NONSUCH HIGH SCHOOL FOR GIRLS

E-SAFETY POLICY

Contents

1 Introduction and Overview 2-6

2 e-Safety in the Curriculum 6-7

3 Conduct and Incident Management 8

4 IT Infrastructure, Systems and Management..... 9-11

Appendix A Student and Staff Acceptable Use Statement..... 12

Appendix B Nonsuch Student and Staff Acceptable Use Agreement 12

Appendix C Managed Learning Environment (MLE) Rules 13

Appendix D Phone / Bring Your Own Device (BYOD) protocol..... 14

Appendix E Curriculum and PSHE Overview 15-16

Appendix F Annual e-Safety Checklist..... 17

Appendix G Governors' Checklist 17

Reviewed and Agreed by the Nonsuch Local Governing Body: October 2024

Next review: July 2025

Policy Notes may be subject to review and revision at any time by the Nonsuch Local Governing Body notwithstanding that the next review date has not been reached.

Review dates are for guidance only and whilst the intention is always to arrange reviews within the stated time frame all Policy Notes will remain in force until this has taken place and been formally approved by the Nonsuch Local Governing Body.

1. Introduction and Overview

1.1 Rationale

1.1.1 Purpose

This policy concerns student and staff e-Safety.

'Keeping children safe in education' 2024 states that:

"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate."

This policy will aim to:

- set out the key principles expected of all members of the Nonsuch school community with respect to the safe use of IT-based technologies;
- assist school staff to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice;
- set expectations of behaviour and / or codes of practice relevant to e-Safety;
- provide structures to deal with e-Safety issues and possible consequences (such as disciplinary or legal action) which might arise;
- ensure that all members of the school community are aware what constitutes unsafe or unhealthy behaviour;
- minimise the risk of allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, privacy issues, digital footprint and online reputation, health and well-being, sexting, bullying behaviour and use of inappropriate language

Commerce: risks such as online gambling, inappropriate advertising, phishing, financial scams and evolving cyber-crime technologies.

This policy applies to all members of our community and any guests who have access to and are users of our IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site, as well as in school, and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-Safety incidents covered by this policy, which may take place outside the school (e.g. as part of remote online provision), but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and within electronic devices and the deletion of data. See the school's Behaviour for Learning policy for further information on the Power of Search

The school will deal with such incidents and, where appropriate, will inform parents / carers of incidents of inappropriate e-Safety behaviour that take place out of school.

1.1.2 Limits

This policy does not define or implement IT Strategy or working practices, data protection, implementation of IT legislation (including copyright, licensing, computer misuse or GDPR legislation) or the IT /CS /PSHE curricula. Such areas will be referenced in specific connection with e-Safety only.

This policy will not duplicate detailed content of other policies but may recommend updates or additions to them.

1.2 Roles and Responsibilities

Headteacher

- To take overall responsibility for e-Safety provision and ensure that the e-Safety policy is up to date with other related policies.
- To ensure the school uses an approved, filtered Internet Service which complies with current statutory requirements.
- To be responsible for ensuring that staff receive suitable training to carry out their e-Safety roles and to train other colleagues, as relevant.
- To be aware of procedures to be followed in the event of a serious e-Safety incident.
- To receive and respond to regular monitoring reports from the Designated Safeguarding Lead.
- To ensure that there is a system in place to monitor and support staff who carry out internal e-Safety procedures (e.g. network manager).

Designated Safeguarding Lead

- To take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).

E-Safety Co-ordinator (reporting to the Designated Safeguarding Lead)

- To take day-to-day responsibility for e-Safety issues and have a leading role in establishing and reviewing the school e-Safety policies and documentation.
- To promote an awareness of and commitment to e-safeguarding throughout the school community.
- To ensure that appropriate e-Safety education is embedded across the curriculum.
- To liaise with school IT technical staff.
- To communicate regularly with SLT, with a minimum of once a term, to discuss current issues and review incident logs.
- To summarise issues and incidents for the e designated e-Safety Governor via the Headteachers report.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident.
- To ensure that e-Safety incidents are recorded according to safeguarding record-keeping procedures as appropriate.
- To facilitate e-Safety training and advice for all staff.
- To be regularly updated on e-Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from e-Safety matters.
- To coordinate transmission of information to parents (via information evenings or events, newsletter, e-Safety web page updates)
- To ensure the school communicates updated advice to students, staff and parents concerning E-Safety via the school website

Computer Science Curriculum Leader

- To oversee the delivery of the e-Safety element of the Computer Science curriculum for KS3.
- To liaise with the E-Safety Co-ordinator on e-Safety matters and inform the development of e-Safety teaching in PSHE lessons for KS4 &KS5

Network Manager / IT Technician

- To report e-Safety related issues that arise to the Designated Safeguarding Lead.
- To be proactive in monitoring use of the school's systems and detecting e-Safety concerns.
- To manage systems which enable logging of network and software activity, and to provide access and tracking reports when investigating incidents or concerns.
- To maintain appropriate web monitoring and filtering systems.

Teachers

- To embed e-Safety issues in all aspects of the curriculum and other school activities as appropriate.
- To supervise and guide students when engaged in learning activities involving online and communications technology.

All staff

- To read, understand and help promote the school's e-Safety policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Statement (see Appendix A) and Bring Your Own Device (BYOD) protocol.
- To be aware of e-Safety issues related to the use of mobile devices, monitor their use and implement current school policies regarding these devices.
- To report any suspected misuse or problem to the Designated Safeguarding Lead.
- To maintain an awareness of current e-Safety issues and guidance e.g. through CPD.
- To model safe, responsible and professional behaviours in their own use of technology.
- To ensure that any digital communications with students are conducted on a professional level and only through school-based systems, in accordance with the Student and Staff Acceptable Use Statement (GLT IT Policy, Appendix A)

Students

- To read, understand and sign to agree to adhere to the Student and Staff Acceptable Use Statement (GLT IT Policy, Appendix A & B) and Managed Learning Environment (MLE) Rules (Appendix C)
- To understand the importance of reporting abuse, misuse of or access to inappropriate materials.
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To know and understand school protocol on the use of mobile devices (Appendix D).
- To adhere to the school's Behaviour for Learning policy with relation to e-Safety
- To understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school.
- To take responsibility for learning about the benefits and risks of using the Internet, social media/network and other technologies safely both in school and at home.

Parents / Carers

- To support the school in promoting e-Safety.
- To read, understand and endorse the Staff and Student Acceptable Use Policy.
- To sign the copy of the Staff and Student Acceptable Use Agreement.
- To support and promote the school Staff and Student Acceptable Use Policy
- To read and agree the BYOD protocol
- To sign the BYOD protocol
- To access the school website, MLE and online student records responsibly
- To consult with the school if they have any concerns about their child's use of technology

Governors

- To ensure a member of the Governing Body has taken on the role of e-Safety Governor

E-Safety Governor

- To ensure that the school follows all current e-Safety advice to keep the students and staff safe.
- To approve the e-Safety Policy and review the effectiveness of the policy, via the Local Governing Body.
- To ensure that the school has appropriate filtering and monitoring systems in place and reviews their effectiveness.
- To support the school in encouraging parents and the wider community to become engaged in e-Safety activities.

1.3 Communication:

The policy will be communicated to staff, students and Governors in the following ways:

- The Policy to be posted on the school's website
- The Policy and Agreement will be part of the school induction programme for new staff.
- The Student Acceptable Use Policy and Agreement and BYOD protocol will be discussed with students at the start of each year by form tutors and to late starters by our admissions officer.

1.4 Handling Complaints:

- The school takes reasonable precautions to ensure e-Safety. However, due to the scale and range of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.
- The school cannot accept liability for material accessed, or any consequences of Internet access or use of communications technology.
- Inappropriate on-line content/contact/conduct should in the first instance be reported to a form tutor or Head of Year depending on the severity. Our Designated Safeguarding Lead will act as first point of contact for any complaint that triggers our safeguarding thresholds.
- Any complaint about staff misuse will be referred to the Head teacher. Staff should refer to the Girls' Learning Trust Whistleblowing Policy.
- Complaints of cyberbullying are dealt with in accordance with the Behaviour for Learning Policy and the Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with the Child Protection and Safeguarding Policy.

1.5 Review and Monitoring

The e-Safety policy should be read in conjunction with (but not limited to) the following policies:

- Child Protection and Safeguarding Policy
- Data Protection Policy
- Anti-Bullying Policy
- Behaviour for Learning Policy

The e-Safety Co-ordinator, working with the Designated Safeguarding Lead, will be responsible for document ownership, review and updates. The e-Safety Policy will be updated when significant changes occur regarding the technologies in use within the school.

2. e-Safety in the Curriculum

This school plans delivery of some aspects of e-Safety education as part of the Computer Science curriculum and others in the PSHE curriculum. Broadly, technical and practical aspects are delivered in computing lessons, with social, moral and emotional aspects met through the

PSHE programme. It is also expected that all teachers address aspects of e-Safety education as appropriate across all areas of the curriculum.

2.1 Computing Curriculum

- Computer Science teachers will remind KS3 students about their responsibilities through an Acceptable Use Policy which every student agrees to when using school-based IT systems**. Year 12 students will be given a reminder of their responsibilities as part of the Sixth Form Transition process.**
- The Computer Science department ensures that staff model safe and responsible behaviour in their own use of technology during lessons.
- e-Safety aspects of the Computer Science curriculum are documented in the appendix.

2.2 PSHE Curriculum

- Tutors will deliver through PSHE lessons a range of e-Safety topics appropriate to the age of the students.
- These lessons will ensure the risks of inappropriate content, contact and conduct are all covered comprehensively and understood clearly by the students.
- The lessons will also link where appropriate to Relationships and Sex Education and safeguarding issues such as Child Sexual Exploitation and Radicalisation and Extremism.
- The curriculum will be regularly updated to reflect the latest developments in technology, social media and online behaviour.
- An overview of the PSHE curriculum regarding e-Safety is documented in the appendix.

2.3 Staff and Governor Training

The school:

- provides, as part of the induction process, all new staff with information and guidance on the e-Safety policy and the school's Acceptable Use Policy and BYOD protocol.
- delivers training and education on e-Safety issues and conduct online and reporting concerns available to all staff.
- ensures staff know how to send, receive, handle or store sensitive and personal data appropriately and respond to potential security issues.

2.4 Parent awareness and training

The school runs a rolling programme of advice, guidance and training for parents, including:

- updates to the e-Safety information on the school's website
- provision of information about national support sites for parents
- annual e-Safety information shared with parents
- suggestions for safe Internet use at home updated regularly

3. Conduct and Incident Management

3.1 Expected conduct

All users must conduct themselves in accordance with the requirements of the relevant Acceptable Use Policy. In addition:

All staff must:

- understand the importance of misuse of or access to inappropriate materials and to be aware of the consequences
- report receipt of or abuse/ misuse / access to inappropriate materials
- adopt good e-Safety practice when using digital technologies out of school
- understand that the school's e-Safety Policy covers their actions out of school when using school devices or when identifiable as a member of staff
- know and understand school guidance on the use of mobile devices and BYOD policy
- know and understand school policies on the taking photographs, the use of images and cyber-bullying

3.2 Incident management

- all members of the Nonsuch community are encouraged to be vigilant in reporting issues, in the confidence that these will be dealt with quickly and sensitively, through the school's processes
- as documented in the GLT Child Protection and Safeguarding Policy, any incident causing concern over child protection must be passed to Designated Safeguarding Lead (DSL). The DSL then determines whether an investigation needs to take place. If a safeguarding concern is raised, then the documented child protection procedures will be followed, and the incident logged.
- reports regarding concerns that relate to staff should be referred directly to the Head teacher.
- more minor concerns will be reported to and dealt with by the pastoral team or teaching staff, following the procedures outlined in the Behaviour for Learning policy.
- depending on the nature of the concern, support may be sought from other agencies (e.g. the local authority, CEOP, UK Safer Internet Centre helpline)
- depending on the nature of the concern, parents / carers may be specifically informed of e-Safety incidents involving young people for whom they are responsible
- the school will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law

4. IT Infrastructure, Systems and Management

This section documents e-Safety policy only.

4.1 Internet access and filtering

The school:

- connects to the Internet via a filtered web service, which is monitored, maintained and updated by IT administrators. **Monitoring and filtering reports** track potential inappropriate use of IT.
- installs, maintains and updates software to proactively detect and report computer-based activity which leads to e-safely concerns and incident management
- informs all users that Internet use is monitored
- informs staff and students that they must report concerns regarding unfiltered content to the IT Support Team (including emails, internet search content, uninvited Team participants)
- ensures that all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through policy and CPD
- refers illegal activity to the appropriate authorities including, if necessary, the police.

4.2 Email

The school:

- provides staff with an email account for their professional use;
- will contact the Police if one of our staff or students receives or sends an email that is considered to be particularly disturbing or illegal
- will ensure that email and MLE accounts are maintained and up to date, including the disabling of obsolete accounts
- reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the Police

Student email/MLE communication:

Students are introduced to the use of email as part of the Computer Science scheme of work Students are taught about the safety and etiquette of using email both in school and at home. They are taught:

- that they should not respond to malicious or threatening emails or messages, but instead keep the original copy as evidence, and report any email or message which makes them feel uncomfortable, is offensive or bullying in nature immediately to a member of staff
- that an email or message is a form of publishing which should be formal, clear, concise and respectful to all who read it.
- not to email or send messages to groups of students larger than their form / class.

- not to give out their email address unless it is part of a school managed project or is given to someone they know and trust and is approved by their teacher or parent / carer
- that they must not reveal private details of themselves or others in an email or message, such as address, telephone number, etc.
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe
- that they should think carefully before sending any attachments or uploading documents;
- to communicate during appropriate hours (e.g. not in the middle of the night) and be patient in waiting for a response.

Staff email:

Staff use of the school email system, including provision for monitoring and accessing content, is documented in the Student and Staff Acceptable Use Statement (GLT IT Policy, Appendix A)

Limited numbers of staff have access to whole school email groups. If a member of staff needs to email a group of students larger than their form, class or extra-curricular group, they must refer to their respective line manager for support. Further guidance on sending out emails en-masse is given in the Communications Protocol in the Staff Handbook.

4.3 School Website

- Uploading of information is restricted to our website authorisers.
- Photographs published on the website do not have full names attached.
- We do not use students' names when saving images or tags which are published on the school website.
- We do not use embedded geodata in respect of stored images.
- We expect teachers using school approved blogs or social media platforms to have all content approved by a member of the Leadership Team before it is published

4.4 MLE and internal publishing platforms

- Uploading of information on the school's MLE / virtual learning environment (eg Microsoft SharePoint) is shared between different staff members according to their responsibilities e.g. all class teachers can upload information in their class areas. Teachers must therefore ensure that materials they provide on the MLE do not raise e-Safety concerns.

- Copying and sharing materials available on the school systems and MLE with external individuals or bodies is prohibited, as outlined in the Staff and Students Acceptable Use Policy/Agreement and the MLE rules.

- In school, students must only upload and publish materials within school-approved and closed systems, such as the MLE and other internal systems used in computing lessons as part of the computing curriculum. Teaching staff take responsibility for monitoring content published on these systems. These internal systems are not accessible from outside the school.

4.5 Social Networking

Staff should read this in conjunction with the provisions of the Student and Staff Acceptable Use Statement (GLT IT Policy, Appendix A) and the Teachers' Standards Part Two:

- Teachers are instructed not to run social network spaces for students or allow access to their own personal spaces by students.
- Teachers must regularly review security settings on personal social media profiles to ensure that access by students remains denied.
- School staff will ensure that in their private use of social media:
  - no reference is made to students, parents/carers or school staff
  - they do not engage in online discussion relating to members of the school community which may have been initiated by others
  - that personal opinions are not attributed to the school or Trust.

4.6 Personal mobile phones and devices

- Mobile phones brought into school are entirely at the own risk of staff, students, parents and visitors. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- Students must adhere to the Bring Your Own Device (BYOD) protocol, listed in the Appendices

Appendices

Appendix A **GLT Student and Staff Acceptable Use Policy**
(located within GLT IT Policy, Appendix A)

Appendix B **Nonsuch Student and Staff Acceptable Use Agreement**

By signing underneath, I confirm that I have read the GLT IT policy, Appendix A, and confirm that, when using the school's IT equipment, peripherals, software, data and web resources, I will:

- use only my assigned network, e-mail and Microsoft Office
- not view, use, copy or delete passwords, data, or information to which I am not authorised
- not distribute private information and/or images regarding myself or others
- treat all ICT equipment with care
- report damage, security risks or violations to a teacher or network administrator at the earliest possible opportunity.
- not destroy, damage or alter data or other resources that do not belong to me
- not download or install software onto school PCs or laptops (even if the software licence allows)
- not infringe copyrights by making illegal copies of music, games, or films
- not plagiarize the work of others
- communicate only in ways that are respectful and appropriate
- report threatening or offensive materials, messages or e-mails to a member of staff at the earliest possible opportunity (and NOT share with other students)
- not intentionally access, share, copy or create material that is threatening, offensive, discriminatory, or intended to harass
- not use the school's IT resources to promote materials that are criminal or that violate the school's rules
- not create, send or forward spam e-mail, chain letters, or other mass unsolicited mailings
- not use the school's IT resources to buy, sell, advertise, or otherwise conduct business, unless approved as a school project by a member of the school's senior leadership team
- ensure that my mobile phone is switched off in the school grounds, unless directed to use it by a member of staff. I understand that it will be confiscated if seen.

I accept that the school may view and monitor my on-line activity, my saved files, e-mails, and contributions to web sites.

Signed by parent and student

Appendix C Managed Learning Environment (MLE) Rules

MLE Use (information published on student homepage, visible when students log-in)

I agree that I will not:

- Use another student's password or allow other users to use your password
- Upload, link to, post or send inappropriate, offensive, rude or unpleasant documents, content, e-mails, posts, forum messages or chat contributions.
- Publish, share or distribute any personal information about any user (such as email address, phone number or home address).
- Publish, share or distribute any images of staff or students without their permission.
- Upload, publish or distribute any material where copyright or licence restrictions forbid it (such as music files).
- Engage in any activity which may result in the loss of or damage to another person's work.
- Use obscene, discriminatory or racist language.
- Harass, insult or attack others, directly or indirectly.

Appendix D Phone / Bring Your own Device (BYOD) protocol

This protocol covers use of mobile devices (phones, laptops, tablets etc.) anywhere in the school and on the school grounds and during school visits, field trips, or other offsite activities.

Key stages 3 & 4:

- Y7 – Y11 students may not use a mobile device at any time and for any purpose, except when given specific permission from a member of staff to do so, and then only for the agreed purpose. This includes before and after the school day.

Key stage 5:

- Y12-13 students may not use a mobile device at any time and for any purpose **when on the school premises or on a school-endorsed activity such as a trip**, except when given specific permission from a member of staff to do so, and then only for the agreed purpose. This includes before and after the school day.
- Sixth form students may use laptops or tablets (but not phones) **when on the school premises** for study purposes only, within the Sixth Form common room and study area.

All students:

- **If they have been given permission to use a mobile device within school**, students must log in to the school's Wi-Fi network and turn off their mobile data connection. The school's Internet connection is filtered and monitored. The use of personal mobile data connections within school is expressly forbidden.
- Any form of recording, copying or distribution of audio, video or images of other students or staff using students' mobiles or other electronic devices is strictly forbidden. If students need to take photo / video for a specific school purpose, agreed by a member of staff, they should use a school approved device.
- The school does not provide secure facilities for students to store personal devices and the school cannot be held responsible for any device which is lost, damaged or stolen. The school is not responsible for any damage or data loss even if this has resulted from a permitted activity or via the school's internet connection.
- In allowing any device into school, parents/carers agree that the device may be examined or confiscated (for a reasonable time) by the school and will provide authentication details to facilitate investigations if required.

Appendix E Curriculum and PSHE Overview

Year	PSHE	Computing
7	• Dealing with Bullying and Friendships via the internet / social media • Understand why it's important to have a safe password • Evaluate strength of internet passwords • Discuss why it is important to be a good digital citizen – avoiding giving out private details	• explain what constitutes a "strong" password for an online account • describe a code of conduct • list some of the dangers and drawbacks of social networking sites • list some possible responses to cyberbullying • use a search engine to find information • describe guidelines for keeping their identity secure on the Internet • describe what is meant by identity theft and how to minimize the risks of this • identify a probable phishing email and deal with it appropriately • describe how to minimize the danger of having their computer infected by a virus • describe why the information they find may not be accurate
8	• Safer social networking – including what is appropriate to include and avoid on profile pages • Dangers of internet grooming • Limits on screen time • Acceptable behaviour using message boards / chat rooms /etc	
9	• Using the internet safely • Problems with chat rooms and how to stay safe – what language is appropriate • Cyber bullying and how to respond to it • Digital footprint	• Create and use accounts on Web2.0 sites effectively, including use of Forums, Blogs, Wikis and Cloud Computing • Have strategies to deal with the problem of multiple login names and passwords • Understand issues concerning sharing of personal information online. • Identify common features in digital scams and learn how to deal appropriately with them.

Year	PSHE	Computing
		• Analyse and evaluate information, judging its value accuracy, plausibility and bias • Communicate and exchange information effectively, safely and responsibly • Develop the appropriate understanding to use social networking websites safely.
10	• Developing a digital compass – relative risks of activities on the internet • Sexting • Appropriate relationships using the internet	• Social, cultural and environmental impacts of Computer Science (including social media)
11	• Social Media and Happiness – Addiction / Echo Chambers / "False Positives" • CEOP Exploited – harassment and bullying • Sex and relationships, including internet / pornography angle • Extremism	• Publishing websites via FTP to a webserver (including licencing, copyright and privacy concerns).
KS5	• e-Safety Talk with the Cognus e-Safety lead as a member of Sutton's safeguarding team Teaching e-Safety to lower school • Reinforcement of e-safety messages especially linked to sex and relationships to accommodate students new to Nonsuch in Y12 • Cyber security – e.g., avoiding scams and phishing attacks	

Appendix F **Annual e-Safety Checklist**[i]

- Read the DfE guidance
- Appoint a Designated Safeguarding Officer
- Set up internet filters and monitoring
- Train staff
- Teach age-appropriate e-Safety
- Establish effective e-Safety policies
- Set up clear reporting channels
- Include governors in e-Safety delivery
- Engage with parents

Appendix G **Governors' Checklist**

- Is the governing body involved in the e-Safety policy and practice in school?
- Have all staff read Part 1 of the DfE Keeping Children Safe in Education Guidance?
- Does the school have a Designated Safeguarding Lead?
- Are appropriate filtering and monitoring systems in place?
- Have all staff received e-Safety training and had regular updates?
- Are e-Safety lessons included in the cross-curricular timetable?
- Does the school have effective policies in school which have been issued to all staff?
- Are there clear reporting channels which are understood by pupils and staff?
- Are parents and the wider school community included in e-Safety activities?
- Does the school address online issues related to Online Sexual Abuse, Child Sexual Exploitation and Radicalisation?
- Is the school monitoring and protecting its digital reputation?

[i] www.e-Safetysupport.com