E-safety Policy

Date of last review: **June 2018**
Date of next review: **June 2019**
SMT Responsible: **Charles Irish (Assistant Head)**
Governor Responsible: **Kelly Davis**

This policy was produced by the e-safety committee which comprises:

Staff role	Staff name
Assistant Head / DSL	Charles Irish
Head of Boarding	Martin Tippetts
Head of Computer Science	Andrew Miller
IT Managers	Mike Hands and James Moate
Director of Finance	Sarah Wills
E-safety Governor	Kelly Davis

Reference Documents/Websites:

Southwest Grid for Learning - 360 safe
UK Safer Internet Centre www.saferinternet.org.uk
Plymouth Inter-agency E-safety Pledge

Keeping Children Safe in Education (Sept 2016) – To be reviewed 2018 when updated documents available.
Working Together to Safeguard Children (March 2015)

The Prevent Duty (June 2015)
The use of social media for on-line radicalisation (July 2015)
https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

CEOP Thinkuknow www.thinkuknow.co.uk

UKCCIS guidelines entitled "Sexting in schools and colleges"
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

TES AND NSPCC safety policy summary of recommendations - https://www.nspcc.org.uk/globalassets/documents/information-service/esat-briefing-what-to-include-in-an-e-safety-policy-for-schools.pdf

NSPCC ESafety incident report (Appendix 6) - https://www.nspcc.org.uk/globalassets/documents/information-service/esat-briefing-sample-e-safety-incident-report-form.pdf

Esafety incident flow process - https://www.nspcc.org.uk/globalassets/documents/information-service/esat-briefing-what-to-do-if-a-pupil-or-a-teacher-reports-an-e-safety-incident.pdf

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 Plymouth College with respect to the use of electronic communication technologies.
- safeguard and protect the children and staff of Plymouth College.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and 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 and the dangers of radicalisation which are cross referenced with the Safeguarding and Child Protection and Anti-bullying Policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

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
- exposure to radicalisation and extremism propaganda
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content
- inappropriate sharing or use of personal data

Contact

- grooming
- cyber-bullying in all forms
- Radicalisation
- 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)
- extremist views
- copyright (little care or consideration for intellectual property and ownership – such as music and film)
- Ensure that all information is stored, kept and distributed in line with GDPR (May 2018)

Scope

This policy applies to all members of Plymouth College community (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 school.

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

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

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To ensure the school-based ICT network uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident • To receive updates from the E-Safety Co-ordinator on significant incidents • 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)
Director of Finance	• To take overall responsibility for data and data security

E-Safety Co-ordinator / Designated Safeguarding Lead	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• promotes an awareness and commitment to e-safeguarding throughout the school community
	• ensures that e-safety education is embedded across the curriculum
	• liaises with school ICT technical staff
	• To communicate regularly with SMT and the designated e-safety committee to discuss current issues, review incident logs and filtering
	• 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 cyber bullying incident log is kept up to date
	• facilitates training and advice for all staff
	• liaises with the Local Authority and relevant agencies
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers

Role	Key Responsibilities
	• potential or actual incidents of grooming and radicalisation • cyber-bullying and use of social media
Head of marketing & Communications	• Takes responsibility for the taking and publishing of photographic and video material relating to the school • Advising colleagues on correct procedures for use of digital imagery • Ensures schools social media forums are moderated for appropriate content
Governors / E-safety governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors' designate. A member of the Governing Body has taken on the role of E-Safety Governor • The role of the E-Safety Governor will include: • annual review with the E-Safety Coordinator including cyberbullying logs, filtering and policies
Computer Science Curriculum Leader (HoD)	• To oversee the delivery of the e-safety element of the Computer Science curriculum • To liaise with the e-safety coordinator regularly
Network Manager/ technician	• To report any e-safety related issues that arises, to the e-safety coordinator. • 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 • the school's policy on web filtering is applied and updated on a regular basis • 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 • that the use of the network / Intranet / remote access / email is monitored in order that any misuse / attempted misuse can be reported to the E-Safety Coordinator/Headteacher 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
Intranet Co-ordinator	• To ensure that all data held on pupils on the Intranet is adequately protected • Takes responsibility for the taking and publishing of photographic and video material relating to the school
Data Managers	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place

Role	Key Responsibilities
Teachers	• To embed e-safety issues in relevant aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • To know the procedures following an incident of cyberbullying, inappropriate use of the internet or suspicion of radicalisation.
All staff	• To be aware of their responsibilities in respect to GDPR and act accordingly • To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff 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 know the procedures following an incident of cyberbullying, inappropriate use of the internet or suspicion of radicalisation. • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal accounts, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • 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, social media sites and other technologies both in school and at home • to help the school in the creation/ review of e-safety policies • to know their rights and responsibilities for sharing data

Role	Key Responsibilities
Parents/carers	• to support the school in promoting e-safety and endorse the Pupil Acceptable Use Policy • to read and understand the pupil ICT AUP and promote it with their children • to consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

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

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use agreements distributed to all pupils and staff for reading, understanding and signing at the start of each year.
- Acceptable use agreements to be held in Admin.

Handling complaints:

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies, mobile networks and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - Interview by Head of Year or Assistant Head
  - Informing parents or carers;
  - Discipline sanctions and device confiscation in accordance with the School's Behaviour Management Policy.
  - Removal of Internet or computer access for a period
  - Referral to Police if deemed serious enough.

- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

- All incidents of cyberbullying are recorded on the Central bullying file by the Assistant Head.

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

Review and Monitoring
The e-safety policy is referenced from within other school policies: Safeguarding and Child Protection policy, Anti-Bullying policy, Behaviour Management policy, Personal, Social and Health Education policies, Privacy Notice, Data Breach and Record Keeping Policy.

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety committee and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SMT, E-safety Committee and approved by Governors. All amendments to the school e-safety policy will be published to all members of teaching staff.

2. Education and Curriculum

Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the PSHE curriculum / Computer Science curriculum. It is built on SWGfL guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - 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 or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
    - to understand why and how some people will 'groom' young people for sexual reasons;
    - to STOP and THINK before they CLICK
    - Be aware that terrorist organisations are trying to radicalise and recruit young people through an extensive use of social media and the internet and be resilient to this.
    - to understand acceptable behaviour when using an online communication, i.e. be polite, no bad or abusive language or other inappropriate behaviour that might upset or offend; keeping personal information private;
    - to understand why they must not post pictures or videos of others without their permission;
    - 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 appropriate privacy settings;
    - to have strategies for dealing with receipt of inappropriate materials;
    - to know not to download any files – such as music files - without permission;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - 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 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 that mobile device content can be addictive and the School will encourage periods of time when the use of these devices is prohibited

- Acknowledges that pupils may access the Internet through their own devices on mobile networks – Our school strategy is to educate pupils of the dangers of using unfiltered access rather than the wholesale prohibiting of personal devices on the school site.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an ICT Acceptable Use Policy which every student will sign.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This school

- Makes training available to staff on e-safety issues and the school's e-safety education program through INSET and staff briefings.
- Provides, as part of the induction process, all new staff with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.
- Provides training on GDPR and data security

Parent awareness and training

This school

- Makes parents aware of the pupil acceptable use policy to ensure that principles of e-safe behaviour are made clear.
- Delivers occasional e-safety awareness presentations at school for parents.
- Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems and their own devices in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- 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 to the Assistant Head or Headmaster
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if it affects the school in any way
- will be expected to know and understand 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
- are expected to ensure the data they are responsible for is secure and to report any potential breaches to breach@plymouthcollege.com

Staff

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

Students/Pupils

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

Parents/Carers

- should understand and endorse the school's Pupil ICT AUP at time of their child's entry to the school

- should know and understand what the ‘rules of appropriate use’ are and what sanctions result from misuse

Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely 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 behaviour management system.
- support is actively sought from other agencies as needed (e.g. the local authority and SWGfL, UK Safer Internet Centre helpline) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and used to improve the e-safety policy in the future
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- We will contact the police and Plymouth Prevent duty officer if we suspect one of our pupils to be involved in radicalisation.
- If data security is breached we have a breach policy in place which is stored on the intranet.

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Uses the Smoothwall filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved ‘web filtering management’ status, data logs are only kept for 6 months;
- Ensure the network safety through the use of ESET Endpoint Security etc. and network set-up so staff and pupils cannot install executable files without permission;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Is vigilant in its supervision of pupils’ use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;

- Requires staff to preview websites beforehand and direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Yahoo for Kids, Google Safe Search , …..
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Network Manager.
- 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 pupils, staff and parents
- Immediately refers any material we suspect is illegal to the police.

- **Network management (user access, backup)**
  This school
  - Uses individual, audited log-ins for all users;
  - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
  - Uses teacher 'remote' management control tools for controlling workstations.
  - Storage of all data within the school will conform to the UK data protection requirements

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also use the same username and password for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username. From Year 7 they are also expected to use a personal password;
- All pupils have their own unique username and password which gives them access to the Internet and the Intranet and all pupils have their own school approved email account;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to 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 pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off/lock when they have finished working or are leaving the computer unattended;
- Requires all users to log-off any unattended machines and then log-on as themselves.
- Has set-up the network so that student users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;

- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained 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".
- Has integrated curriculum and administration networks, but access to the SIMS system is set-up so as to ensure staff users can only access modules related to their role
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems:
  e.g. teachers access their area / a staff shared area for planning documentation via Remote Desktop/Ranger Portico
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical SIMS Support
- Provides pupils and staff with access to content and resources through the intranet which staff and pupils access using their username and password;
- Makes clear responsibilities for the daily back up of SIMS 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;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- Reviews the school ICT security systems regularly.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff and pupils have their own unique username and private passwords to access school systems. Staff and pupils are responsible for keeping their password private.
- We require staff and pupils to use strong passwords as defined by Microsoft for access into our computer network.
- We require staff and pupils to change their passwords into the computer network system every 90 days.

E-mail

This school

- Provides staff with an email account for their professional use and makes clear personal email traffic should be through a separate account;
- When contacting pupils and parents, staff must only use school systems.

- Does not publish personal e-mail addresses of pupils or staff on the school website. We must ensure if personal email addresses are used, they are put in the BCC section of the email and not in a mail group/list.

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date, removing unnecessary messages/accounts.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product ESET, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Pupils:

- We use MDaemon email software with pupils
- Pupils are introduced to, and use e-mail as part of the CS scheme of work.
- Pupils 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 respond to any propaganda that may be linked to radicalisation
    - not to delete malicious or 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.

- Pupils sign the Pupil ICT AUP and boarding pupils sign an additional boarding AUP 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 only use MDAEMON e-mail systems for professional purposes
- 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. That it should follow the school 'house-style':
    - 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 Staff ICT AUP 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 Headteacher 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: Director of Communications, Prep Registrar and other authorised administrators
- 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, e.g. info@plymouthcollege.com or admin@plymouthcollege.com. Home information or personal e-mail identities will not be published;

Intranet

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

Social networking

- Teachers are instructed not to run personal social network spaces for student use, but to use the schools' preferred system for such communications; this includes setting up departmental social networking.
- The school's preferred system for social networking will be maintained in adherence with the Social Media Policy.

School staff will ensure that in private use of their own social media sites:

- Will not be friends on social media sites with existing students
- No reference should be made to students 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 should minimise risk of loss of personal information.

Video Conferencing

- The school only uses a single account for Skype video conferencing activity

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings publically without permission, except where disclosed to the Police as part of a criminal investigation.

- All CCTV cameras are logged in a report called the Impact Assessment; which details the purpose of installation, who has access to the recordings and when it will be deleted. This report is maintained by the Infrastructure Manager and is updated any time a CCTV camera is installed or when there is a change.

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

Strategic and operational practices

At this school:

- The Director of Finance is the school's Data Controller.
- The Infrastructure Manager is the Data Privacy officer.
- Staff are clear who are the key contact(s) for key school information
- We ensure staff know to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record (SCR)
- We ensure ALL staff and pupils sign an ICT Acceptable Use Policy form. We have a system so we know who has signed. This makes clear staff's responsibilities with regard to data security, passwords and access.
- We have an approved and secure remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Intranet access are working within the approved system and follow the security processes required by those systems.
- Staff are reminded and should undertake regular house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- Staff have been provided with encrypted memory sticks which they must use if removing digital files containing personal data from site.

Technical Solutions

- Staff have secure areas on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 15 minutes idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- All servers are in lockable locations and managed by DBS-checked staff.
- Back-ups are encrypted. No back-up media leaves the site.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

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

Mobile Phone use

There has been much media discussion about how the constant use of mobile phones is affecting children. The emphasis should be on digital citizenship as well as e-safety, and how devices can be used in a positive way (e.g. in lessons). The focus should also be on educating pupils how to use devices, and teach them filtering skills; they need to learn manners, courtesy and discretion whilst online – "netiquette" - and that devices can be very addictive (especially with younger pupils – there is no "off" button).
As such the school has introduced a Mid-week digital detox which promotes a period of time during school hours on Wednesdays during which staff and students should refrain from using their mobile devices.

General Usage

1. Mobile phones brought into school are entirely at the staff member, student's & parent's or visitor's own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
2. 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 that which promotes pornography, violence or bullying.
3. Designated 'mobile use free' areas are situated in the setting, and signs to this effect are to be displayed throughout. The areas which should be considered most vulnerable include: toilets, bathrooms and in some settings - sleep areas and changing areas.
4. No images or videos should be taken on mobile phones or devices without the prior consent of the person or people concerned.
5. 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.
6. The College gains parental 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.
7. The College blocks/filters access to social networking sites or newsgroups unless there is a specifically approved educational purpose. The school acknowledges that pupils may access the Internet using their own devices on mobile networks – however, our school strategy is to educate pupils of the dangers of using unfiltered access rather than the wholesale prohibition of personal devices on the school site.
8. Students are taught about how images can be manipulated and to consider the consequences of sharing with a wider audience.
9. Students are advised to be very careful about placing any personal photos on any 'social' network space. They are taught to understand the need to maintain privacy settings so as not to make personal information public.
10. 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' use of personal devices

1. Student mobile phones which are brought into school must be turned to **silent** with the **vibrate** facility turned off.

2. Students may not use their phones whilst **between lessons**.
3. Students may only use their devices during **mid-break and mid-lunchtime only** (i.e. not on the way to lessons). They should find a quiet location to use the phone and should NOT walk around campus whilst using them.
4. Mobile phones may 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.
5. Mobile phones are not allowed in the **Dining Hall, Assemblies or Tutor time**.
6. During **Private Study sessions or Supervised Prep**, students may use Mobile Phones appropriately for educational research and they may listen to music through headphones at the discretion of the supervising member of staff. Pupils may not access social media at these times.
7. Mobile devices must not be taken into **examinations**. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
8. If a **student does not have a mobile phone** and needs to contact his or her parents or carers, they should ask to use the phone in the school office.
9. **Parents** are advised not to contact their child via their mobile phone during lesson times. They may contact the school office in an emergency.
10. Students are encouraged to report to the **health centre** first before contacting parents if feeling unwell or requiring assistance.
11. The recording, taking and sharing of **images, video and audio** on any mobile device by a student is not allowed; except where it has been explicitly agreed by the teacher. Such authorised use is to be monitored. All mobile device use will be open to scrutiny and the staff are able to withdraw or restrict authorisation for use at any time if deemed necessary.
12. 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.
13. If a student **breaches** the Mobile Phone Use policy, then the phone or device will be confiscated in accordance to our 3 strike policy which resets each term and sanctions applied:
    1. For the 1st offence the phone will be confiscated by the member of staff who will hand it in to the school office. It can be collected at the end of the day by the student. 1 behaviour point will be added onto SIMS
    2. For the 2nd offence in the same term the phone will be confiscated by the member of staff who will hand it in to the school office. It can be collected at 5pm by the student. For the next 5 days the pupil will hand the phone in to the office by 8.30am and will be able to collect it at the end of the day. 3 behaviour points will be added onto SIMS
    3. For the 3rd offence in the same term the phone will be confiscated by the member of staff who will hand it in to the school office. It will be collected by the Head of Year. The phone can then only be collected by parents after a meeting with the Head of Year. 5 behaviour points will be added onto SIMS

Staff use of personal devices

1. Staff sign the school's **Staff ICT Acceptable Use Policy** and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

2. Staff are permitted to use their own mobile phones or devices for contacting parents in a **professional capacity**.
3. For emails, staff must only **use the school email** to contact pupils and parents.
4. Staff can use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students for school purposes only (in accordance with the digital photography policy) and these images must be uploaded to a school system if appropriate and then be deleted from personal devices at the earliest opportunity including cloud/external locations.
5. If a member of staff breaches the school policy then disciplinary action may be taken.
6. Where staff members are required to use a mobile phone for **school duties**, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and are advised to hide (by inputting 141) their own mobile number for confidentiality purposes.
7. Staff members should not give their **personal mobile numbers** to pupils except under exceptional circumstances. This should be reported to the Assistant Head along with the reason for doing so.

Asset disposal

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

Appendix 1:

Plymouth Inter-Agency E-safety Pledge

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

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

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

Plymouth College Pupil ICT Acceptable Use Policy

This Plymouth College Acceptable Use Policy is intended to ensure that:

- You are a responsible user, staying safe while using the internet.
- College ICT systems and users are protected from anything that could damage them.

The College will try to ensure that you will have good access to ICT to enhance your learning and will expect you to be a responsible user.

NB: Each Plymouth College boarder has an **Individual Boarder's ICT Acceptable Use Contract**.
This policy covers the use of ICT outside the Boarding Houses.

Key Points of the Acceptable Use Policy

1. I must be very careful before providing any personal information to a website or an individual online.
2. I must be aware of the legal issues surrounding sending or receiving inappropriate images on my personal communication devices.
3. I must use College ICT systems in a responsible way, as a member of the College community.
4. I must understand that my online actions must not have a negative effect on others, or the College.
5. The requirements of this Acceptable Use Policy apply to any personal communication equipment that I use at any time in a way that relates to me being a member of this College.
6. I will respect any copyright that exists on information found online.

Acceptable Use Policy – Detail

I understand that I must use College 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 will keep my username and password secret and not share it with anyone else.
- I will not use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about others when on-line. This includes pictures.
- I will be cautious about information I choose to share online.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report to a teacher any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- School will monitor my use of the ICT systems.

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

- I understand that the College ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission.
- I will not make large downloads or uploads that might take up internet bandwidth and prevent other users from being able to carry out their work.
- I will not use the College ICT systems for on-line gambling, internet shopping, peer to peer (e.g. torrent) file sharing.

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, offensive, aggressive or inappropriate language or comments and I appreciate that others may have different opinions.
- I will not take or distribute illegal or inappropriate images of myself or anyone else.
- If I receive an inappropriate image I will delete it immediately from any of my electronic communication devices and/or cloud storage.
- I will not take and distribute any images of anyone else without their permission.

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

- I understand that if I do use my own devices in College, I will follow the rules set out in this agreement just as if I was using College 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.
- I will not try to use any programmes or software that might allow me to bypass the filtering systems in place to prevent access to such materials.
- I will immediately report to a teacher or the IT managers any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I am responsible for all activity carried out using my network login ID and I will remember to log off when I have finished using my machine.
- If I bring a personal mobile media device (e.g. USB device) into school, I will ensure that it has had a virus check before I insert it into a school machine.
- If I bring a personal device or computer/laptop into school, I will ensure that I have working, up to date anti-virus software installed.

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 copyright protected, I will not download copies (including music and videos)
- I understand the seriousness of plagiarism when undertaking a self-study exercise and accept that the school will take disciplinary action if I attempt this.
- 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 College:

- I understand that the College also has the right to take action against me if I am involved in any incident of inappropriate behaviour that is covered in this agreement even out of College hours (examples include cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to College discipline. This may include loss of access to the network/internet, detentions, suspensions, contact with parents and, in the event of illegal activities, involvement of the police.

Plymouth College Pupil ICT Acceptable Use Agreement

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

I have read and understand the policy and agree to follow it when:

- I use the College ICT systems and equipment (both in and out of College)
- I use my own equipment in College e.g. mobile phones, laptops, ipads, PDAs, cameras etc
- I use my own equipment beyond the College site in a way that relates to me being a member of this College e.g. communicating with other members of the College, accessing College email, Intranet etc.

Name: _____

Form: _____

Signed: _____

Date: _____

ICT Acceptable Use Policy for Staff and Volunteers

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools 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 safe internet access 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 electronic communications technologies for educational, personal and recreational use.
- that school 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.

Acceptable Use Policy Agreement

I understand that I must use all electronic communication systems in a responsible way, to ensure that there is no risk to my safety or to the safety of others. I also accept responsibility for the security of the school ICT systems. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils 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 ICT systems (eg laptops, email, intranet etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use.
- I will not disclose my school username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate, or harmful material or incident that I become aware of to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will only 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 I will do so in accordance with the school's policy on the use of digital/video images. If I use a personally-owned device, such as a mobile phone or camera to take photos or videos of students, it will only be for school purposes and these images will be uploaded to a school system if appropriate and will be deleted at the earliest opportunity from the device and cloud/external device.
- I will avoid personal use of chat and social networking sites in school time.
- I will only communicate with students and parents/carers in a professional tone and manner using school systems.
- I will not allow any current pupil to become a friend on my personal Facebook account, or any similar social networking site, this rule applies until the child reaches 21 years of age.
- I will not communicate with pupils through any other media than the school email system or via a school mobile phone.
- I will not give current pupils my personal mobile phone number unless I have the permission of the Assistant Head for use in specific offsite situations.
- I will not record mobile phone numbers of current pupils on my personal mobile phone unless I am on an off-site activity, or boarding duty, which may require this to be done, with the permission of the Assistant Head. If sharing of contact details is required, I will ensure that all parties have deleted the contact details at the earliest opportunity.
- 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 personal hand held/external 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 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 use personal email addresses for correspondence with pupils.
- I will not open any attachments to emails, unless the source is known and trusted, 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 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 not (unless I have permission) make large downloads or uploads that might take up internet bandwidth 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 school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined by GDPR (or other relevant school policy). Where personal data is transferred outside the secure school network, a school provided encrypted USB device must be used.

- I understand that GDPR requires that any staff or student/pupil 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 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, or I am unsure of the copyright status, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of ICT systems and equipment out of school that might affect my professional position and my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors, dismissal and in the event of illegal activities the involvement of the police.

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

Staff/Volunteer Name

Signed

Date

Appendix 4 - Boarder's ICT Acceptable Use Contract

This contract exists to define a boarder's internet access privileges. The extent of these privileges will be reviewed from time to time, for example as a result of a boarder's request, or for technical reasons. With this list of privileges set out below comes a list of responsibilities and a series of consequences if the responsibilities are ignored or flouted.

Privileges
The Head of Boarding, in consultation with the IT Managers, may grant privileges to a boarder which are different from the following categories, but for most boarders, the privileges will be:

☐ Level 1 access (typically Years 7 – 9)
Websites: non-chat games, BBC i-Player, Spotify
Other: Skype (voice only)

☐ Level 2 access (typically Years 10 – 11)
As above plus
Websites: YouTube, Facebook, Twitter

☐ Level 3 access (typically Sixth Form)
Websites: Only restricted by school filtering

These privileges will only operate outside normal school hours.

Responsibilities
When you sign this contract, you are accepting everything that follows:
"I understand that with the internet privileges listed above come certain responsibilities. By signing this contract, I agree to abide by the Plymouth College ICT acceptable use policy (this may be subject to change; the current version may be viewed online at http://www.plymouthcollege.net/computing/rooms/?page=acceptable use policy).

In particular, as a boarder, I will not:
1. allow younger pupils, or students whose parents stated they cannot have internet access, to view or use my computer.
2. use anyone else's username and password to logon to the network, or interfere with anyone else's computer.
3. access material that is inappropriate for someone of my age, or try to.
4. give personal information on the Internet, for example: bank account or credit card details, home telephone numbers, full names, addresses or photographs.
5. illegally download material, or try to.
6. access pornographic sites, or try to.
7. look at, create, upload or use material that is illegal or has racist, sexist, obscene, violent, offensive or bullying content. This includes making unpleasant comments about others on any website forum or public space.
8. make any software or hardware changes to the setup of my computer that seek to bypass any controls placed on my access of the internet through the school network.
9. access, or attempt to access, the internet using any network that I have not obtained permission to use.

Internet access includes the use of direct connection to the internet on mobile phones and other internet-capable devices. I understand that breaking any of these conditions will be treated as a serious matter and will result in one or more sanctions, ranging from confiscation of my computer (or other internet-capable device), to suspension from school."

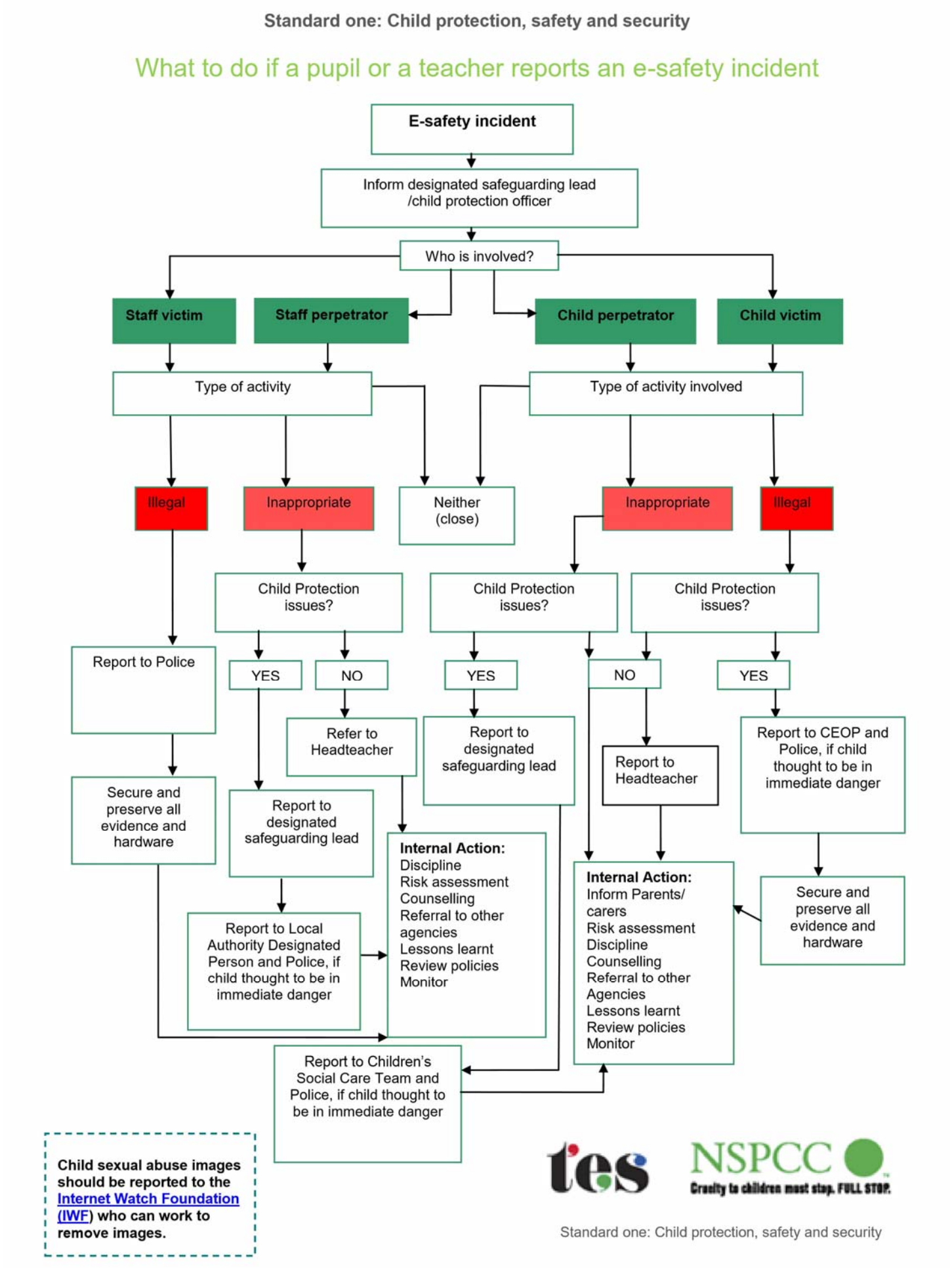
Name: _____

Form: _____

Signed: _____

Date: _____

Appendix 5 – Flowchart for responding to e-safety incidents



Appendix 6

NSPCC

Sample e-safety incident report form

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