g. Ensure any technical E-Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose
h. Make him/herself aware of any reporting function with technical E-Safety measures, i.e. internet filtering reporting function, Net Support's DNA tool violation log viewer by student and date/time; liaise with the Headteachers of both schools, and the Trust, to decide on what reports may be appropriate for viewing.

2.4 Managed Service

CSE, under the direction of the E-Safety officer and Deputy Facilities Manager, are responsible for ensuring that the IT technical infrastructure across the Trust is secure. This will include at a minimum:

a. Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
b. Windows updates are regularly monitored and devices updated as appropriate
c. Any E-Safety technical solutions such as Internet filtering are operating correctly
d. 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 Headteachers.
e. Passwords are applied correctly to all users regardless of age

2.5 All Staff

Staff are to ensure that:

a. All details within this policy are understood. If anything is not understood, it should be brought to the attention of the E-Safety Officers.
b. The boundaries for use of ICT equipment and services in both schools, 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 relevant Headteacher.
c. Any E-Safety incident is reported to the appropriate E-Safety Officer, who log the incident, or in his/her absence to the relevant Headteacher.
d. The reporting flowcharts contained within this E-Safety policy (Appendices 6 and 7) are fully understood.

2.6 All Students

a. The boundaries for use of ICT equipment and services in this school, and/or personal equipment are given in the student Acceptable Use Policy. Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the School's Behaviour Policy.

b. E-Safety is embedded into the curriculum of both schools. 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

a. 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 schools 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.

b. Parents are informed of their responsibilities on FIREFLY

3. Technology

The Gregg 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.

3.1 Internet Filtering and Monitoring

The school uses Smoothwall software that prevents unauthorized 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. Staff and student devices are monitored using Net Support software. Staff are able to see what students are doing on school devices remotely. The E-Safety Officer is 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 Trust 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 schools' IT systems including email and VPN.

3.4 Anti-Virus

All capable devices will have anti-virus software. This software, ESET, 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

a. 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.

b. Students

Senior School
Where a student does bring their phone to school, it should not be switched on during the school day unless they are instructed to use it by a member of staff as part of a lesson.

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

a. **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.

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

b. 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, Personal Digital Assistants (PDAs), 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.

c. Students and parents/guardians using any BYOD technology must adhere to this policy and, for the Senior School, the student AUP.

d. 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).

e. BYOD devices must not be used to record, transmit or post photographic images or video of a person, or persons on campus 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.

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

3.7 Cloud Storage

All student cloud drives will be monitored by the E-Safety Officer(s).

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

a. 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.

b. 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

a. 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.

b. **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. 24SmithT@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

a. 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.

b. 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.

c. 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 which is sent out by the Registrar. 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 held on Schoolpod.

For both schools, 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

a. There are many social networking services available and The Trust 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.

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

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

i. 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.
ii. There is to be no identification of students using first name and surname; first name only is to be used.
iii. Where services are "comment enabled", comments are to be set to "moderated".
iv. 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 either 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 in his/her absence the relevant Headteacher. The E-Safety Officers will assist you in taking the appropriate action to deal with the incident and to fill out an incident log. At the Senior School this will be on SIMS and the Monitoring Overview document (Staff Share > Pastoral), at the Prep School, this will be on SchoolPod.

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:

a. To communicate to anyone who is not authorised to receive information that is confidential to the school
b. To deliberately present personal views or opinions as those of the school
c. To knowingly access, view, download, post, e-mail or otherwise transmit pornography or sexually suggestive or harassing materials or messages
d. To knowingly access, view, download, post, e-mail or otherwise transmit materials or messages that promote extreme religious beliefs
e. 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
f. To access, view, download, post, e-mail or otherwise transmit material that contains viruses
g. To use the school's facilities to undertake gambling, trading or any other action for personal gain or political purposes
h. To undertake any activity which has negative implications for the safeguarding of young people
i. 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

a. 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, each school will have an annual programme of training which is suitable to the audience (see Appendix 10).

b. 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.

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

d. The relevant E-Safety Officer is responsible for recommending a programme 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

a. 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.

b. 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 pro-active 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 School's Anti Bullying and Behaviour & Discipline Policies.

c. What advice we give to students

Through our curriculum and assembly programme 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.

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

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 – Student Acceptable Use Policy

The Senior School Student AUP is shared with students electronically on their Firefly dashboard.

Senior School - Student Acceptable Use Policy

Use of Equipment:

- I will not install programs on to school equipment.
- I will take care to look after all computing equipment.
- I will not eat or drink near computing equipment.
- I will use my personal laptop for schoolwork only whilst it is in school.
- I will ensure my device is charged for use each day.

Use of Internet and email:

- I will use the Internet for school activities only.
- I will not cyberbully.
- 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 not copy and paste materials off the Internet and present it as my own.
- I will use the school email system and Teams responsibly.
- I will only open emails if I know who has sent it to me.
- I will not open attachments from unknown sources.

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.
- I will not post anything online in school.
- 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 my device is not running the school's monitoring software, I will not be able to use it in school
- I am aware that if I am found to be using my personal my personal device for anything other than school work, I will lose the privilege of using my own device.

Appendix 3 – Prep Student Acceptable Use Policy

The Prep School Student AUP is shared with students via their parents Starter pack on joining the school. Any updates or changes are sent out via email.

Prep School - 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 3 – Why we filter and monitor – Staff version

This document can be found on the staff Firefly dashboard.

Why do we Filter and Monitor?

These guidance notes attempt to explain to staff why monitoring is important. Staff who wish to ask further questions or voice concerns are welcome to direct these to the Headteacher.

The School filters Internet activity for two reasons:

We filter to ensure:

- As far as possible, that students (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results
- As far as possible, that the school has mitigated any risk to the students, and thereby reduces any liability to the School by making reasonable endeavours to ensure the safety of those children and young people.

We monitor for assurance:

- As far as possible that no inappropriate or illegal activity has taken place
- To add to any evidential trail for disciplinary action if necessary.

A right to privacy?

Everybody has a right to privacy, whether adult or child. However, in certain circumstances there is a reduced expectation of privacy. In the context of this policy, that reduction is for security and safeguarding. This expectation is applicable whether it is school-owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network, but is used in school or for school business).

Consent to monitor is not a requirement, however under the requirements of General Data Protection Regulations 2018, the School will make all reasonable efforts to inform users that they may be monitored and to work with them to understand why.

Some staff, students or parents may disagree with what the School is doing, but that is their right and consent is not a requirement of the Regulations. It is the understanding, not the consent that is important.

Students – will be made aware that their activity may be monitored, the reasons why this may be necessary and given the opportunity to ask questions at the beginning of each Autumn Term.

Parents – have access to a document on the Parent Firefly dashboard which explains that internet activity may be monitored and why. It also informs parents that the School will talk to students and allow them to voice concerns and ask questions. Parents and students will be required to sign and return a reply slip to say they understand (even if they do not agree).

Appendix 4 – Why we filter and monitor – Student/Parent version

This version can be found on the student and parent Firefly dashboards.

E-Safety, Internet Filtering and Monitoring

Keeping our students safe is at the core of what we do here at the Gregg School. As use of ICT to enhance learning is a growing part of how we educate children, we are using the Internet increasingly across all areas of the curriculum.

Keeping children safe whilst using ICT is known as E-Safety and is governed by the School's E-Safety Policy.

Use of the Internet in school is a vital part of the education of your son/daughter. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access such sites. We are able to do this using software known as an Internet filter. The filter categorizes websites in accordance with their content, and the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use, as the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school, therefore, in order to ensure that there have been no attempts at inappropriate Internet activity, we may occasionally monitor these logs. If we believe there has been an attempt at questionable Internet activity involving your child, we will inform you of the circumstances.

At the beginning of each school year we explain the importance of Internet filtering to all students. Furthermore, we explain that there has to be a balance between personal privacy and safety. We also inform students that we can monitor their Internet activity. As part of this, Students are also given the opportunity to ask questions and give their viewpoint on the School's policy regarding Internet use.

A copy of the School's updated E-Safety Policy is available on Firefly. If you have any questions or concerns about Internet filtering and monitoring at The Gregg School, please contact Ms Cooke at hcc@thegreggschools.org

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
Welcome to the Computing Lab	My Media	Trillion Dollar Footprint
Welcome to your workstation	A Creator's Responsibilities	Identifying High Quality Sites
Respectful online communication	Safe Online Talk	Reality of Digital Drama
Presenting to an audience (Cyberbullying)	Which Me Should I Be?	Cyberbullying - Crossing the line
Who are you talking to?	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.

In PSD lessons, student 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 programme 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 Designated Safeguarding Lead will run an annual training session for parents on how they can support safe e-use by their child. 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 up-date 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	Year 1	Year 2
Staying Safe on the internet (Buddy the Dog's story/discussion cards)	Owning your Creative Work	Digital Footprints
What do we use the internet for?	Safe Image Searching	Keywords
Staying SMART online	Staying SMART online	You be the judge
	My Personal Information	Rate and Review
	What is email?	Being Kind Online
	Keeping Zibb safe online	Cyber Snakes and Ladders

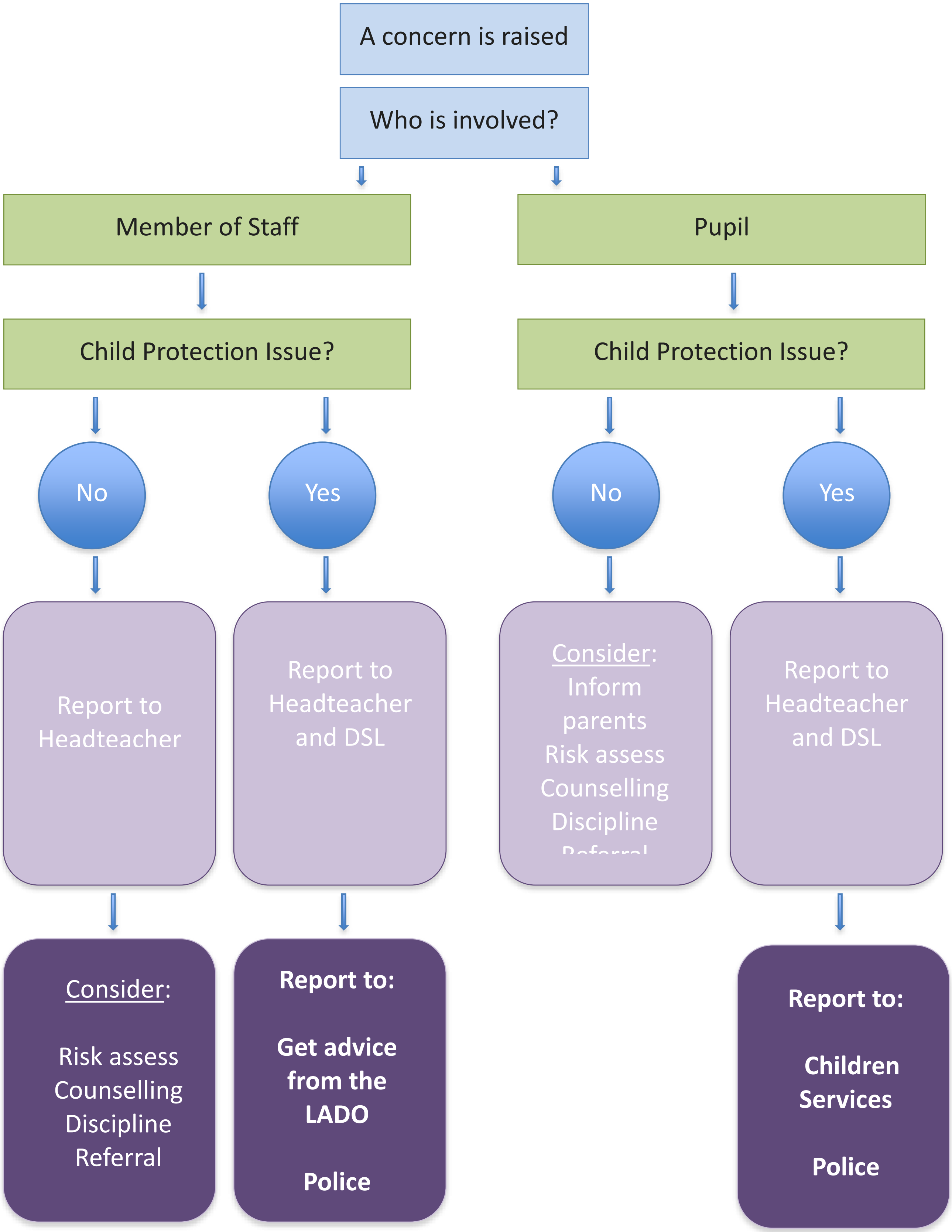
This covers the following topics in Key Stage 2:

Year 3	Year 4	Year 5	Year 6
What is Cyberbullying?	Cyberbullying	Spam!	Cyberbullying
To buy or not to buy?	Super Searchers	Sites and cite	Secure Websites
Keep it to yourself	Copycats!	Powerful Passwords	People Online
Emailing	Too much Information?	False Photography	Girls and Boys Online
Online Communication	The Online Community	Online Safety Story Planning	SMARTbots
Party Planners	Cyber Superheroes	Online Safety Comics	Let's get quizzical

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

Appendix 6 – Inappropriate Activity Flowchart

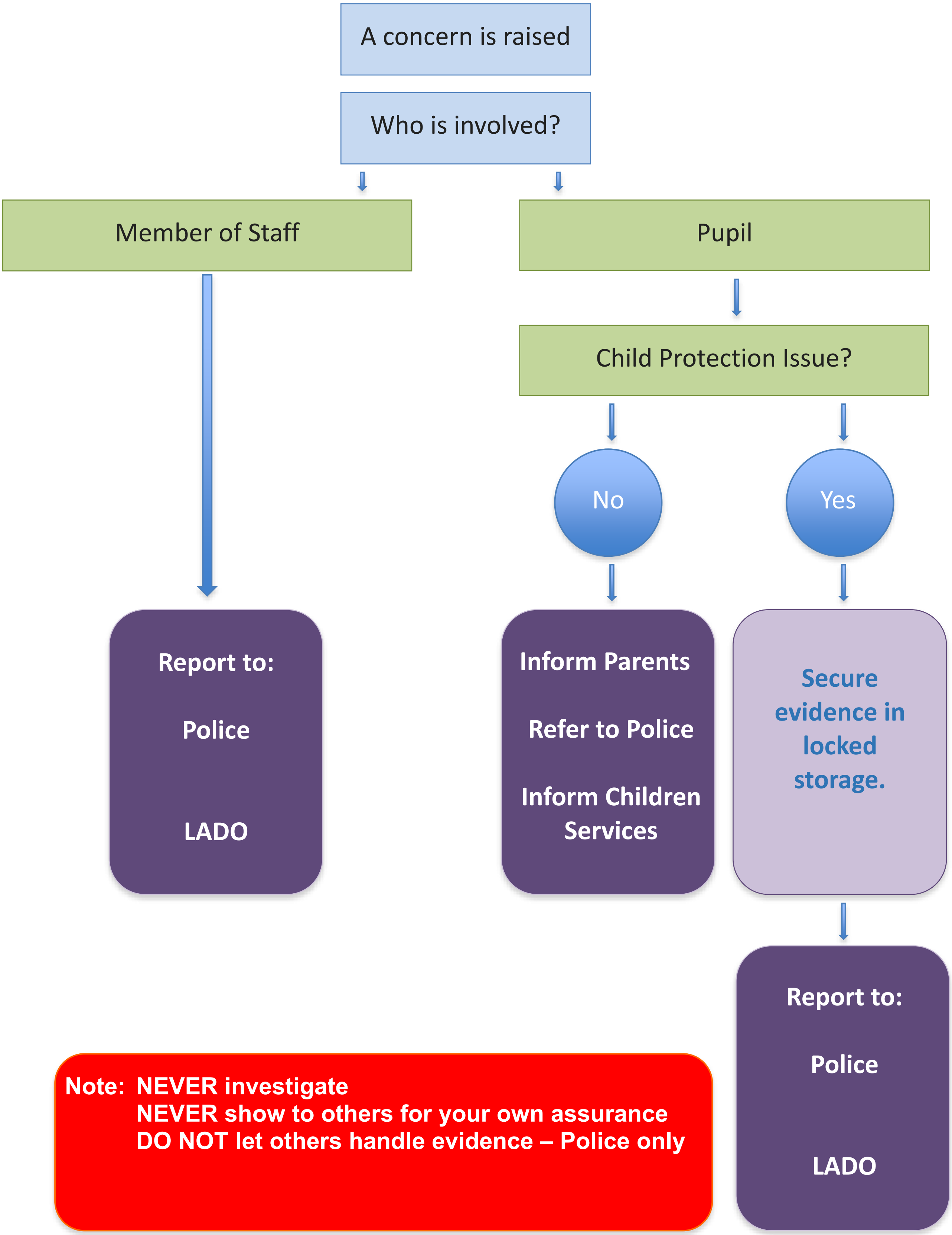
Inappropriate Activity Flowchart


A concern is raised
Who is involved?
Member of Staff
Pupil
Child Protection Issue?
Child Protection Issue?
No
Yes
No
Yes
Report to Headteacher
Report to Headteacher and DSL
Consider: Inform parents Risk assess Counselling Discipline Referral
Report to Headteacher and DSL
Consider: Risk assess Counselling Discipline Referral
Report to: Get advice from the LADO Police
Report to: Children Services Police

If you are in any doubt, consult the Headteacher and DSL

Appendix 7 – Illegal Activity Flowchart

Illegal Activity Flowchart



Note: NEVER investigate
NEVER show to others for your own assurance
DO NOT let others handle evidence – Police only

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. CSE 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. CSE will install, update, and run antivirus software.

6. When instructed to by CSE, we will then reconnect to your network.

7. Monitor network traffic and run antivirus scans to identify if any infection remains.