DEVONPORT HIGH SCHOOL FOR GIRLS

ICT AND E-SAFETY POLICY

(Including Student and Staff ICT Acceptable Use Policies)

Named person: A Thomas

Category: School

Review: Annually (or as significant changes occur)

Date to be reviewed: Summer 2019

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

Adopted by the Governors' Policy Committee on: 09/07/18

Ratified at the Full Governors' meeting on: 11/07/18

Contents

1. Introduction and Overview

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 with respect to the use of ICT-based 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 ICT 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 e-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 with regard to 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 e-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.
- ICT Acceptable Use Policy discussed with students at the start of each year.
- ICT Acceptable Use Policy to be issued to whole school community, usually on entry to the school.
- Signed ICT Acceptable Use Policy to be held in student and staff personnel files.

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 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 sanctions.
- Our Designated or Deputy Designated Safeguarding Lead act as first point of contact for any complaint. Any complaint about staff misuse is referred 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 e-safety policy is referenced from within other school policies.
- The school has one person monitoring E-Safety the Deputy Designated Safeguarding Lead who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The e-safety policy has been written by the school Deputy Designated Safeguarding Lead 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 Governors. This policy is reviewed annually by Governors and Staff.

2. Education and Curriculum

Student e-safety curriculum

This school:

- Has a clear, progressive e-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 e-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 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 Policy which every student will sign and is displayed in computer suites.
- 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 e-safety issues and the school's e-safety education programme.
- Provides, as part of the induction process, all new staff [including ITT students on placement] with information and guidance on the ICT and e-safety policy and the school's Acceptable Use Policies.

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.
    - Demonstrations, practical sessions held at school.
    - 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.

Contact

- Grooming – sexual and radicalisation.
- Cyber-bullying in all forms.
- Identity theft (including 'frape' (hacking Facebook 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)).
- 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).

4. Prevent Duty and E-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. Islamic State of Iraq and the Levant (ISIL) for example have used images and videos to present their cause as an exciting alternative to life in the West as well as social media to encourage users to share material. In the 12 months to the end of June 2015 around 38,889 internet takedowns were undertaken by the Counter Terrorism Internet Referral Unit (CTIRU) reducing extremist material available on the Internet; that means over 100,000 since the unit was set up in 2010.

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 system essential Safety 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 on line 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 have a seconded police officer and arrangements in place with other police forces to deal with the intelligence appropriately.

Using an advanced filtering system we are able to filter based on an individual or specific group basis (e.g. year 7, Sixth form). We are also able to obtain reports on search terms that have been used by students which will enable us to be more pro-active in protecting them online.

5. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant ICT Acceptable Use Policy 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 are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- 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 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 e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students:

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

Parents/carers:

- Should provide consent for students to use the Internet, as well as other technologies, as part of the e-safety 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 very positive and there is rarely need to apply sanctions.
- 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) 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.
- 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 students receives online communication that we consider is particularly disturbing or breaks the law.

6. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

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, thereby closing down or opening up options appropriate to the age/stage of the students.
- The school 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 set-up so staff and students cannot download executable files.
- 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.
- Ensures all staff and students have signed an ICT Acceptable Use Policy and understand that they must report any concerns.
- Ensures students only publish within an appropriately secure environment such as Moodle.
- requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform Moodle as a key way to 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.
- 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 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. The DSL, who will then refer it to the appropriate authorities; e.g. Police, Channel Panel and Prevent Referral Services.

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 NetSupport for controlling workstations/viewing users/setting-up applications and Internet web sites, 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 E-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, the Learning Platform and their own school approved email account.
- Makes clear that no one should log on as another user and makes clear that 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 are leaving the computer unattended.
- 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 that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained 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" as defined by HM Revenue & Customs.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as 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 Education Welfare Officer accessing attendance data on specific students, parent/carers using a secure portal to access information on their child.
- Provides students and staff with access to content and resources through the approved Learning Platform which staff and students access using their username and password.
- Makes clear responsibilities for the daily back up 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 ICT systems regularly with regard to health and safety and security.

Password policy

- 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 COMPLEX passwords which include different characters, upper and lower case letters and numbers.

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 a number of 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' Office 365 e-mail accounts are 'part-anonymised' for their protection.
- Students are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Students are taught about the-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.
    - 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 ICT Acceptable Use Policy to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff

- Staff can only use Office 365 e-mail systems on the school system and only for professional purposes.
- Access in school to external personal e-mail accounts may be blocked.
- Never use email to transfer staff or student personal data to other schools or employers without placing the term 'encrypt', 'encrypted' or 'confidential' in the email subject heading to ensure it is encrypted.
- 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 ICT Acceptable Use Policy to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

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.

Learning platform

- Uploading of information on the schools' Learning Platform is shared between different staff members according to their responsibilities.
- Photographs and videos uploaded to the schools Learning Platform and Shared Area will only be accessible by members of the school community.
- In school, students are only able to upload and publish within school approved and closed systems, such as the Learning Platform.

Social networking

Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students, parent/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

This school:

- Only uses the SWGfL supported services for video conferencing activity.
- Only uses approved or checked webcam sites.

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.
- We use specialist lesson recording equipment IRIS on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

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 ICT Acceptable Use Policy. We have a system so we know who has signed.
  - staff
  - governors
  - 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, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping 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 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 use the SWGfL secure data transfer system for creation of online user accounts for access to broadband services.
- 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 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 cross cut shredder or collected by secure data disposal service.

8. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parent/carers' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into school must be turned off (not placed on silent) whilst in lessons. Students may use their phones during school break times. Staff are requested to keep their phones on silent and not use them during lessons. All visitors are requested to keep their phones on silent.
- 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. All mobile phone use is to be open to scrutiny and the Head Teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary. There are a number of 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. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- 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 in to 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.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- 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.
- 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.
- 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.
- 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 will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- 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.

- 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.

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 Policy 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 e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parent/carers or younger students as part of their ICT 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.

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. 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) ICT Acceptable Use Policy

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 communications 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 internet access at all times.

This ICT 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 DHSG ICT 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 ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT 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.

ICT Acceptable Use Policy

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

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of DHSG ICT systems (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 ICT 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 will be professional in my communications and actions when using DHSG ICT 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 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.

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, in the same way as if I was using DHSG equipment. I will also follow any additional rules set by DHSG 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 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, unless this is allowed in DHSG policies.
- 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.

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

- I understand that this ICT Acceptable Use Policy applies not only to my work and use of DHSG ICT equipment in school, but also applies to my use of DHSG ICT systems 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 ICT Acceptable Use Policy, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT 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 ICT Acceptable Use Policy

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 at all times.

This ICT Acceptable Use Policy 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.

The school will try to ensure 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.

ICT Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT 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 on-line (including on my own device whilst at school).

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 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 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. 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 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 only use social media sites with permission and at the times that are allowed.

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 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).
- I understand that if I fail to comply with this ICT Acceptable Use Policy, 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.

Please complete the sections on the below to show that you have read, understood and agree to the rules included in the ICT Acceptable Use Policy. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student ICT Acceptable Use Policy

This form relates to the Student ICT Acceptable Use Policy 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 ICT Acceptable Use Policy. If you do not sign and return this agreement, access will not be granted to School ICT 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, 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

Dear Parent/Carer,

For many years the school has recognised the importance of celebrating achievement and promoting the success of our students. Both parents/carers and young people alike, gain great pride in seeing photographic images and/or video recordings of family members in the local press, on the television, following sports day, prize giving, school plays etc. and have supported the whole school ethos in the past. In other circumstances the taking of photographs or video recordings of students at our school may be for strictly educational purposes or for purposes ancillary to the running of the school (e.g. taking photographs for use in the school's prospectus or on the school website).

There may also be occasions when the local press visit our school to record particular school events (e.g. school productions) and they may wish to publish photographs of the students on television when reporting these events.

Following changes in the law and in order to comply with the Data Protection Act 1998, the school needs your consent in the future before allowing the taking of photographs or making video recordings of your child for purposes which are not part of its activities. **We should therefore be grateful if you could answer the following questions, sign and date the form and return it to the school as soon as possible.**

Name of Student: …….. **Form:** ……. **Date of Birth:** ……..	***Please delete as appropriate***
1. I agree that the school can take photographs of my child which may be used in school literature (e.g. school newsletters, the school prospectus and other promotional material etc.)	**Yes/No**
2. I agree that the school can use images of my child on its website and social media pages	**Yes/No**
3. I agree that the school can use my child's full name/ first name only on its website and social media pages	**First name only** **First and surname**
4. I agree that the school can use images of my child in video recordings to promote the school	**Yes/No**
5. I agree that the school can take photographs and make video recordings of my child for the school's own records, archives and future interest (e.g. photographs of sports teams)	**Yes/No**
6. I agree that the school can take photographs and make video recordings of my child for the school's own records for the purpose of reviewing **Learning and Teaching** (e.g. filming evidence and reviewing progress in lessons). Also for submission as evidence of performance to examination boards	**Yes/No**
7. I agree that my child can appear in video recordings or in collections of photographs stored on DVD which the school may make of school events and which it may sell to parents of students at the school to raise funds for the benefit of the school	**Yes/No**
8. I am happy for the press to take and use images of my child	**Yes/No**
9. The school may give the press the first name only/first and surname of my child for publishing with the child's photograph in a newspaper or for captioning on television	**First name only** **First and surname**

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

Signature of parent/carer: …….....

Date: ……

Name (in block capitals): ……..

DEVONPORT HIGH SCHOOL FOR GIRLS

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 Data Protection Act, other legislation and industry codes of practice.

Roles and Responsibilities

Role	Key Responsibilities
Head Teacher	• To take overall responsibility for e-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 e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident • To receive regular monitoring reports from the Designated Safeguarding Lead (DSL) • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)
Designated Safeguarding Lead	• To take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies • To promote an awareness and commitment to e-safeguarding throughout the school community • To ensure that e-safety education is embedded across the curriculum • To liaise with school ICT technical staff and Network Manager • To communicate regularly with other members of SLT and the designated safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • To ensure that an e-safety incident log is kept up to date • To facilitate training and advice for all staff • To liaise with relevant agencies • To ensure they are regularly updated in e-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

Role	Key Responsibilities
Governors / Safeguarding governor	• To ensure that the school follows all current e-safety advice to keep the students and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors/Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor • To support the school in encouraging parents/carers and the wider community to become engaged in e-safety activities • The role of the Safeguarding Governor will include: o regular review with the Deputy Designated Safeguarding Lead (including e-safety incident logs, filtering/change control logs)
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the Deputy Designated Safeguarding Lead regularly
Network Manager/ technicians	• To report any e-safety related issues that arises, to the Deputy Designated Safeguarding Lead. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date • To ensure the security of the school ICT system • 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 • 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 e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • To ensure that the use of the *network/Virtual Learning Environment (LEARNING PLATFORM)/remote access/email* is regularly monitored in order that any misuse/attempted misuse can be reported to the Deputy Designated Safeguarding Lead */Head Teacher for investigation/action/sanction* • 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 e-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 the LEARNING PLATFORM Moodle is adequately protected

Role	Key Responsibilities
Data and Assessment Administrator	• To ensure that all data held on Students on the school office machines have appropriate access controls in place
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school Staff ICT Acceptable Use Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Students	• Read, understand, sign and adhere to the Student ICT Acceptable Use Policy • 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 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 • 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 e-safety student user agreement
Parent/carers	• To support the school in promoting e-safety including the safe and responsible use of the Internet and photographic or video images • To read, understand and promote the school Student ICT Acceptable Use Policy with their students • To access the school website/on-line student records in Parent/carer Gateway in accordance with the relevant school ICT Acceptable Use Policy • To consult with the school if they have any concerns about their students' use of technology
External groups	• Any external individual/organisation will sign an ICT Acceptable Use Policy Form prior to using any equipment or the Internet within school