



PLYMOUTH COLLEGE
E-SAFETY POLICY
Including the Early Years Foundation Stage

Last reviewed:	August 2026
Next review date:	August 2027
Responsibility:	Senior Deputy Head

This policy was produced by the E-Safety Committee, which comprises:

STAFF ROLE	NAME
Group Head of Systems and IT, DPO	James Moate
Designated Safeguarding Lead	Beth Field
Head of Boarding	Lee Ilott

Reference Documents / Websites

1. Southwest Grid for Learning (SWGfL) – 360safe: <https://360safe.org.uk/>
2. UK Safer Internet Centre: www.saferinternet.org.uk
3. Plymouth Interagency E-safety Pledge
4. Keeping Children Safe in Education (September 2024)
5. Working Together to Safeguard Children (December 2023)
6. Revised Prevent Duty Guidance for England and Wales (December 2023):
<https://www.gov.uk/government/publications/prevent-duty-guidance>
7. The use of social media for online radicalisation (July 2015):
<https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation>
8. CEOP Think u know: www.thinkuknow.co.uk
9. **UKCIS guidance:** "Sharing nudes and semi-nudes: advice for education settings working with children and young people" (December 2020):
<https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>
10. NSPCC E-Safety incident report (Appendix 3):
<https://learning.nspcc.org.uk/media/1513/esat-briefing-sample-e-safety-incident-report-form.pdf>
11. E-safety incident flow process (Appendix 2):
<https://learning.nspcc.org.uk/media/1512/esat-briefing-what-to-do-if-a-pupil-or-a-teacher-reports-an-e-safety-incident.pdf>
12. Online Safety Act 2023
13. UK General Data Protection Regulation (UK GDPR)
14. Data Protection Act 2018
15. Data Use and Access Act 2025 (DUAA 2025)
16. Information Commissioner's Office (ICO) Guidance: <https://ico.org.uk>

Plymouth College's

- ICT Acceptable Use Policy - for Boarders
- ICT Acceptable Use Policy - for Pupils
- ICT Acceptable Use Policy - for Staff

Contents

1. Introduction and Overview
 2. Education and Curriculum
 3. Expected Conduct and Incident Management
 4. Managing the ICT Infrastructure
 5. Data Security & UK Data Protection Legislation (UK GDPR / DPA 2018 / DUAA 2025)
 6. Equipment and Digital Content
- Appendices

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the community at Plymouth College ("the School") with respect to the use of electronic communication technologies.
- safeguard and protect the children and staff of Plymouth College.
- assist School staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practices.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse, such as cyberbullying and the dangers of radicalisation, which are cross-referenced with the Safeguarding & Child Protection and Anti-Bullying Policies.
- ensure that all members of the School community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

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

Content

- inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language); substance abuse
- radicalisation and extremism propaganda
- lifestyle websites, for example, pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: How to check the authenticity and accuracy of online content
- inappropriate sharing or use of personal data

Contact

- grooming
- cyber-bullying in all forms
- radicalisation
- identity theft (including 'fraping' - hacking social media profiles) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- Sharing nudes and semi-nudes (sending and receiving of personally intimate images) — also referred to in statutory guidance as 'youth-produced sexual imagery'. Staff should follow the UKCIS guidance 'Sharing nudes and semi-nudes: advice for education settings' (December 2020) when responding to incidents.
- extremist views
- copyright (little care or consideration for intellectual property and ownership, such as music and film)

- ensuring all information is stored, kept and distributed in line with UK data-protection legislation — comprising the UK GDPR and the Data Protection Act 2018, as extended by the Data Use and Access Act 2025 (DUAA).
- use of generative AI tools (such as large language models and image generators) which may expose pupils to misinformation, inappropriate content, or data privacy risks.

Scope

This policy applies to all members of the Plymouth College community (including staff, students, volunteers, parents/guardians / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of School.

The Education and Inspections Act 2006 empowers school Heads to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, radicalisation or other e-safety incidents covered by this policy, which may take place outside of the school, but be linked to membership of the school. The Education Act increased these powers with regard to the searching for and of electronic devices and deletion of data. Action will be taken over issues in accordance with the School's Behaviour Management Policy.

The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/guardians/carers of incidents of inappropriate e-safety behaviour that take place out of School.

Role	Key Responsibilities
Head	• takes overall responsibility for e-safety provision • ensures the school-based ICT network uses an approved, filtered Internet Service, which complies with current statutory requirements • is responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • is aware of procedures to be followed in the event of a serious e-safety incident • receives updates from the E-Safety Coordinator on significant incidents • ensures there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. Head of Systems & IT)
Bursar	• takes overall responsibility for financial data governance and data security within the School's financial and administrative systems • ensures that appropriate financial data handling procedures comply with data protection requirements
Data Protection Officer (DPO)	• takes overall responsibility for compliance with UK GDPR, Data Protection Act 2018, and DUAA 2025 • advises the School on data protection obligations and e-safety data handling requirements

	• liaises with the ICO and acts as the first point of contact for data protection matters • maintains the Data Breach Register and oversees incident response • approves Data Protection Impact Assessments (DPIAs) for new technologies and high-risk processing
Designated Safeguarding Lead	• takes day-to-day responsibility for e-safety issues • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-safety education is embedded across the curriculum • liaises with the school ICT technical staff • communicates regularly with SMT and the designated e-safety committee to discuss current issues, review incident logs and filtering • ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • ensures that a cyber-bullying incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • is regularly updated on e-safety issues and legislation, and is aware of the potential for serious child protection issues to arise from: - o sharing of personal data - o access to illegal/inappropriate materials - o inappropriate online contact with adults/strangers - o potential or actual incidents of grooming and radicalisation - o cyber-bullying and use of social media
Head of Marketing & Communications	• takes responsibility for the taking and publishing of photographic and video material relating to the school • advises colleagues on correct procedures for use of digital imagery • ensures School social media forums are moderated for appropriate content
LAB / E-safety LAB	• ensure the School follows all current e-safety advice to keep the children and staff safe, • approve the E-Safety Policy, and review the effectiveness of the policy. This will be carried out by the LAB's designate. A member of the Governing Body has taken on the role of E-Safety LAB. • The role of the E-Safety LAB will include: - o annual review with the E-Safety Coordinator, including cyberbullying logs, filtering and policies

Computer Science Curriculum Leader (HoD)	• oversees the delivery of the e-safety element of the Computer Science curriculum • reports to the Head of Systems & IT and DSL regularly about curriculum training.
Head of Systems & IT / technician	• takes day-to-day responsibility for e-safety issues • enforces all school policies across all systems. • ensures that users may only access the School's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • ensures that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date) • ensures the security of the school's ICT system • ensures that access controls/encryption exist to protect personal and sensitive information held on School-owned devices, and that - o the school's policy on web filtering is applied and updated on a regular basis - o they keep up to date with the School's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant - o the use of the network / Intranet / remote access/email is monitored in order that any misuse / attempted misuse can be reported to the E-Safety Coordinator / Head for investigation/action / sanction • ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • keeps up-to-date documentation of the School's e-security and technical procedures
Intranet Coordinator	• ensures that all data held on pupils on the Intranet is adequately protected • takes responsibility for the taking and publishing of photographic and video material relating to the school
Data Manager	• ensures that all data held on pupils on the School office machines has appropriate access controls in place
Teachers	• embed e-safety issues in relevant aspects of the curriculum and other school activities • supervise and guide pupils carefully when engaged in learning activities involving online technology (including extracurricular and extended school activities if relevant) • ensure pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content, such as copyright laws

	• know the procedures following an incident of cyberbullying, inappropriate use of the internet or suspicion of radicalisation.
All staff	• are aware of their responsibilities in respect to UK GDPR and act accordingly • read, understand and help promote the School's e-safety policies and guidance • read, understand, sign and adhere to the School Acceptable Use Policy for Staff • are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices, monitor their use and implement current school policies with regard to these devices • report any suspected misuse or problem to the E-Safety Coordinator • maintain an awareness of current e-safety issues and guidance, e.g. through CPD • know the procedures following an incident of cyberbullying, inappropriate use of the internet or suspicion of radicalisation. • model safe, responsible and professional behaviours in their own use of technology • ensure any digital communications are on a professional level and only through School-based systems, never through personal accounts, e.g. email, text, mobile phones, etc.
Pupils	• read, understand, sign and adhere to the Pupil Acceptable Use Policy • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • understand the importance of reporting abuse, misuse or access to inappropriate materials • know what action to take if they or someone they know feels worried or vulnerable when using online technology. • know and understand the school policy on the use of mobile phones, digital cameras and hand-held devices. • know and understand the school policy on the taking/use of images and on cyberbullying. • 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, if related to their membership of the School • take responsibility for learning about the benefits and risks of using the Internet, social media sites and other technologies both in School and at home • help the School in the creation/review of e-safety policies • know their rights and responsibilities for sharing data

Parents/guardians / carers	• support the School in promoting e-safety and endorse the Pupil Acceptable Use Policy • read and understand the pupil ICT AUP and promote it with their child/ren • consult with the School if they have any concerns about their child/ren's use of technology
External groups (individuals or organisations)	• will sign an Acceptable Use Policy prior to using any systems, equipment, or the Internet within the school

Communication

The policy will be communicated to staff, pupils and parents in the following ways:

- Policy to be posted on the school website;
- Policy to be part of the school induction pack for new staff;
- Acceptable use agreements are distributed to all pupils and staff for reading, understanding and signing at the start of each year;
- Acceptable use agreements to be held in Admin;
- Should this policy be updated we will email a copy to all Plymouth College members; newly actioned points will be highlighted and take immediate effect upon receipt.

Handling complaints

- The School will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies, mobile networks 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.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
 - o Interview by Head of Year or Deputy Head
 - o Informing parents or carers
 - o Discipline sanctions and device confiscation in accordance with the School's Behaviour Management Policy
 - o Removal of Internet or computer access for a period
 - o Referral to the Police if deemed serious enough
- Our E-Safety Coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Head.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school's child protection procedures.
- All incidents of cyberbullying are recorded on the central bullying file by the Senior Deputy Head.

- All data security concerns should be reported to privacy@plymouthcollege.com

Review and Monitoring

- The E-Safety Policy is referenced from within other School policies: Safeguarding & Child Protection Policy; Anti-Bullying Policy; Behaviour Management Policy; Pupils' Personal Development Policy; Privacy Notice; Data Breach Policy; and Record Keeping Policy.
- The School has an E-Safety Coordinator who will be responsible for document ownership, review and updates.
- The E-Safety Policy will be reviewed annually or when significant changes occur in legislation or technology affecting e-safety and data protection (for example, amendments to the UK GDPR, the Data Protection Act 2018 or the Data Use and Access Act 2025).
- The E-Safety Policy has been written by the School E-Safety Committee and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the Policy and it has been agreed by the SMT, E-Safety Committee and approved by LABs. All amendments to the School E-Safety Policy will be published to all members of teaching staff.
- The School will maintain an auditable record of each policy review, in line with the accountability principle under UK GDPR (Article 5(2)), including details of participants, version history, and any decisions regarding e-safety data handling. Staff will be required to confirm that they have read and understood each updated version

2. Education and Curriculum

Pupil e-safety curriculum

This school

- has a clear, progressive e-safety education programme as part of the PSHE curriculum / Computer Science curriculum. It is built on SWGfL (South West Grid for Learning Trust Ltd) guidance. This covers a range of skills and behaviours appropriate to age and experience, including:
 - o understand the impact of cyberbullying, sharing of intimate images, and trolling and know how to seek help if affected by any form of online bullying;
 - o know how to report any abuse, including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button;
 - o understand why and how some people will 'groom' young people for sexual reasons;
 - o STOP and THINK before they CLICK;
 - o be aware that terrorist organisations are trying to radicalise and recruit young people through an extensive use of social media and the internet, and be resilient to this;

- o understand acceptable behaviour when using online communication, i.e. be polite, no bad or abusive language or other inappropriate behaviour that might upset or offend; keep personal information private;
 - o understand why they must not post pictures or videos of others without their permission;
 - o understand why online 'friends' may not be who they say they are, and to understand why they should be careful in online environments;
 - o understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned on appropriate privacy settings;
 - o have strategies for dealing with receipt of inappropriate materials;
 - o know not to download any files – such as music files – without permission;
 - o understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
 - o develop a range of strategies to evaluate and verify information before accepting its accuracy, including understanding how generative AI tools can produce plausible but inaccurate content;
 - o be aware that the author of a website may have a particular bias or purpose, and develop skills to recognise what that may be;
 - o know how to narrow down or refine a search;
 - o understand how search engines work and to understand that this affects the results they see at the top of the listings;
 - o understand that mobile device content can be addictive, and the School will encourage periods of time when the use of these devices is prohibited.
 - o understand the risks associated with the use of generative AI tools, including data privacy, misinformation, plagiarism, and the potential for AI-generated content to be harmful or deceptive.
- acknowledges that pupils may access the Internet through their own devices on mobile networks – our School strategy is to educate pupils about the dangers of using unfiltered access rather than the wholesale prohibition of personal devices on the School site.
 - plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
 - will remind students about their responsibilities through an ICT Acceptable Use Policy, which every student will sign.
 - ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
 - ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.
 - ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, an age-appropriate way. This may include risks in pop-ups, buying online, and online gaming/gambling.

Staff and LAB training

This school

- makes training available to staff on e-safety issues and the School's e-safety education program through INSET and staff briefings.

- provides, as part of the induction process, all new staff with information and guidance on the e-safeguarding policy and the School's Acceptable Use Policies.
- provides training on UK GDPR and data security.

Parent awareness and training

This school

- makes parents aware of the pupil Acceptable Use Policy to ensure that principles of e-safe behaviour are made clear.
- delivers occasional e-safety awareness presentations at school for parents.
- provides information about national support sites for parents.

3. Expected Conduct and Incident Management

Expected conduct

In this school, all users

- are responsible for using the school ICT systems and their own devices in accordance with the relevant Acceptable Use Policy, which they will be expected to sign before being given access to school systems. Should any urgent changes be made to this policy, members will be notified and changes will take immediate effect upon receipt.
- need to understand the importance of misuse or access to inappropriate materials, and be aware of the consequences.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials to the Senior Deputy Head or Head.
- should 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, if it affects the School in any way.
- will be expected to know and understand the school policies on the use of mobile phones, digital cameras, handheld and wearable devices. They should also know and understand School policies on the taking/use of images and on cyber-bullying (within Anti-Bullying Policy).
- are expected to ensure the data they are responsible for is secure and to report any potential breaches to breach@plymouthcollege.com.

Staff

- are responsible for reading the School's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, handheld and wearable devices.

Students/Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- should understand and endorse the School's pupil ICT Acceptable Use Policy at the time of their child's entry to the school.
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

In this school

- there is strict monitoring and application of the E-Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely a need to apply sanctions.
- all members and their wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the School's behaviour management system.
- support is actively sought from other agencies as needed (e.g. the local authority and SWGfL, UK Safer Internet Centre helpline) in dealing with e-safety issues.
- monitoring and reporting of e-safety incidents takes place and contributes to developments in policy and practice in e-safety within the School. The records are reviewed/audited and used to improve the e-safety policy in the future.
- parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- we will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- we will contact the police and Plymouth Prevent duty officer if we suspect one of our pupils to be involved in radicalisation.
- if data security is breached, we have a Data Breach Policy in place (held on the intranet).

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This school

- uses the Sophos filtering system, which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status. Data logs are only kept for 6 months.
- ensures network safety through the use of Sophos Endpoint Security, etc. and network setup so staff and pupils cannot install executable files without permission.
- blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
- only unblocks other external social networking sites for specific purposes / Internet Literacy lessons.
- has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- ensures all staff and students have signed an Acceptable Use agreement form and understand that they must report any concerns.
- requires staff to preview websites beforehand and direct students to age/subject appropriate websites; plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required, e.g. Yahoo for Kids, Google Safe Search.
- is vigilant when conducting 'raw' image search with pupils, e.g. Google image search.
- informs all users that Internet use is monitored.
- informs staff and students that they must report any failure of the filtering systems directly to the Head of Systems and IT.
- makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse, through staff meetings and teaching programmes.
- provides advice and information on reporting offensive materials, abuse/bullying, etc. to pupils, staff and parents.
- immediately refers any material it suspects is illegal to the police.

Network management (user access, backup)

This school

- uses individual, audited log-ins for all users.
- uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services.
- uses teacher 'remote' management control tools for controlling workstations.
- Ensures all data within the School is stored in a way that conforms to the UK data protection requirements.

To ensure the network is used safely, this school:

- ensures staff read and sign that they have understood the School's E-Safety Policy. Following this, they are set up with Internet, email access and network access. Online access to the service is through a unique, audited username and password. We also use the same username and password for access to our School's network.
- ensures staff access to the school's management information system is controlled through a separate password for data security purposes.
- provides pupils with an individual network login username. From Year 7, they are also expected to use a personal password.
- ensures all pupils have their own unique username and password, which gives them access to the Internet and the intranet, and all pupils have their own school-approved email account.
- makes clear that no one should log on as another user and makes clear that pupils should never be allowed to use teacher and staff logins, as these have far fewer security restrictions and inappropriate use could damage files or the network.
- has set up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- requires all users to always log off/lock when they have finished working or are leaving the computer unattended.
- requires all users to log off any unattended machines and then log on as themselves.
- has set up the network so that student users cannot download executable files/programmes.
- has blocked access to music/media download or shopping sites – except those approved for educational purposes.
- makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained and up-to-date, and the School provides them with a solution to do so.
- makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities and that they notify the school of any "significant personal use". Staff must also be aware that the device's activity can be logged and reviewed.
- has integrated curriculum and administration networks, but access to the iSAMS system is set up so as to ensure staff users can only access modules related to their role.
- ensures that access to the School's network resources from remote locations by staff is restricted and access is only through school-approved systems: e.g. teachers access their area / a staff shared area for planning documentation via Remote Desktop/Ranger Portico.
- does not allow any outside agencies to access our network remotely except where there is a clear professional need, and then access is restricted and is only through approved systems; e.g. technical iSAMS Support.
- provides pupils and staff with access to content and resources through the intranet, which staff and pupils access using their username and password.
- makes clear the responsibilities for the daily backup of iSAMS and finance systems and other important files.
- has a clear disaster recovery system in place for critical data that includes a secure, remote backup of critical data that complies with external audit requirements.
- follows ISP advice on Local Area and Wide Area security matters, and firewalls and routers have been configured to prevent unauthorised use of our network.

- has a wireless network which has been secured to an industry-standard Enterprise security level /appropriate standards suitable for educational use.
- reviews the School ICT security systems regularly.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff and pupils have their own unique username and private passwords to access the school systems. Staff and pupils are responsible for keeping their passwords private.
- Staff and pupils are required to use strong passwords as defined by NCSC (National Cyber Security Centre) guidance for access to the computer network.
- User passwords are set not to expire. Research and NCSC guidance have found that users gradually pick weaker passwords the more frequently they are asked to change them. Instead, a high-strength requirement at creation is enforced, supported by multi-factor authentication (MFA) on systems that handle personal data.

Email

This school

- provides staff with an email account for their professional use and makes clear that personal email traffic should be through a separate account.
- requires staff to use school systems only when contacting pupils and parents.
- does not publish personal email addresses of pupils or staff on the school website. Staff must ensure that if personal email addresses are used, they are put in the BCC section of the email and not in a mail group/list.
- will contact the Police if one of its staff or pupils receives an email that it considers is particularly disturbing or breaks the law.
- will ensure that email accounts are maintained and up-to-date, removing unnecessary messages/accounts.
- reports messages relating to or in support of illegal activities to the relevant authority, and if necessary, to the Police.
- knows that spam, phishing and virus attachments can make emails dangerous. A number of technologies are used to help protect users and systems in the School, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Pupils

- We use Gmail email software with pupils.
- Pupils are introduced to and use email as part of the CS scheme of work.
- Pupils are taught about the safety and 'netiquette' of using email both in School and at home, i.e. they are taught:
 - o not to give out their email address unless it is part of a school-managed project or to someone they know and trust, and sharing is approved by their teacher or parent/carer;

- o that an email is a form of publishing where the message should be clear, short and concise;
- o that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school-headed paper;
- o they must not reveal private details of themselves or others in email, such as address, telephone number, etc.;
- o to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- o that they should think carefully before sending any attachments;
- o that embedding adverts is not allowed;
- o that they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
- o not to respond to malicious or threatening messages;
- o not to respond to any propaganda that may be linked to radicalisation;
- o not to delete malicious or threatening emails, but to keep them as evidence of bullying;
- o not to arrange to meet anyone they meet through email without having discussed with an adult, and to take a responsible adult with them;
- o that forwarding 'chain' email letters is not permitted.
- Pupils sign the Pupil ICT Acceptable Use Policy, and boarding pupils sign an additional boarding AUP to say they have read and understood the e-safety rules, including email, and understand how any inappropriate use will be dealt with. If changes are required between academic years, students will receive an email with the new agreement, and the updates will take immediate effect upon receipt.

Staff

- only use the school email systems for professional purposes.
- know that email sent to an external organisation must be written carefully (and may require authorisation), in the same way as a letter written on school-headed paper. That it should follow the School 'house-style':
 - o the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
 - o the sending of chain letters is not permitted;
 - o embedding adverts is not allowed;
- sign our School Staff ICT Acceptable Use Policy to say they have read and understood the e-safety rules, including email and understand how any inappropriate use will be dealt with. If changes are required between academic years, staff will receive an email with the new agreement and the updates will take immediate effect upon receipt.

School website

- The Head takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: Head of Marketing, Prep Registrar, IT Manager and other authorised administrators;

- Most material is the School's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the website is the School address, telephone number and we use a general email contact address, e.g. mail@plymouthcollege.com. Home information or personal email identities will not be published.

Intranet

- Uploading of information on the school's intranet is shared between different staff members according to their responsibilities.
- Photographs and videos uploaded to the School's intranet will only be accessible by members of the school community and are protected.
- Photographs should only be uploaded if the parent (below year 9) or pupil (year 9 and above) has given permission.

Social networking

- Teachers are instructed not to run personal social network spaces for student use, but to use the school's preferred system for such communications; this includes setting up departmental social networking.
- The School's preferred system for social networking will be maintained in adherence with the Staff Social Media Policy.
- School staff will ensure that in private use of their own social media sites:
 - o they will not be friends with existing students;
 - o no reference will be made to students or School staff;
 - o they do not engage in online discussion on personal matters relating to members of the School community;
 - o their personal opinions are not attributed to the School;
 - o their security settings on personal social media profiles are set up to minimise the risk of loss of personal information.

Video Conferencing

- The School uses approved video conferencing platforms (currently Microsoft Teams or Google Meet) for secure remote communication. All video conferencing activity is conducted through School-approved accounts only. Personal or consumer video conferencing accounts must not be used for School business or communication with pupils or parents.

CCTV

- Plymouth College has CCTV as part of its site surveillance for staff and student safety. No recordings will be revealed publicly without permission, except where disclosed to the Police as part of a criminal investigation.
- All CCTV cameras are logged in a report called the Impact Assessment, which details the purpose of installation, who has access to the recordings and when they will be deleted. This report is maintained by the Infrastructure Manager and is updated any time a CCTV camera is installed or when there is a change.

5. Data Security & UK Data Protection Legislation (UK GDPR / DPA 2018 / DUAA 2025)

Strategic and operational practices

At this school

- Plymouth College is the School's Data Controller under the UK GDPR and Data Protection Act 2018. The Data Controller is the institution, not an individual; the Bursar and Data Protection Officer (DPO) are responsible for discharging data protection obligations on behalf of the School.
- The Head of Systems and IT serves as the Data Protection Officer (DPO) for compliance and reporting purposes.
- staff are clear who the key contact(s) are for key school information.
- staff know to report any incidents where data protection may have been compromised.
- all staff are DBS checked and records are held in one central record (SCR).
- all staff and pupils sign an ICT Acceptable Use Policy form. This makes clear staff's responsibilities with regard to data security, passwords and access. There is a system in place to monitor who has signed.
- there is an approved and secure remote access solution so staff can access sensitive and other data from home, without the need to take data home.
- staff with access to setting up usernames and passwords for email, network access and intranet access are working within the approved system and follow the security processes required by those systems.
- staff are reminded and should undertake regular housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- staff are provided with encrypted memory sticks which they must use if removing digital files containing personal data from the site.
- staff using personal devices to work from home must ensure their devices have an up-to-date antivirus installed and no inbuilt firewall controls have been removed.

The School ensures that any data-processing, transfer or access to third-party digital services is covered by a Data Sharing Agreement or Data Processing Agreement (as required under Article 28 UK GDPR). The School keeps a register of these arrangements and audits them annually to confirm compliance with UK GDPR, DPA 2018 and DUAA 2025 requirements for lawful basis, security and data minimisation.

In line with UK GDPR Article 22 and the accountability principle, any deployment of AI or automated decision-making tools involving personal data must undergo a Data Protection Impact Assessment (DPIA) and receive DPO approval before use. Individuals retain the right to human review of automated decisions and to opt out where appropriate.

Technical Solutions

- Staff have secure areas on the network to store sensitive documents or photographs.
- Staff are required to log-out of systems when leaving their computer. There is an enforced lock-out after 15 minutes of idle time.
- Pupil CTF data files are transferred to other schools using the DfE's current approved secure transfer mechanism. (Note: the DfE S2S service was decommissioned in 2023 and has been replaced; staff should confirm the current approved method with the Head of Systems & IT.)
- All servers are in lockable locations and managed by DBS-checked staff.
- Back-ups are encrypted. No back-up media leaves the site.
- The School complies with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and gets a certificate of secure deletion for any server that once contained personal data.
- Paper-based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

6. Equipment and Digital Content. School / Personal mobile phones and mobile devices

Mobile Phone use – please refer to the School's Mobile Phone Policy

Asset disposal

- Details of all School-owned hardware will be recorded in a hardware inventory.
- Details of all School-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for all items disposed of.
- All redundant equipment that may have held personal data will have the storage media removed prior to disposal. Alternatively, if the storage media has failed, it will be physically destroyed.
- Disposal of any equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the Environment Agency website.

Plymouth Inter-Agency E-safety Pledge

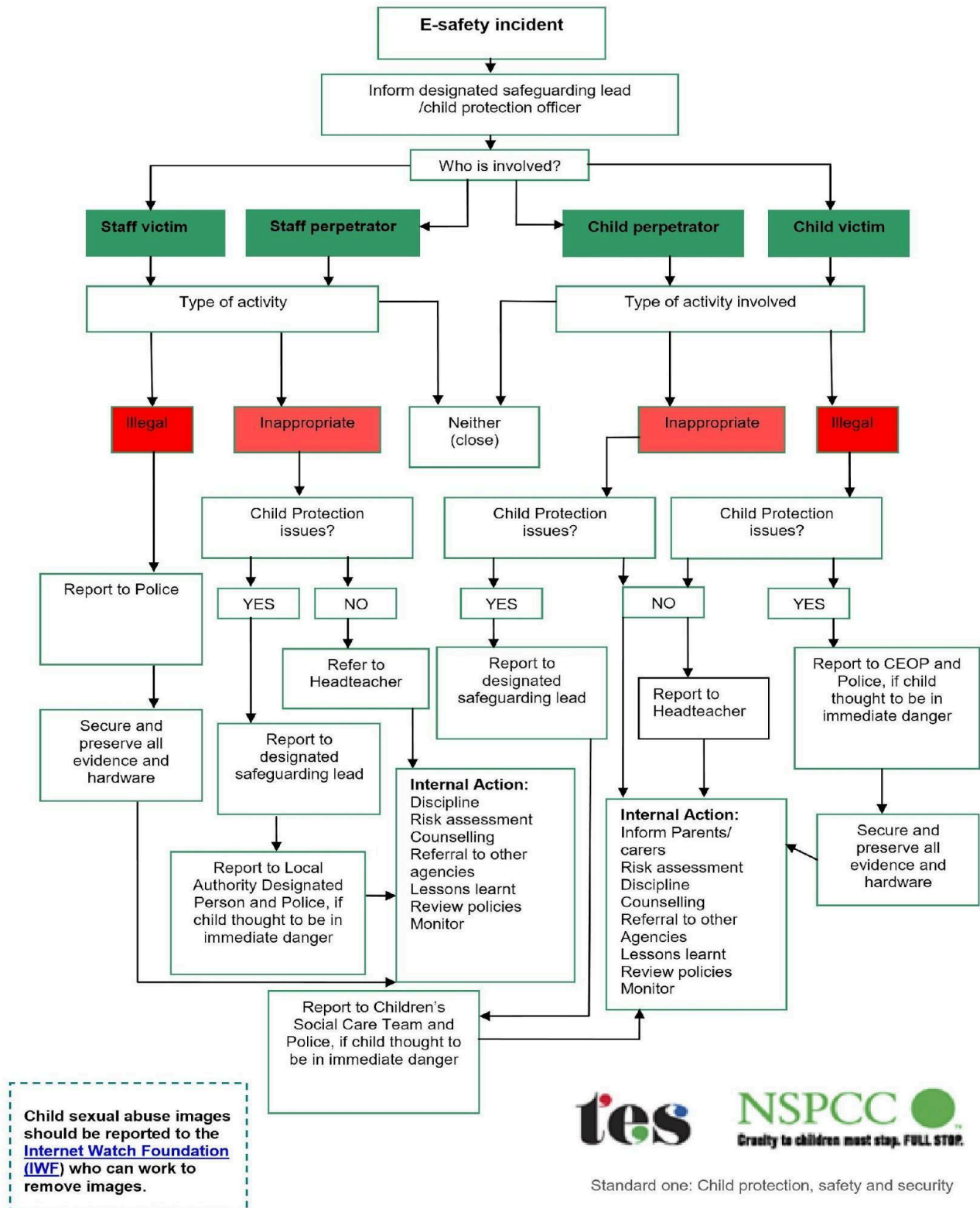
The Plymouth Safeguarding Children Partnership and our partner agencies are committed to ensuring that children and young people are safeguarded while using Information and Communication Technology (ICT).

To ensure this commitment **We Pledge** the following:

1. The advantages and positive aspects of using ICT will be continually promoted among children and young people.
2. Our agency will have its own Acceptable Use Policy (AUP), which will be kept up to date as technology, and its use, develops and which will be promoted among the agency's staff.
3. Our agency will have a member of staff designated as an E-safety Officer, who is fully conversant with children and young people's safe use of ICT and responsible for ensuring that all necessary policies and procedures, and safeguarding measures, are in place.
4. The AUP will be promoted and made available to children and young people using ICT and their parents/carers.
5. Electronic safeguards, appropriate to the setting, will be put in place, in line with guidance from the Plymouth Safeguarding Children Partnership (www.plymouthscb.org.uk) and the UK Council for Internet Safety (UKCIS), and will be updated regularly. Reports generated from these will be used to confirm adherence to AUPs.
6. Children and young people using ICT within agencies will be made aware of their online rights, and the potential risks and dangers.
7. Children and young people will be equipped with the knowledge and encouraged to take responsibility for keep themselves safe whilst using ICT, in line with the agency's Acceptable Use Policy.
8. Our agency will promote Peer Mentoring (sub-committee of School Council) as a method for children and young people to keep each other safe online.
9. Relevant members of staff will be made aware of safeguarding issues for children and young people using ICT, and key staff, including those who supervise the use of ICT, will be fully informed about its safe use.
10. Procedures will be in place to ensure that action will be taken when there are concerns that the ICT equipment has been used by users, staff or members of the public to abuse others.
11. Young people, parents/carers and members of the public will be made aware of how to report concerns / who to speak to if they feel worried about, or are aware of, the use of ICT to abuse others.
12. Young people will be consulted about, and involved in, the implementation of our Pledge.

Standard one: Child protection, safety and security

What to do if a pupil or a teacher reports an e-safety incident





Sample e-safety incident report form		
Name of school:		
Your details		
Your name:	Your position:	Date and time of incident:
Details of e-safety incident		
Date and time of incident:		
Where did the incident occur? i.e. at school or at home:		
Who was involved in the incident?		
Child/young person	☐	Name of child:
Staff member/ volunteer	☐	Staff/volunteer name:
Other	☐	Please specify:
Description of incident (including IP addresses, relevant user names, devices and programmes used)		
Action taken:		
☐	Incident reported to head teacher/senior manager	
☐	Advice sought from Safeguarding and Social Care	
☐	Referral made to Safeguarding and Social Care	
☐	Incident reported to police	
☐	Incident reported to Internet Watch Foundation	
☐	Incident reported to IT	
☐	Disciplinary action to be taken	
☐	E-safety policy to be reviewed/amended	
☐	Other (please specify)	
Outcome of investigation:		