DEVONPORT HIGH SCHOOL FOR GIRLS

ONLINE SAFETY AND IT SECURITY POLICY

(Including Student and Staff Acceptable Use Policy Agreements)

Named persons: Ruth Morgan

Category: School

Review: Annually (or as significant changes occur)

Date to be reviewed: Autumn 2026

This policy has been reviewed with regard to the work/life balance of staff.

Ratified on behalf of Trustees by the Head Teacher: 11/07/2025

Contents

Appendices:

1. Introduction and Overview

Please read alongside the following linked policies:

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

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Devonport High School for Girls regarding the use of school digital technologies.
- safeguard and protect the students and staff of Devonport High School for Girls.
- assist school staff working with students to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- 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, which are cross-referenced with other school 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 students.

Scope

This policy applies to all members of Devonport High School for Girls (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of Devonport High School for Girls.

The Education and Inspections Act 2006 empowers Head Teachers 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, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parent/carers of individuals involved in inappropriate Online Safety behaviour that take place out of school.

Communication

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

- Policy to be posted on the school website and shared staff area on the school network.
- Policy to be part of school induction pack for new staff.
- Acceptable Use Agreement discussed with students at the start of each year.
- Acceptable Use Agreement to be issued to whole school community, usually on entry to the school.
- Signed Acceptable Use Agreement is held by ICT for students and in staff personnel files.

Handling complaints

- The school will take all reasonable precautions to ensure Online Safety through robust filtering and monitoring, however, owing to the international scale and linked nature 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.
- Staff and students are given information about infringements in use and possible responses.
- Our DSL will act as a first point of contact for any complaint in this area. Any complaint about staff misuse is referred immediately to the Head Teacher.
- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy; complaints related to child protection are dealt with in accordance with school child protection procedures.

Review and Monitoring

- The Online Safety policy is referenced from within other school policies.
- The school has a team monitoring Online Safety (roles and responsibilities of this team are outlined in the appendices) and the DSL/ Assistant Head Teacher/Designated Safeguarding Lead will be responsible for document ownership, review and updates.
- The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The Online Safety policy has been written by the school's Head Teacher and online safety team 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 Senior Leadership Team (SLT) and approved by Trustees. This policy is reviewed annually by Trustees and Staff.

2. Education and Curriculum

Student Online Safety curriculum

This school:

- has a clear, progressive Online Safety education programme as part of the Computing curriculum/PSHEE curriculum. It is built on South West Grid for Learning (SWGfL) and national guidance on online safeguarding. This covers a range of skills and behaviours appropriate to age and experience, including:
    - to STOP and THINK before they CLICK.
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy.
    - to recognise and question content generated by artificial intelligence, including identifying signs of deepfakes or misinformation.
    - to understand how generative AI tools (e.g. ChatGPT, image generators) work, including their limitations, potential biases, and responsible use.
    - to critically evaluate AI-generated content for authenticity, accuracy, and appropriate context.
    - to be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be.
    - to know how to narrow down or refine a search.
    - to understand how search engines work and to understand that this affects the results they see at the top of the listings.
    - to understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
    - to 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 privacy settings.
    - to understand why they must not post pictures or videos of others without their permission.
    - to know not to download any files – such as music files - without permission.
    - to have strategies for dealing with receipt of inappropriate materials.
    - to understand why and how some people will 'groom' young people for sexual reasons or to radicalise them with extremist views.
    - to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - to 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/carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

This school:

- 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 end-user Acceptable Use Agreement which every student will sign, signage displayed in computer suites and presented at user logon.
- 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 students 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 students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include: risks in pop-ups, buying on-line, on-line gaming/gambling.

Staff training

This school:

- ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection (see Data Protection Policy).
- makes training available to staff on Online Safety issues via our Safeguarding training programme.
- provides, as part of the induction process, all new staff [including ITT students on placement] with information and guidance on the Online Safety policy and the school's Acceptable Use Policy Agreements.
- includes awareness training on the ethical and pedagogical implications of AI tools, including how students may use them, how to guide responsible use, and how to identify misuse (e.g., AI-assisted plagiarism or inappropriate content generation).

Parent/carer awareness and training

This school:

- runs a rolling programme of advice, guidance and training for parents/carers, including:
    - we share the Acceptable Use Policies with new parents/carers, to ensure that principles of e-safe behaviour are made clear.
    - information leaflets.
    - suggestions for safe Internet use at home.
    - provision of information about national support sites for parents/carers.

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

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.
- AI-generated fake news, deepfake videos, and manipulated media.
- Inappropriate or harmful content produced by or shared through generative AI tools.

Contact

- Grooming – sexual and radicalisation.
- Cyber-bullying in all forms.
- Identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords.
- Use of AI chatbots for grooming, coercion or impersonation.

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)).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).
- Use of AI to plagiarise content or submit misrepresented schoolwork.
- Creation and distribution of non-consensual AI-generated imagery or offensive content.

Commerce

- Online gambling
- Advertising
- Phishing scams
- Finance scams
- Online transactions
- Targeted advertising and scams via AI-personalised content.

4. Prevent Duty and Online Safety

We understand the risks posed to our students of on-line radicalisation as the amount of terrorist and extremist content on-line grows daily. Many such groups use the internet as a propaganda tool. Since 2010 the Counter Terrorism Internet Referral Unit (CTIRU) has reduced extremist material available on the Internet by taking down over 310,000 pieces of terrorist content, including right wing and Islamic terrorism.

To combat the threat of on-line radicalisation of our students we adopt practices in line with the Prevent Duty to ensure those in our care are not drawn into terrorism. We use SWGfL filtering and safety systems as well as NetSupport DNA which forms part of the Core Service and ensures that any attempt to access content on the Internet Watch Foundation (IWF)/Child Abuse Image Content (CAIC) list as well as online terror content is blocked as it is illegal.

Both lists are proactively monitored and if there is any attempt made, on the South West Grid connection, SWGfL alerting system is activated and the intelligence is passed to the police. SWGfL has a seconded police officer and arrangements in place with other police forces to deal with the intelligence appropriately.

Using an advanced filtering system we can filter based on an individual or specific group basis (e.g. year 7, Sixth form). We also obtain reports on search terms that have been used by students using Netsupport DNA which enables us to be more pro-active in protecting them online – these alerts are directly monitored by the DSL.

5. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school digital technologies in accordance with the relevant Acceptable Use Agreement which they will be expected to sign before being given access to school systems.
- 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 threats and cyber security or access to inappropriate materials and know how to do so.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.

Staff:

- are responsible for reading and abiding by the school's Online Safety policy and using the school digital technologies accordingly, including the use of mobile phones and hand-held devices.
- must model and encourage responsible use of AI tools, including educating students on critical evaluation of AI-generated content, and safeguarding against misuse.

Students:

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations, including benefits and risk with engaging AI.
- should understand the ethical use of generative AI technologies, including transparency when AI tools are used in schoolwork, and avoidance of using AI to deceive, plagiarise, or impersonate others.

Parents/carers:

- should provide consent for students to use the Internet, as well as other technologies, as part of the Online Safety Acceptable Use Agreement at the time of their child's entry to the school;
- should know and understand what the 'rules of appropriate use' are and what responses result from misuse.
- Should be vigilant with their child's online safety and report safeguarding concerns working collaboratively with the DSL as appropriate.

Incident Management

In this school:

- there is strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of responses, though the attitudes and behaviour of users are very positive and there is rarely need to apply responses.
- we recognise that the school will need to deal with incidents including those involving misuse of generative AI, such as generating offensive or harmful content, impersonation using deepfake media, or use of AI to plagiarise academic work, that more likely will involve inappropriate rather than illegal misuse. Incidents are dealt with as soon as possible in a proportionate manner, members of the school community are aware that incidents are always dealt with. Incidents of misuse will be dealt with through our normal behaviour/disciplinary procedures.
- all members and its 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 escalation processes.
- support is actively sought from other agencies as needed (e.g. SWGfL, UK Safer Internet Centre helpline, Police and Social Care as appropriate) in dealing with Online Safety issues.
- monitoring and reporting of Online Safety incidents takes place and contributes to developments in policy and practice in Online Safety within the school.
- parents/carers are specifically informed of Online Safety incidents involving young people for whom they are responsible.
- we will contact the Police if one of our staff or a student is found / suspected of having illegal materials or engaging with illegal online activities or receives an online communication that we consider is disturbing or breaks the law, or if the creation or sharing of malicious synthetic media (e.g. AI-generated explicit or defamatory content) is suspected.

Other Incidents

- It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process (in most situations the Deputy Head Teacher, Assistant Head Teacher/Designated Safeguarding Lead and Head Teacher). This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the Head Teacher working with DSL will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Materials should not be viewed, printed, shared or forwarded. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- **Isolate the computer or device in question as best you can. Any change to its state may hinder a later police investigation.**

- It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the senior leaders group for evidence and reference purposes.

6. Managing the infrastructure

Internet access, security (virus protection) filtering and monitoring

This school:

- has the educational filtered secure broadband connectivity through the SWGfL and so connects to the 'private' National Education Network.
- uses the RM Safety net 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.
- uses user-level filtering where relevant, closing down or opening up options appropriate to the age/stage of the students.
- will routinely create reports based on searches made by groups or individual students.
- ensures network health through use of anti-virus software etc. and network security so staff and students cannot download executable files.
- will minimise risk of harm to students, staff and the school by ensuring that personal information is not published
- will provide training including: acceptable use; social media risks; checking of settings; cyber security; data protection; reporting issues.
- uses secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site.
- 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 student access to music downloads or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- works in partnership with the SWGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas, e.g. NetSupport DNA is utilised to monitor key words used in documents and searches in all languages spoken within the school community.
- ensures all staff and students have signed an Acceptable Use Agreement and understand that they must report any concerns.
- requires staff to preview websites before use [where not previously viewed or cached] and direct students to age/subject appropriate web sites; plans the curriculum context for Internet use to match students' ability, using child-friendly search engines where more open Internet searching is required.
- is vigilant when conducting 'raw' image search with students e.g. Google image search.
- informs all users that Internet use is monitored.
- informs staff and students that that they must report any failure of the filtering systems directly to the Network Manager. The Network Manager logs or escalates as appropriate to SWGfL Helpdesk as necessary and liaises with the DSL.
- makes clear all users know and understand what the 'rules of appropriate use' are and what responses result from misuse – through staff meetings and teaching programme;
- provides advice and information on reporting offensive materials, abuse/ bullying etc. available for students, staff and parents/carers.
- immediately refers any material we suspect is illegal to the DSL, who will then refer it to the appropriate authorities; e.g. Police, Channel Panel and Prevent Referral Services.
- Safe search is enabled as default on our search engines.

Network management (user access, backup)

This school:

- uses individual, audited logins 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 NetSupport for controlling workstations/viewing users/setting-up applications and Internet websites, where useful.

- ensures the network manager and IT technicians are up to date with SWGfL services and policies.
- storage of all data within the school will conform to the UK data protection requirements.
- students and staff using mobile technology, where storage of data is online, will conform to the General Data Protection Regulation where storage is hosted within the EU.

To ensure the network is used safely, this school:

- ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- staff access to the schools' management information system is controlled through a separate password for data security purposes.
- we provide students with an individual network log-in username. From Year 7 they are also expected to use a personal password.
- all students have their own unique username and password which gives them access to the Internet, and their own school approved email account.
- makes clear no one should log on as another user and makes clear students should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas.
- requires all users to always log off when they have finished working or to lock it if they are leaving the computer unattended. PC's are configured to lock automatically after 30 minutes of inactivity.
- where a user finds a logged-on machine, we require them to always log off and then log on again as themselves.
- requests that teachers and students do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 5 o'clock to save energy.
- has set-up the network so that users cannot download executable files/programs;
- has blocked access to music/media download or shopping sites – except those approved for educational purposes.
- makes clear staff are responsible for ensuring that all equipment that goes home has the anti-virus software maintained up-to-date and the school provides them with a solution to do so.
- makes clear 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" as defined by HM Revenue & Customs.
- has an integrated curriculum and administration networks, but access to the Management Information System is set up to ensure staff users can only access modules related to their role, e.g. teachers access report writing module in SIMS.
- ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems.
- 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 support.
- our MIS provider is responsible for the daily backup of MIS and finance systems and other important files.
- has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data that complies with external Audit's requirements.
- uses our broadband network for our CCTV system and have had set-up by approved partners.
- ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system.
- follows Internet Service Provider (ISP) advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- ensures that our wireless network has been secured to appropriate standards suitable for educational use.
- all computer equipment is installed professionally and meets health and safety standards.
- projectors are maintained so that the quality of presentation remains high.
- reviews the school digital systems regularly with regard to health and safety and security.

Password policy

- Staff are required to use 2FA to access the network, both internally and externally.
- Logging in from outside the UK is blocked except for special circumstances.
- This school makes it clear that staff and students must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We encourage users to apply long passwords comprising a minimum of at least 15 characters and 3 unrelated words..

E-mail

This school:

- provides staff with an email account for their professional use within Office 365 and makes clear personal email should be through a separate account.
- does not publish personal e-mail addresses of students or staff on the school website. We use anonymous or group e-mail addresses, dhsg@dhsg.co.uk for communication with the wider public.
- will contact the Police if one of our staff or students receives an e-mail that we consider breaks the law.
- will ensure that email accounts are maintained and up to date.
- reports messages relating to or in support of illegal activities including extremist groups and sexual grooming to the relevant authority e.g. the Police.
- knows that spam, phishing and virus attachments can make e-mails dangerous. We use several SWGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus software. Finally, and in support of these, SWGfL filtering monitors and protects our Internet access to the World Wide Web.

Students

- We use Office 365 with students and lock this down where appropriate.
- Students are introduced to and use e-mail as part of the Computing scheme of work.
- Students are taught about Online Safety and 'netiquette' of using e-mail both in school and at home i.e., they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer.
    - that an e-mail is a form of publishing where the message should be clear, short and concise.
    - that any e-mail 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.
    - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.
    - to 'Stop and Think before They Click' and not open attachments unless sure the source is safe in relation to cyber security.
    - that they should think carefully before sending any attachments.
    - embedding adverts is not allowed.
    - that they must immediately tell a teacher/responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature.
    - not to respond to malicious or threatening messages.
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying.
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.
    - that forwarding 'chain' e-mail letters is not permitted.

- Students sign the school Acceptable Use Agreement to say they have read and understood the Online Safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff

- Staff are aware how to encrypt sensitive data: to encrypt – new email – options – click on the yellow padlock and select "encrypt".
- Access in school to external personal e-mail accounts may be blocked.
- Staff know that e-mail 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:
    - The sending of multiple or large attachments should be limited and may also be restricted by the provider of the service being used.

- The sending of chain letters is not permitted.
- Embedding adverts is not allowed.

- All staff sign our school Acceptable Use Policy Agreement to say they have read and understood the Online Safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Social Networking
With an increase in use of all types of social media for professional and personal purposes we give clear guidance to staff to manage risk and behaviour online. Core messages include the protection of our students, the school and individuals when publishing material online. Teachers are instructed not to run social network spaces for student use on a personal basis or to open their own spaces to their students, but to use the schools' preferred system for such communications. Expectations for teachers' professional conduct are set out in the 'Teachers Standards 2012'.

School staff are made aware that:
- no reference should be made in social media to students / parents / carers / or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions are not attributed to the school
- security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.

Where official school social media accounts are used we ensure that:
- the school social media sites are solely managed by the Deputy Head Teacher under the Head Teacher's authority to ensure that it is carried out in a safe and responsible way
- no references to students / or staff are made without consent from individual
- personal opinions are not attributed to the school
- security settings are regularly checked to minimise risk.

Monitoring of Public Social Media
- As part of active social media engagement, we pro-actively monitor the Internet for public postings about the school.
- In discussion with the HT the DHT would effectively respond to social media comments made by others.
- The school's use of social media for professional purposes is checked regularly by the Head Teacher and DSL to ensure compliance with the school policies.

School website
- The Head Teacher/Deputy Head Teacher 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: Network Manager and authorised IT technicians.
- The school web site complies with the statutory DfE guidelines for publications.
- Most material is the school's own work; where other's 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 web site is the school address, telephone number and we use a general email contact address dhsg@dhsg.co.uk. Home information or individual e-mail identities will not be published.
- Photographs published on the website do not have full names attached.
- We do not use students' names when saving images in the file names or in the tags when publishing to the school website.
- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

CCTV
- We have CCTV in the school as part of our site surveillance for staff and student safety. CCTV images will not be shared with anyone outside the school without permission unless the law and our rules permit it.

7. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- the Business Manager is the Data Protection Officer (DPO).
- staff are clear who the key contact(s) for key school information are.
- we ensure staff know who to report any incidents where data protection may have been compromised.
- all staff are DBS checked and records are held in one central record.
- we ensure ALL the following school stakeholders sign an Acceptable Use Policy Agreement. staff
  - Trustees
  - students

  This makes clear staffs' responsibilities with regard to data security, passwords and access.

- Users of SIMS, FMS (Finance Management System), On-line Banking and Secure Access (including student data) all require passwords to be changed every month
- We follow recognised secure methods for the transfer of any data, such as reports of students, to professionals working in the Local Authority or their partners in Student Services/Family Services, Health, Welfare and Social Services.
- We require that any protected and restricted material must be encrypted if the material is to be removed from the school and limit such data removal.
- school staff with access to setting-up usernames and passwords for email and network access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual housekeeping to review, remove and destroy any digital materials and documents which no longer need to be stored.

Technical Solutions

- Staff have a secure area in the staff shared area on the network to store sensitive documents or photographs.
- We require staff to log-out of or to lock systems when leaving their computer.
- We insist that encrypted flash drives are used when any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF Student data files to other schools and Government departments.
- We store any protected and restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof safe. No back-up tapes leave the site on mobile devices.
- We have a disaster recovery procedure to mitigate against ransomware attacks and other scenarios in which the school network becomes unavailable to users.
- We comply with the 'Waste electrical and electronic equipment recycling' 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 get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using crosscut shredder or collected by secure data disposal service.

8. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile technology devices which might include: smartphone, tablet, smartwatch, notebook/laptop or other technology brought into school are entirely at the staff member, students' & parent/carers' or visitors' own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- Student mobile devices which are brought into school must be turned off (and out of sight as they enter the school site for the whole school day until 3.35pm. This restriction applies equally to staff and visitors.

- The recording, taking and sharing of images, video and audio on any mobile phone is not permitted; except where it has been explicitly agreed otherwise by the Head Teacher. Such authorised use is to be monitored and recorded. There are several school mobile devices that staff use when leading offsite activities or to take images of students for school use.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. This will be done in conjunction with the Department for Education's guidance on Searching, Screening and Confiscation – July 2022. Please see the Behaviour for Learning Policy for further detail. Where there are suspicions of child pornography or sexual images of children, the device will not be searched and processes as laid out in the Safeguarding and Child Protection will be followed / lead by the DSL
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Mobile phones and personally owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- The Bluetooth or similar function of a mobile phone should be always switched off and not used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- If a student breaches the school policy, then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will be released to parent/carers in accordance with the school policy. Students are only allowed to use the school's secure wi-fi connection to access the internet whilst on site.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an examination will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- Parents/carers are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day. Permission for use of personal devices for this purpose must be sought from the Head Teacher or Deputy Head Teacher first. Where possible, school devices should be used.
- Staff are not permitted to use their own mobile phones or devices for contacting students, young people or their families within or outside of the setting in a professional capacity (unless with the prior permission of the Head Teacher).
- Staff will be issued with a school phone where contact with students, parent/carers is required.
- Mobile Phones and personally owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally owned devices are only to be used in line with the Staff Code of Conduct.
- If members of staff have an educational reason to allow students to use mobile phones or a personally owned device as part of an educational activity due vigilance must be observed and accommodations made for students without a device or data.
- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in the case of emergency during off-site activities, or for contacting students or parents/carers, then in most cases a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes. This usage should be reported to the Head Teacher/DSL.

Digital images and video

In this school:

- we gain parent/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school.
- we do not identify students by using full names in online photographic materials or include the full names of students in the credits of any published school produced video materials/DVDs.
- staff sign the school's Acceptable Use Agreement, and this includes a clause on the use of mobile phones/personal equipment for taking pictures of students.
- the school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- students are taught about how images can be manipulated in their Online Safety education programme and taught to consider how to publish for a wide range of audiences which might include Trustees, parent/carers or younger students as part of their Computing scheme of work.
- students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- students and staff are made aware of the risks of AI-generated imagery, including the creation of fake or misleading images and videos, and how these may be used to bully, defame, or exploit individuals.
- the policy prohibits the creation, use, or sharing of synthetic media that misrepresents, harms, or manipulates individuals without their informed consent.

Asset disposal

Details of all school-owned hardware and software will be recorded in an inventory.
All redundant equipment will be disposed of through an authorised agency with the prior agreement of the Business Manager. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
Disposal of any equipment will conform to Waste Electrical and Electronic Equipment Regulation (WEEE) No. 3113 from 2013
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/292632/bis-14-604-weee-regulations-2013-government-guidance-notes.pdf Further information can be found on the Environment Agency website.

Appendices

Staff (and Volunteer) Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of school digital technology and communication systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, iPads, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I understand that when using generative AI tools for educational purposes, I must ensure they are approved by the school and align with our safeguarding, data protection policies and wider GDPR.
- I will critically evaluate AI-generated content before using it with learners, understanding that such content may contain inaccuracies, biases, or inappropriate material.
- I will not input personal data about learners, staff, or families or their intellectual property into generative AI systems without explicit permission from senior staff and in accordance with data protection policies. The only pre-approved AI platform for this purpose is Microsoft 365 copilot.
- I will model responsible AI use for learners and incorporate AI literacy into my teaching where appropriate.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others that they are suitable and I will do so with their permission and in accordance with the DHSG's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers, staff and Trustees using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will not use AI tools to create content that could be mistaken for authentic student work, staff communications, or official school materials without clear disclosure.
- I will ensure that any AI-generated content used in communications with learners, parents/carers, or colleagues is clearly identified as such and has been reviewed for accuracy and appropriateness.
- I will not use AI to generate images, audio, or video content of real people (including students, staff, or parents) without explicit consent and in accordance with school policies.
- When using AI tools for lesson planning or resource creation, I will verify the accuracy of information and ensure content is age-appropriate for my learners.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement and Mobile Phone Policy, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I must not create, access, transmit or download inappropriate terrorist or extremist materials, as defined within the Prevent Guidance (2015), using the School's IT systems or network. The school has a statutory duty to take steps to prevent individuals being drawn into extremism and terrorism, and a duty to alert and report any attempted access to, or dissemination of, such inappropriate material.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to DHSG equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the DHSG Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school/DHSG policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- I understand that inputting personal data about learners, staff, or families into generative AI systems may constitute a data breach and will only do so with explicit authorisation and in accordance with data protection policies.
- I will be aware that AI systems may retain and use input data for training purposes, and I will not share confidential or sensitive school information with unauthorized AI tools.

- I will ensure that any AI-generated content used in my professional capacity complies with data protection requirements and does not inadvertently disclose personal information.
- I understand that the school's filtering systems are designed to prevent access to harmful and inappropriate AI-generated content, and I will not attempt to bypass these protections.
- I understand that my interactions with generative AI tools will be monitored and logged in accordance with school policies.
- I will immediately report any AI-generated content that appears harmful, inappropriate, or concerning to the appropriate safeguarding personnel.
- I will not install or use unauthorised AI applications or tools on school devices without explicit permission from the IT department.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that AI-generated content may incorporate copyrighted material, and I will verify the copyright status of any AI-generated content before using it in my professional work.
- I will properly attribute the use of AI tools in my professional work and will not present AI-generated content as my own original creation.
- I will educate learners about the importance of acknowledging AI assistance in their work and the potential copyright implications of using AI-generated content.

Responsible Use of Generative AI in Education: (New Section)

- I understand that generative AI tools can enhance teaching and learning when used appropriately and ethically.
- I will only use AI tools that have been approved by the school leadership team and comply with our safeguarding and data protection policies.
- I will maintain my professional judgment and expertise when using AI tools, ensuring that AI supplements rather than replaces my pedagogical knowledge and understanding of my learners' needs.
- I will be transparent with learners about when and how I use AI tools in my teaching and will model critical evaluation of AI-generated content.
- I will stay informed about developments in AI technology and its educational applications through appropriate professional development opportunities.
- I will be transparent with learners about when and how I use AI tools in my teaching and will model critical evaluation of AI-generated content.
- I will contribute to the development of learners' AI literacy by teaching them to:
    - Identify potentially AI-generated content
    - Critically evaluate the accuracy and reliability of AI-generated information
    - Understand the ethical implications of AI use
    - Use AI tools responsibly and transparently in their learning

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of DHSG digital equipment in school, but also applies to my use of school digital technologies and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use policy, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Trustees and the Local Authority and in the event of illegal activities the involvement of the police.
- I understand that the school's filtering systems must "effectively and reliably prevent access to harmful and inappropriate content generated by Generative AI systems" and that monitoring systems must "maintain robust activity logging procedures that capture interactions with generative tools."
- I will cooperate with these monitoring procedures and understand that my AI tool usage will be logged and reviewed as part of the school's safeguarding responsibilities.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name _____

Signed _____

Date _____

Devonport High School for Girls Student Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access to these digital technologies.

This acceptable use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school digital technologies in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that I am only allowed to access the internet via the school's secure Wi-Fi connection.
- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online (including on my own device whilst at school).
- I will not share personal information with AI systems or generative AI tools without explicit permission from school staff.
- I understand that AI-generated content (including text, images, audio, and video) may not be accurate or truthful, and I will verify information from multiple reliable sources before using it for educational purposes.
- I will be aware that AI-generated content may contain biases or inappropriate material, and I will report any concerning AI-generated content to a member of staff.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g., YouTube). Any exception to this would require the permission of a member of staff.
- I will not use AI tools to complete assignments or assessments in ways that would constitute academic dishonesty or plagiarism.
- I understand that when using generative AI tools for educational purposes, I must have explicit permission from a member of staff and will use these tools responsibly and ethically.
- I will acknowledge when AI tools have been used to assist with my work and will ensure that any AI-generated content is appropriately referenced and fact-checked.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I will not use AI tools to create, generate, or distribute content that could be harmful, offensive, or inappropriate, including deepfakes, fake images of real people, or content that could be used for bullying or harassment.
- I will not use AI to impersonate others or create false identities online.

I recognise that the School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the School:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission as indicated in the Mobile Devices Policy. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will not install or attempt to install or store programs of any type on any school device, nor will I try to alter computer settings.
- I must not create, access, transmit or download inappropriate or extremist materials, as defined within the Prevent Guidance (2015), using the school's systems or network. The school has a statutory duty to take steps to prevent individuals being drawn into extremism and terrorism, and a duty to alert and report any attempted access to, or dissemination of, such inappropriate material.
- I will not use social media sites without explicit permission from a member of staff whilst on the school site.
- I understand that the school's filtering systems are designed to prevent access to harmful and inappropriate content generated by AI systems, and I will not attempt to bypass these protections.
- I understand that the school's monitoring systems will capture my interactions with generative AI tools, and I will use these tools responsibly.
- I will immediately report any AI-generated content that appears harmful, inappropriate, or concerning to a member of staff.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I understand that AI-generated content may appear convincing but could contain inaccuracies, biases, or fabricated information, and I will critically evaluate all AI-generated content before using it.
- I will not present AI-generated work as my own original work and will properly attribute the use of AI tools in my academic work.
- I will develop my critical thinking skills to identify potentially AI-generated content, including text, images, audio, and video.

Responsible Use of Generative AI (New Section)

- I understand that generative AI tools can be powerful educational resources when used appropriately under staff supervision.
- I will only access generative AI tools that have been approved by the school and will use them in accordance with school policies and staff guidance.
- I will not use AI tools to create inappropriate content, including but not limited to: content that violates school policies, mimics or impersonates real people without consent, or could be used to deceive or mislead others.
- I understand that AI-generated content should supplement, not replace, my own learning and critical thinking.
- I will be transparent about my use of AI tools and will discuss any concerns about AI-generated content with my teachers.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information, posting or liking posts which refer to the school, staff or students in a way that might cause offense on social media or other web-based platforms).
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents/carers and in the event of illegal activities involvement of the police.
- I understand that my use of AI tools and sharing of AI-generated content outside of school that relates to the school community is subject to the same standards as outlined in this agreement.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student Acceptable Use Agreement Form

This form relates to the student acceptable use agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to l school digital systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, USB devices, smartwatches, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this School e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student		Tutor Group	
Signed		Date	

Parent/Carer Counter signature

Signed		Date	
Name of Parent/ Carer			

DEVONPORT HIGH SCHOOL FOR GIRLS

STANDARD CONSENT FORMS FOR SCHOOLS
THE USE OF IMAGES OF CHILDREN

The use of digital/video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name will be used.

The school will comply with the Data Protection Act and request parent's/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their own names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Name of Student: …….. **Form:** …… **Date of Birth:** ……..	***Please delete as appropriate***
1. I agree that the school can take digital images/video of my child 2. I agree to these images being used: • To support learning activities. • In publicity that reasonably celebrates success and promotes the work of the school. This might include: Twitter, LinkedIn and Facebook School website and literature Local and national press	**Yes/No** **Yes/No** **Yes/No**

I have read and understood the conditions of consent on the back of this form.

Signature of parent/carer: …….....

Name of Parent/Carer (please print) …….

Date: ……

STANDARD CONSENT FORMS FOR SCHOOLS
THE USE OF IMAGES OF CHILDREN

CONDITIONS OF CONSENT

1. The information which you provide in the Consent Form is valid from the time when the school receives this form until the time your child leaves the school. If your circumstances change or you need to change your mind about any issues addressed in this form, please let the school know immediately.

2. The school will not use any images of your child once your child has left the school without obtaining the parents' / carers' specific consent (exceptions to this would be if they were already printed on school literature, such as website, social media and / or school prospectus).

3. The school will only use images of students who are appropriately dressed.

4. If you agree that the media can take and use images of your child, you should note that the media's use of images of children is governed separately by the General Data Protection Act 2018.

Roles and Responsibilities

Role	Key Responsibilities
Head Teacher	• The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the online safety team • The Head Teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff • To take overall responsibility for online safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. SWGFL • To be responsible for ensuring that staff receive suitable training to carry out their Online Safety roles and to train other colleagues, as relevant • To receive regular monitoring reports from the Designated Safeguarding Lead (DSL) and DSL • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager)
Assistant Head Teacher/Designated Safeguarding Lead	• To take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policy, and online safety team. • To provide training and advice for staff • To report regularly to the Head Teacher and SLT on online matters • To Liaise with school technical staff and Network Manager • To receive reports of online safety incidents from including DNA reports taking appropriate actions. • Ensure they are regularly updated in online safety issues and legislation, and be 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 on-line contact with adults/strangers o potential or actual incidents of grooming o cyber-bullying and use of social media ▪ Attends relevant meetings of Trustees ▪ Lead the Online Safety Team

Role	Key Responsibilities
Trustees / Safeguarding Trustee	• To ensure that the school follows all current online safety advice to keep the students and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. A member of the Trustees has taken on the role of Safeguarding Trustee • To support the school in encouraging parents/carers and the wider community to become engaged in online safety activities • The role of the Safeguarding Trustee will include: o regular review with the Deputy Designated Safeguarding Lead (including Online Safety incident logs, filtering/change control logs) o be a member of the DHSG online safety team
Head of Computing	• To liaise with the DSL regularly and appropriately in regard to online safety and to work with Heads of House to support online safety within PSHEE • To lead on an annual audit of online safety co-ordinating the completion of the SWGfL 360° audit • To oversee the delivery of the online safety element of the Computing curriculum and co-ordinate internet safety day • To be a member of the Online Safety Group
Network Manager/ Technical staff	• To report any Online Safety related issues that arises, to the Assistant Head Teacher/Designated Safeguarding Lead • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date • To ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack • To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices • To ensure that the school's policy on web filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person • To ensure that SWGfL is informed of issues relating to the filtering applied by the Grid • To ensure that he/she keeps up to date with the school's Online Safety Policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • To ensure that the use of *digital technologies* is regularly monitored in order that any misuse/attempted misuse can be reported to the Deputy Head Teacher/Head Teacher and Assistant Head Teacher/Designated Safeguarding Lead for investigation/action/response • To ensure that monitoring software/systems are implemented and updated

Role	Key Responsibilities
	• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures • To ensure that all SWGfL services are managed on behalf of the school • To ensure that all data held on students on any online platform is adequately protected • To ensure measures and planning is in place for cyber security
Office Manager	• To ensure that all data held on Students on the school office machines have appropriate access controls in place
All staff	Are responsible for ensuring that: • they have an up-to-date awareness of online safety matters and of the current *school* online safety policy and practices • they have read, understood and signed the staff acceptable use policy agreement (AUPA) • they report any suspected misuse or problem to the *Head teacher/DSL/Deputy Head Teacher* for investigation/action/response • all digital communications with students/parents/carers should be on a professional level *and only carried out using official school systems* • online safety issues are embedded in all aspects of the curriculum and other activities • students understand and follow the Online Safety Policy and Acceptable Use Policy • students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices • in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
Students	• Read, understand, sign and adhere to the Student Acceptable Use Agreement • To develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse 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 policy on the use of mobile phones, digital cameras and hand held devices • To know and understand school policy on the taking/use of images and on cyber-bullying • To understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Role	Key Responsibilities
	• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/ review of online Student Acceptable Use Agreement
Parent/carers	Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: • digital and video images taken at school events • access to parents/carers' sections of the website/Learning Platform and on-line student/pupil records their children's personal devices in the school
External groups	• Any external individual/organisation will be asked to read an Acceptable Use Policy Form prior to using any equipment or the Internet within school

Mobile Devices Policy

Introduction

There is a growing bank of literature such as National research as evidenced in a paper by the London School of Economics http://cep.lse.ac.uk/pubs/download/dp1350.pdf referring to the impact of technology. Nationally, schools are witnessing an increasing number of issues with the mis-use of social media, sometimes by students from a very young age.

Many studies have shown that there are gains to be made in progress and mental health when access to social media is limited during the school day. In our recent survey of students, parents, carers, staff and Trustees, many identified that students were either directly or indirectly affected by some of the issues surrounding the mis-use of social media and recognised that it was time to reconsider our approach to the management of mobile devices.

To support the development of good interpersonal skills and to promote good physical and mental health, we will encourage students to attend the comprehensive selection of clubs and societies which take place during the lunch break.

We believe that there are many positive uses of digital technologies. We will use computer suites and school tablets in lessons and internet safety will be taught through the computing and pastoral curriculum. Both students and staff, through Microsoft Office 365, will continue to have access to Outlook / One Drive / One Note / Word / Excel / Powerpoint and Calendar in school and at home. Students will also have access to computer rooms from 8.00am to 4.45pm.

These expectations have been in force since 2019.

Expectations

All students

- Must ensure that mobile devices are switched off at the school gate and put away out of sight for the whole of the school day until 3.35pm. After school for health and safety reasons mobile devices should never be used in corridors and stairwells.
- The only exception to this is if a teacher invites students to use a mobile device in a lesson in pairs /groups (negating the need for all students to have a mobile device) but at all other times the mobile device must be switched off and out of sight.
- Must only access the internet through the school's Wi-Fi network and not use their mobile data network.

Sixth Form students

May use mobile devices in the allocated Sixth Form areas; the Sixth Form Centre and Rooms 6 and 7 when used for independent study.

Staff

We believe that adults should be leading by example so we have amended procedures for staff. Staff mobile devices should be switched off and out of sight in lessons and when circulating around the school site. The only exception to this is if a teacher uses their mobile device in a teaching activity with their class.

Visitors

When signing in, if visitors have a mobile device they will be asked to switch it off and keep it out of sight between the hours of 8.00am and 3.35pm.

If parents/carers need to contact their child in an emergency, we ask that they call the school office.

Staff will enforce the new expectations by managing a **WE SEE IT, WE HEAR IT, YOU LOSE IT** strategy:

First sanction

A member of staff will confiscate a mobile device place it in a secure bag with a record card and take it to the HoH/Sixth Form office. An email / letter will be sent home and the student will collect their device at the end of the school day. Details will be recorded on SIMS and a behaviour mark will be awarded.

Second sanction

A member of staff will confiscate the mobile device as above and take it to the HoH/Sixth Form office. A letter/email will be sent home. The student will collect the mobile device at the end of the day but will be required to hand in their device to their HoH/Sixth Form office at the start of each day for four consecutive days. Details will be recorded on SIMS and a behaviour mark will be awarded.

Third sanction

A member of staff will confiscate the mobile device as above and take it to the HoH/Sixth Form Office. The pastoral team will send a letter/email home requesting parents/carers to come in for a meeting with the HoH/Sixth Form Leadership Team to discuss their child's use of the mobile device and agree on a way forward. The device will be held at the HoH/Sixth Form Office at the start of each day until this meeting has taken place. Details will be recorded on SIMs, and a detention will be awarded.

Any further breaches of these expectations will be referred to SLT.

Any students accessing social media and messaging services will be referred to their HoH / Sixth Form Leadership Team.