Online Safety Policy

(includes use of images and consent of children, young people and vulnerable adults in educational settings)

Linked Policies/Protocols

- Behaviour Policy
- Relationships Policy
- PSHEe Policy
- T&L Policy
- Child Protection Policy
- Safeguarding Policy
- Anti-Bullying and Harassment
- Social Distancing Policy

Reviewed: Feb 2021	**Next review due:** Feb 2022
Governing Body Committee: CSC	**CLT contact:** Chris Pease/ Becky Lear
Policy adopted by the Full Governing Body on: 31st March 2021	

The points covered in this policy reflect the UNCRC and our commitment to it – we understand the Articles affecting children's' rights in respect of Online Safety are:

- Article 2 – We approach every incident without discrimination
- Article 3 – Everything we do is in the best interests of every child
- Article 4 – We respect and protect the rights of every child
- Article 5 – We respect the rights and responsibilities of parents to guide and advise their child and work together with them to ensure they apply their rights properly
- Article 6 – We ensure that every child survive and develop to grow up to be healthy and happy wherever possible
- Article 8 – We preserve the identity of every child
- Article 12 – We respect the views of every child and take them seriously
- Article 13 – We ensure that every child has the right to say what they think and how they feel
- Article 16 – We respect the privacy of every child
- Article 17 – We respect and ensure that every child has the right to reliable information from the mass media and protection from any materials that could harm them
- Article 19 – We do everything we can to ensure that every child is protected from all forms of violence, abuse, and mistreatment
- Article 18 – We respect and encourage parents to share responsibility for bringing up their child, always considering what is best for them
- Article 27 – Wherever possible we meet the physical, mental and emotional needs of our students
- Article 36 – We ensure that wherever possible we protect children from all forms of exploitation that may harm them

INTRODUCTION

New technologies have become integral to the lives of children and young people in today's society, both within College and in their lives outside College.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in Colleges are bound. A College e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in College and at home has been shown to raise educational standards and promote student achievement.

However, the use of these new technologies can put young people at risk within and outside the College. Some of the dangers they may face include:

- access to illegal, harmful or inappropriate images or recordings or other content;
- unauthorised access to / loss of / sharing of personal information;
- the risk of being subject to grooming by those with whom they make contact on the internet;
- the sharing/distribution of personal images, videos or recordings or other content without an individual's consent or knowledge;
- inappropriate communication/contact with others, including strangers;
- cyber-bullying;
- access to unsuitable video/internet games;
- an inability to evaluate the quality, accuracy and relevance of information on the internet;
- plagiarism and copyright infringement;
- illegal downloading of music or video files;
- the potential for excessive use which may impact on the social and emotional development and learning of the young person;
- the potential risk of radicalisation through access to extreme material or individual with extreme views.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other College policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The College must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

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

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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 College 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 out of College, but is linked to membership of the College.
The College 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 College.

Please note in this College safeguarding young people is paramount. All staff have received training re the Prevent Duty and understand their responsibility to prevent extremism and radicalisation. Students have been advised about the issues surrounding this.

ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for the online safety of individuals and groups within the College:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

The Headteacher and Senior Leaders

- The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the College community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.

- The Headteacher/Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in College who carry out the internal online safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.

- The Headteacher and another member of the College Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Online Safety Co-ordinator/Designated Safeguarding Lead:

- attends the Safeguarding Monitoring Group Meetings;

- oversees the day to day implementation of the Online Safety Policy and has a leading role in establishing and reviewing the College e-safety policies/documents;

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;

- provides training and advice for staff;

- liaises with the Local Authority/other agencies and/or external services where necessary;

- liaises with College ICT technical staff;

- work with parents to ensure they are aware of any behaviour that could be putting their young person at risk;

- receives reports of e-safety incidents and creates a log of incidents to inform future online safety developments;

- meets regularly with the Lead DSL to discuss current issues, review incident logs and filtering/change control logs;

- ensures that any incidents of cyber-bullying are logged and dealt with appropriately in line with the College behaviour policy;

- receives reports of students' use of and access to the internet (in light of the policy for students to carry and use mobile phones in the Behaviour Policy);

- reports issues to the police via 101 email service where appropriate;

- is present during police phone seizure and completes E2/3 where appropriate;

- ensures E1/2/3 forms are stored with the Designated Safeguarding Lead and are logged on CPOMs.

- Provides reports on online safety, available to the headteacher and/or governing body

This list is not intended to be exhaustive

Network Manager/Technical staff

ICT Technicians are responsible for ensuring:

- that the College's ICT infrastructure is secure and is not open to misuse or malicious attack;

- that the College meets the online safety technical requirements in accordance with direction / guidance issued by SWGfL and any relevant DFE and Local Authority Online Safety Policy and guidance;

- that users may only access the College's networks through a properly enforced password protection policy, in which passwords are regularly changed;

- SWGfL is informed of issues relating to the filtering applied by the Grid;

- the College's filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;

- that he/she keeps up to date with e-safety 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/Virtual Learning Environment (VLE)/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Co-ordinator;

- that monitoring software / systems are implemented and updated as agreed in College policies.

All Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current College online safety policy and practices;
- they have read, understood and signed the College Staff Acceptable Use Policy/Agreement (AUP)
- they report any concern, suspected misuse or problem to the Online Safety Co-ordinator;
- digital communications with students/pupils (email/Virtual Learning Environment (VLE)/voice) should be on a professional level and only carried out using official College systems;
- e-safety issues are embedded in all aspects of the curriculum and other College activities;
- students understand and follow the College e-safety and acceptable use policy;
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extra-curricular and extended College activities;
- they are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current College policies with regard to these devices;
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- in lessons where students report seeing or accessing inappropriate content (especially content which could be viewed as extreme) this must be report to a member of the DSL team promptly
- record all concerns on E1 form and on SIMS network for the attention of the Online Safety Co-ordinator.

Students:

- are responsible for using the College ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to read when first logging into the ICT system. A copy of the Student Acceptable Use Policy can be found on the student desktops;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

- will be expected to know and understand College policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand College policies on the taking / use of images and on cyber-bullying;

- should understand the importance of adopting good e-safety practice when using digital technologies out of College and realise that the College's Online Safety Policy covers their actions out of College, if related to their membership of the College;

- will understand that the College has a responsibility to take action if they feel a young person is putting themselves at risk;

- will understand it breaches the behaviour expectations of the College to take inappropriate images, videos or recordings or other content of staff or students.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The College will therefore take every opportunity to help parents understand these issues through parents' evenings, the topic, letters, website, College's Facebook and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student Acceptable Use Policy;
- taking appropriate action to safeguard their child from online risks;
- supporting the College's expectations in terms of online safety, appropriateness and behaviour;
- accessing the College website / VLE / on-line student / student records in accordance with the relevant College Acceptable Use Policy;
- compliance with the images consent protocol;
- any content accessed by or sent by devices provided by them as parents.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

Visitors and members of the community

Visitors and members of the community who access College ICT systems/website /VLE as part of the Extended College provision will be expected to sign a Visitor AUP before being provided with access to College systems.

POLICY STATEMENTS

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the College's e-safety provision. Children and young people need

the help and support of the College to recognise and avoid online safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- A planned online safety programme is provided as part of computing/PSHEe/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in College and outside College;

- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities;

- Students / pupils should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside College;

- Students should be taught to understand how it breaches our behavioural expectations to take inappropriate images, videos or recordings or other content, especially without consent;

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;

- Rules for use of ICT systems / internet will be posted in all rooms with ICT facilities and displayed on log-on screens;

- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The College will therefore seek to provide information and awareness to parents and carers through:

- Letters, our regular newsletter, website;
- The College's social media account(s);
- Parents evenings and other parental events;
- Reference to the SWGfL Safe website (the SWGfL "Golden Rules" for parents).
- Bespoke meetings with parents to discuss particular issues which may be of concern;

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of online safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly;

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the College online safety policy and Acceptable Use Policies;

- This Online Safety policy and its updates will be presented to and discussed by staff in staff/ team meetings/INSET days;

- The Online Safety Coordinator will provide advice/guidance/training as required to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in ICT/e-safety /health and safety /child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/ SWGfL or other relevant organisation;

- Participation in College training/information sessions for staff or parents.

Technical – Infrastructure/Equipment, Filtering and Monitoring

The College will be responsible for ensuring that the College infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- College ICT systems will be managed in ways that ensure that the College meets the online safety technical requirements as required by SWGfL and any relevant DFE and Local Authority Online Safety Policy and guidance.

- There will be regular reviews and audits of the safety and security of College ICT systems.

- Servers, wireless systems and cabling must be securely located and physical access restricted.

- All users will have clearly defined access rights to College ICT systems. Details of the access rights available to groups of users will be managed and monitored by the ICT Network Manager (or another person) and will be reviewed, at least annually.

- All users will be provided with a username and password by the ICT Team who will keep an up to date record of users and their usernames. Users will be required to change their password every term.

- The "master/administrator" passwords for the College ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. College safe).

- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- The College maintains and supports the managed filtering service provided by SWGfL.

The College will provide enhanced user-level filtering as and when its filtering service provider makes this provision available.

- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).

- Any filtering issues should be reported immediately to SWGfL.

- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Network Manager / ICT Team.

- The College's ICT Team regularly monitor (and record where appropriate) the activity of users on the College ICT systems and users are made aware of this in the Acceptable Use Policy.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc from accidental or malicious attempts which might threaten the security of the College systems and data.

- User accounts for temporary guests' e.g. external cover have been set up, and will be activated, by the ICT Team as required. These accounts have restricted access to provide additional network security and are based on a standard student account.

- Users are not to download programmes / software onto College standalone or network devices without the approval of the ICT Team.

- College laptops / portable devices issued to staff for use off site are only to be used by the individual. Any breach of this policy may result in the item being withdrawn. Note the ICT Team can request the return of College laptops / portable devices for audit purposes, software upgrades and virus checks at any time; this may include a check of system logs to ensure appropriate usage. Staff should also ensure they have appropriate insurance arrangements in place to cover accidental damage / loss of the equipment for which they will be liable for the replacement cost (this will be based on the cost incurred by the College to source a new like for like piece of equipment).

- Staff are not to store staff, student or College data on laptops / portable devices; this information is to be stored on the College's ICT Network or an encrypted portable storage device. Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of the College's Data Protection Policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal.

- Users of the College's ICT systems are forbidden to install / download software on College workstations/portable devices. Further guidance can be sought from the ICT Team.

- Guidelines for the responsible and safe use of external storage devices is contained in Form C (enclosed). Staff must ensure they are conversant with the College's Data Protection Policy and their responsibilities to mitigate any risk of a data breach. Where possible staff should not use removable media (e.g. memory sticks /CDs / DVDs) containing staff, student or College data off site, but where this is unavoidable devices

used should be encrypted. Further details are to be obtained from the ICT Team where required.

- The College infrastructure and individual workstations are protected by up to date virus software.

- Personal data should not be sent over the internet or taken off the College site unless safely encrypted or otherwise secured.

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

- Students should be taught to understand how it breaches our behavioural expectations to take inappropriate images, videos or recordings or other content, especially without consent.

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of Images of Children, Young People, Vulnerable Adults in Educational Settings

Staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those

images. Those images should only be taken on College equipment; the personal equipment of staff should not be used for such purposes.

Consideration will be given to:

- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.

- Students must not take, use, share, publish or distribute images of others without their permission.

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs, unless parental / carer consent has been given.

The College will ensure that images of a single child with no surrounding context of what they are learning or doing will be avoided.

Children and parents should be encouraged to recognise the value of group photographs or recordings of College events.

The College recognises that images must not be used to cause distress, upset or embarrassment.

The College will use photographs that represent the diversity of the children/young people participating.

Images will be kept securely and held by the College.

Images gathered as evidence of an e-safety incident will be logged on the secure area and will be available only to ICT support, DSLs and E-safety co-ordinator.

Images of children from the College will not be used to illustrate controversial subjects.

The College uses images (photographs, film):

- to record and capture special moments**;**

- to show what we do as a College;

- to liven up our website;

- to celebrate our College as a learning community;

- to celebrate and share our work with the community, including to promote achievements by staff and students;

- to store as evidence of reports made where a child has been put at risk or in in breach of College values.

In May 2004, section 45 of the Sex Offences Act 2003 amended Section 1 of the Protection of Children Act 1978 by raising the age of a 'child' from 16 to 18. This means it is now an offence to 'take, make, allow to take, distribute, show, possess with intent to distribute, or advertise indecent photos or pseudo photographs of children under the age of 18.

Torpoint Community College recognises the need to respect children's and parents' rights of privacy and is aware of potential child protection issues.

Images taken by parents, legal guardians or family members at an event:

- Parents, legal guardians, family members and friends can take images of their child and friends participating in College activities for family and personal use;

- Parents will be asked for their permission before photography is allowed;

- The event organiser must ensure parents; legal guardians or family members are briefed prior to an event starting if images may be taken. If permission is given to take images of their child / friends participating in the event, they must be informed that it is for family and personal use only and they will not be used inappropriately;

- The College will ensure that children who should not be photographed, for example those whose parents/legal guardians have refused consent, are not included in any images;

Images for College Publications

- The College will only take and use images that are appropriate and are considered to not be open to misuse.

- If an image of a child is used, the child's name **will not** be published unless parental / carer consent has been given.

- Children and their parents/legal guardians will be made aware of why their picture is being taken and how it will be used.

- The College will ensure that images of a single child with no surrounding context of what they are learning or doing will be avoided.

- Children and parents should be encouraged to recognise the value of group photographs or recordings of College events.

- The College recognises that images must not be used to cause distress, upset or embarrassment.

- The College will use photographs that represent the diversity of the children/young people participating.

- Images will be kept securely and held by the College for the duration of the student's time here, after which, they will be destroyed or securely stored for use in College publications.

- Images of students from the College will not be used to illustrate controversial subjects.

College Website and Social Media (e.g. Facebook and Twitter)

- The College website and social media accounts are more easily accessible than paper-based College publications. The College will make sure that only appropriate images are used. Image filenames will avoid using children's names.

- The storage of electronic images will be regularly reviewed by a senior member of staff.

CCTV

- The College may use/uses CCTV in some areas of College property as a security measure.

- Cameras will only be used in appropriate areas and there will be/is clear signage indicating where it is in operation.

Video Conferencing

- Video conferencing will only be used in a controlled environment under the close supervision of College staff. This facility can allow an individual or class to interact over the internet with others, support learning with other schools and provide links with approved organisations.

- Both students and staff will be made aware of when the video conferencing facility is in use.

Children Photographing One Another

- Staff will supervise and maintain control over any photographing students do during on-school or off-site activities.

- Camera phones are less visible and can be used to bully or take inappropriate images. Although students are allowed to have mobile phones, they are only for use in designated areas. Their use is **not** permitted in changing rooms, toilets or in other areas with a heightened expectation of privacy.

- If it is found that cameras or camera phones have been misused, the College will follow the disciplinary procedures as outlined in our anti-bullying policy and behaviour policy. In some cases it may be necessary for Torpoint Community College to contact children's social care and/or the police.

- Students should not be taking photos or videos or recordings or other content of each other without prior permission. Where a student has captured an image or video or recording or other content of another student in breach of College values this evidence will be removed from the device and where possible stored on the secure area. This will be treated as a breach of College online safety policy and the evidence used at the discretion of the Head of Year, Online Safety Lead, Headteacher or Police where applicable.

<u>Please note that images taken by the media are not covered by this policy and are subject to a separate set of regulations.</u>

Photographs, video and images are used by students as part of coursework and study. Staff should inform and educate students about the risks associated with taking, using, sharing, publishing and distributing images. The storage of images is in line with our Safeguarding Policy.

Data Protection & GDPR

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and GDPR which states that everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- transfer sensitive staff, student or College data using encryption and secure password protected devices where possible.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- data must be encrypted and password protected;
- the device should be password protected where possible (many memory sticks / cards and other mobile devices cannot be password protected);
- the data must be securely deleted from the device, in line with College policy (below) once it has been transferred or its use is complete.

There is stronger legal protection for more sensitive information, such as:

- the racial or ethnic origin of the Data Subject;
- political opinions;
- religious or other beliefs of a similar nature;
- membership of trade unions;
- physical or mental health or condition;
- sexual life;
- the commission of any offence or criminal records;
- other classes of data which might be regarded as personal are data relating to children and financial information.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the College currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to College	x				x			
Use of mobile phones in lessons				x			x	
Use of mobile phones in social time	x					x		
Taking photos or videos or recordings or other content on mobile phones or other camera devices		x					x	
Use of handheld devices eg PDAs, PSPs		x					x	
Use of personal email addresses in College, or on College network		x						x
Use of College email for personal emails		x						x
Use of chat rooms / facilities		x						x
Use of instant messaging		x						x
Use of social networking sites		x						x
Use of blogs or vlogs		x					x	

When using communication technologies the College considers the following as good practice:

Email:

- The official College email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the College email service to communicate with others when in College, or on College systems (e.g. by remote access).

- Users need to be aware that email communications may be monitored.

- Users must immediately report to the Headteacher or ICT Team (whichever is appropriate) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Any digital communication between staff and students or parents must be professional in tone and content. These communications may only take place on official (monitored) College systems.

- Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications:

    - for the transmission of unsolicited commercial or advertising material, chain letters, press releases, or other junk-mail of any kind, to other user organisations, or to organisations connected to other networks, other than where that material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe;

    - for the unauthorised transmission to a third party of confidential material concerning the activities of Torpoint Community College;

    - for the transmission of material such that this infringes the copyright of another person, including intellectual property rights;

    - for the unauthorised provision of access to Torpoint Community College services and facilities by third parties;

    - for activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users;

    - for activities that corrupt or destroy other users' data for activities that disrupt the work of other users;

    - for the creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material;

    - for the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;

    - for the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs. Torpoint

Community College is committed to fostering a learning and working environment free from discrimination where everyone is treated with dignity and respect;

- for the creation or transmission of defamatory material;
- for the creation or transmission of material that includes false claims of a deceptive nature;
- for so-called 'flaming' i.e. the use of impolite terms or language, including offensive or condescending terms;
- for activities that violate the privacy of other users;
- for criticising individuals, including copy distribution to other individuals;

- If a group email is sent to parents/carers, ensure that all addresses are entered onto the "bcc" address bar, to make sure email addresses aren't seen by other recipients;
- Personal information should not be posted on the College website and only official e-mail addresses will be used to identify members of staff.

Mobile Phones/Mp3 Players and other Handheld Devices

Students and staff who bring such devices onto the College site do so at their own risk, the college will not be responsible for the loss or theft of these items.

Students may only use their mobile phone in designated areas before and after College and during break and lunch times. If they are seen outside of this time and especially in lessons the college is allowed under the Education Act 2011, the college has the right to confiscate these items. (see Pilot BYOD information below for exceptions)

Students are not allowed to use their phone to take pictures, videos, recordings or other content in college (unless with permission) or upload any information relating to another student or member of staff.

Any incidents of bullying using this technology during the college day will be dealt with using our behaviour and anti-bullying and harassment policy. The College accepts that many of these types of incidents happen outside of the college in the evenings and weekends. The College will support the parents, students and sometimes the Police if such incidents occur, but will not necessarily take action. The responsibility for such action in these cases rests with the owner of the computer or device, which in most instances will be the parents/carers.

Staff should not use mobile phones for personal use whilst visible for students. Wherever possible this should be done in staffrooms, offices or classrooms that aren't being used.

Unless in exceptional circumstances, staff shouldn't use their personal phones to contact parents or to take pictures of students.

Any remote access to emails must be password protected.

Students using mobile devices in College

Technology plays a large part in students' lives. Personal devices can enhance and enrich learning opportunities both at home and in school. Torpoint Community College is committed to allowing responsible, learning-centred use of personal devices in College so as to provide as many pathways to understanding as possible for our students. By using their own devices, students will be familiar with how the technology works, take responsibility for their own learning preferences and have greater access to resources outside of the classroom. Where learning is dependent upon the use of technology, the teacher will provide students with access to College iPads or paper alternatives if students do not have their own device.

Access:

- Access to the Torpoint Community College wireless network, whether with College-provided or personal devices, is filtered through the South West Grid for Learning. Access from personal devices is limited to Internet use only. Students are not permitted to access blocked sites through 3G or other mobile phone networks. Students will not have access to any documents that reside on the school network from their personal devices.

- Access to the Torpoint Community College wireless network is a privilege not a right. Any use of the wireless network entails personal responsibility and compliance with all school rules. The use of the Torpoint Community College network also allows IT staff to conduct investigations regarding inappropriate Internet use at any time even on students' personal devices.

Guidelines for use:

- Use of personal devices during the College day is at the discretion of teachers and staff. Students must use devices as directed by their teacher.

- The primary purpose of the use of personal devices at College is educational. Personal use for personal reasons is secondary. Students are not allowed to access personal emails, Facebook, Twitter or other social media accounts except as directed by the teacher for educational purposes.

- The taking of photographs or images or videos or recordings or other content of teachers, adults or students without consent is strictly forbidden. It is also strictly forbidden to take inappropriate images or videos or recordings or other content of students or staff.

- The use of a personal device is not to be a distraction in any way to teachers or students. Personal devices must not disrupt the lesson in any way.

- Students shall make no attempts to circumvent the College's network security and/or filtering policies. This includes setting up proxies and downloading programmes to bypass security.

Consequences for misuse:

- Device may be taken away by the teacher for the lesson.
- Device may be taken away by the teacher and held securely in the College's Hub until collected by the student at the end of the day.
- In certain circumstances, the device may be taken away by the teacher and held securely in the College's Hub until collected by the parent/carer.
- Student not allowed to use personal devices in College.
- Disciplinary referral resulting in internal or external exclusion.

School Liability Statement:

Students bring their devices to use at Torpoint Community College at their own risk. It is their duty to be responsible for the upkeep and protection of their devices.

Torpoint Community College is in no way responsible for:

- Personal devices that are damaged or broken whilst at school or during school-sponsored activities.
- Personal devices that are lost or stolen at school or during school-sponsored activities.

Use of Torpoint Community College iPads:

- The College will provide iPads or iPad Minis for use in lessons for students who do not have their own devices. The iPads will be used in small groups.
- Students must only use the iPads at the direction of the teacher.
- Students are liable for damages to the iPads if caused by misuse.

Remote Learning

Due to an increase in the use of remote learning, staff and students need to be aware of their roles and responsibilities.

Where a staff member is accessing personal data from home for the purposes of completing remote learning needs, staff need to ensure they keep their personal devices safe and secure and utilise the same security practices as if they were in College in so much as is possible. Examples of such measures include but are not exclusive to:

- Keep the device password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Encrypt the hard drive - this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Make sure the device locks if left inactive for a period of time
- Avoid sharing the devices among family or friends
- Install antivirus and anti-spyware software

- Keep operating systems up to date - always install the latest updates

Students are also expected to conform, in so much as is possible, to the expectations of conduct and behaviour set out in the online safety policy and online behaviour policy when engaging in remote learning. Where it is evident a student hasn't met our expectations, the College may contact the student and parent/carer to address the concern.

Staying Safe when Teaching Remotely

- Always follow the College safeguarding/ online safety policy
- Only run live sessions using Microsoft Teams
- Aim to run live sessions with 3 or more participants. If only one pupil accesses a live session, ask a colleague to join the meeting as a passive observer. If this is not possible, a 1 to 1 discussion can happen, but you may want to consider if it is appropriate to record the session (with permission from the student) in order to safeguard yourself and the student.
- Ensure students know that anything typed in the chat is public and all members of the Team can read it.
- Always use College email address when interacting with students
- Plan ahead: dress appropriately, ensure a neutral background and make behaviour expectations clear to students at the beginning of any live sessions
- Inform the DSLs immediately if you have any safeguarding concerns about students
- Ask students to locate themselves in a shared family space for live sessions rather than their bedroom
- Ensure the settings mean the teacher is in control of the screen (see training videos on CPD portal)
- When delivering an interactive session online, teachers should make a note of the lesson timing and who participated.
- Pupils may not record sessions without the teacher's permission, and should not be permitted to record other pupils' participations
- Teachers should not upload recorded lessons to SMHW or other online platforms

Social Networking

Social networking websites provide an opportunity for people to communicate en masse and share ideas regardless of geographic distance.

However, the open nature of the Internet means that social networking sites can leave professionals such as teachers vulnerable if they fail to observe a few simple precautions. The below guidelines are intended not as a set of instructions, but general advice on how to avoid compromising your professional position. You should note that Part two of the teacher's standards make it clear the expectations of how teachers should demonstrate high standards of personal and professional conduct, this can include activities online.

Privacy

To ensure that your Facebook account does not compromise your professional position, please ensure that your privacy settings are set correctly. Privacy settings change frequently so they should be checked by the account holder on a regular basis. Please refer to the College's Social Media Policy for further information.

It is recommended that you do not accept friend requests from a person you believe to be either a parent or a student at the College; this includes ex-students who may have siblings or other relatives at the College.

Privacy Setting Recommended Security Level

Example settings (note these can change frequently but can be reviewed under the 'settings and privacy options in settings):

- Send your messages Friends only
- See your friend list Friends only
- See your education and work Friends only
- See your current city and hometown Friends only
- See your likes, activities and other connections Friends only
- Your status, photos, and posts Friends only
- Bio and favourite quotations Friends only
- Family and relationships Friends only
- Photos and videos you're tagged in Friends only
- Religious and political views Friends only
- Birthday Friends only
- Permission to comment on your posts Friends only
- Places you check in to Friends only
- Contact information Friends only
- Set up unrecognised login alerts
- Set up extra security, such as two-factor authentication
- Run 'Security/Privacy Check-up' to review and add more security to your account

Always make sure that you log out of Facebook after using it, particularly when using a machine that is shared with other colleagues. We strongly recommend that you don't use Facebook whilst in college and especially on computers that students have access to. Your account can be hijacked by others if you remain logged in – even if you quit your browser and/or switch the machine off. Similarly, Facebook's instant chat facility caches conversations that can be viewed later on. Make sure you clear your chat history on Facebook (click "Clear Chat history" in the chat window). Also, watch out for scams or phishing and report fake accounts.

Conduct on Social Networking Sites

Do not make disparaging remarks about the College or your colleagues. Doing this in the presence of others may be deemed as bullying and/or harassment.

Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed.

If you have a concern about information on your social networking site, or if you are the victim of cyber-bullying, you should notify your line manager / Headteacher immediately.

Do not publish your date of birth and home address on Facebook. Identity theft is a crime on the rise with criminals using such information to access to your bank or credit card account. Stop the network provider from passing on your details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click

"Privacy Settings". Under "Applications and websites" click "edit your settings". Scroll down to "instant personalisation" and make sure the checkbox for "enable instant personalisation on partner websites" is unchecked.

Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.

Laptop and other Similar Devices

All laptop usage is bound by the rules contained in the current Torpoint Community College User Agreement. As laptops are portable there is a greater risk of physical damage or theft. Any person with access to a Torpoint Community College laptop must assume a reasonable amount of responsibility for its safety against theft or damage. In the event that a laptop is presumed stolen, Torpoint Community College ICT Network Manager must be notified immediately and a police report must be filed. Torpoint Community College ICT Network Manager must receive a copy of this report.

No unauthorised software shall be installed on any Torpoint Community College owned computer, including laptops. Prohibited software includes, but is not limited to, such programs that allow downloading and/or distribution of copyright material such as games, music, movies, etc. These types of programs introduce a security risk to the College computing environment. Any person holding administrative rights to a laptop in their possession must be held responsible for ensuring that updates of the operating system and virus scanner are carried out to the College standards. Automatic updates will be set up for those laptop users who do not have administrative rights.

The College reserves the right to audit any laptop at any time.

Any abuse that occurs may result in laptops being prohibited from leaving Torpoint Community College property or the suspension of computer account privileges.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Dealing with harmful online challenges and online hoaxes

A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.

Children and young people should be free to enjoy the internet safely. The online environment you create, how your institution plans and responds to harmful online challenges and online hoaxes, and how your institution teaches about online safety, are important.

Below is a useful guide to approaching such harmful challenges and hoaxes and underpins our responses to them.

https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes

Unsuitable/Inappropriate Activities

The College believes that the activities referred to in the following section would be inappropriate in a College context and that users, as defined below, should not engage in these activities in College or outside College when using College equipment or systems.

The College policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images/ pornographic images of children/ youth-produced sexual imagery					X
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the College or brings the College into disrepute				X	
Using College systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the College					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					X	
On-line gaming (educational)			X			
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce				X		
File sharing					X	
Use of social networking sites			X			
Use of video broadcasting e.g. YouTube				X		

Responding to Incidents of Misuse

It is hoped that all members of the College community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.:

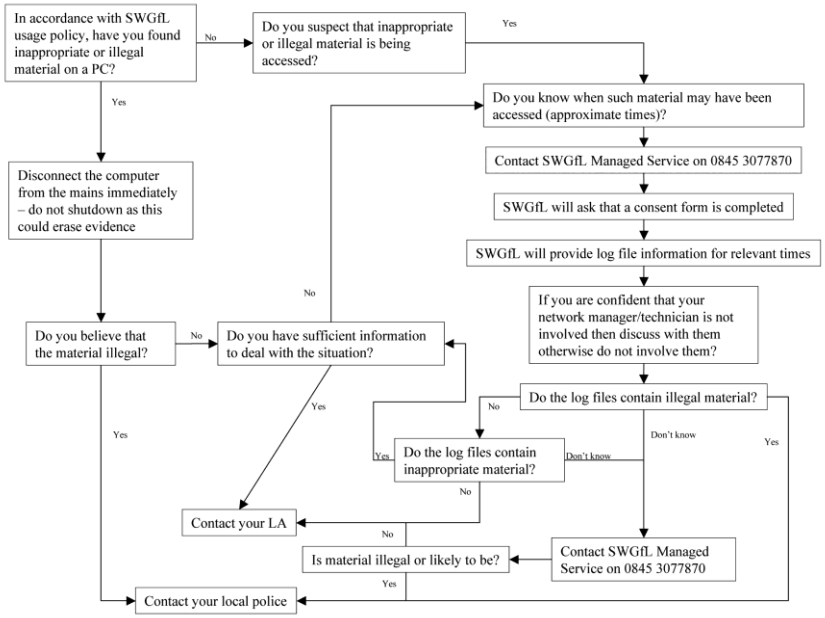
- child sexual abuse images;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials;
- potentially extreme material.

All concerns will be raised with DSL team and recorded on CPOMs.

Our protocol for responding to instances of sexting or youth-produced sexual imagery follows government guidelines, which can be found as follows:

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

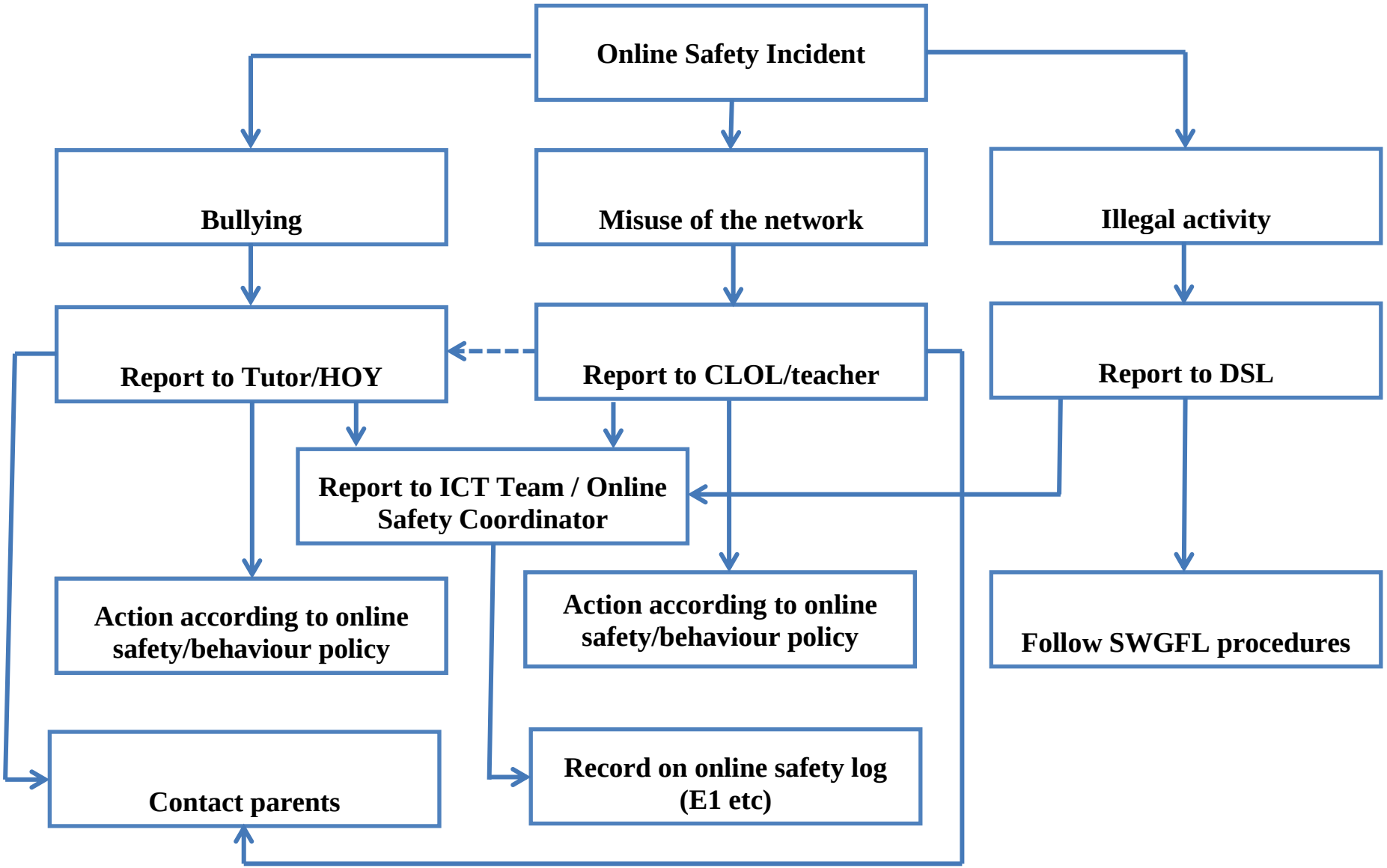
The SWGfL flow chart (below) and online safety resources should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If a member of staff suspects that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that the online safety Coordinator (for students) / Headteacher (for staff) is informed

It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the College community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:



Students Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer CLOL/HOY	Refer to Deputy Headteacher /Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x	x	x	x		x
Unauthorised use of non-educational sites during lessons	x	x						x	
Unauthorised use of mobile phone / digital camera / other handheld device	x	x						x	
Unauthorised use of social networking / instant messaging / personal email	x	x						x	
Unauthorised downloading or uploading of files		x			x	x	x		x
Allowing others to access College network by sharing username and passwords		x			x	x	x		x
Attempting to access or accessing the College network, using another student's / pupil's account		x			x	x	x		x
Attempting to access or accessing the College network, using the account of a member of staff		x	x		x	x	x		x
Corrupting or destroying the data of other users		x	x		x	x	x		x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x			x	x	x		x
Continued infringements of the above, following previous warnings or sanctions		x	x	x	x	x	x		x
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College		x	x	x		x			x
Using proxy sites or other means to subvert the College's filtering system		x	x	x	x	x	x		x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x						x	
Deliberately accessing or trying to access offensive or pornographic material		x	x		x	x	x		x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x				x			x

Actions / Sanctions

Staff

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x			x	x
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	x					x		
Unauthorised downloading or uploading of files	x				x	x		
Allowing others to access College network by sharing username and passwords or attempting to access or accessing the College network, using another person's account	x				x	x		
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x			x	x		
Deliberate actions to breach data protection or network security rules	x	x			x		x	x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x			x		x	x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x	x						x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x					x	x
Actions which could compromise the staff member's professional standing	x	x				x		x
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College		x						
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x			x	x		
Deliberately accessing or trying to access offensive or pornographic material		x			x		x	x
Breaching copyright or licensing regulations	x					x		
Continued infringements of the above, following previous warnings or sanctions	x	x					x	x

FORM A

STAFF, GOVERNOR VOLUNTEER AND VISITOR ACCEPTABLE USE POLICY AGREEMENT

College Online Safety Policy - Overview

New technologies have become integral to the lives of children and young people in today's society, both within Colleges and in their lives outside College. 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 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 College 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 College 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. The full E-safety Policy should be referred to also.

Staff Acceptable Use Policy Agreement

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. 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.

Please note in this College safeguarding young people is paramount. All staff have received training re the Prevent Duty and understand their responsibility to prevent extremism and radicalisation. Students have been advised about the issues surrounding this.

For my professional and personal safety:

- I understand that the College will monitor, and record where appropriate, my use of the ICT systems, e-mail and other digital communications.
- I understand that the rules set out in this agreement also apply to use of College ICT systems (e.g. laptops, email, remote access etc) out of College.
- I understand that the College 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 College.
- 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 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 College 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 I will do so with their permission and in accordance with the College's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the College website / Facebook) it will not be possible to identify by name, or other personal information, those who are featured unless parental / carer consent has been given.
- I will only use chat and social networking sites in College in accordance with the College's policies.
- I will only communicate with students and parents / carers using official College 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 College and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the College:

- When I use my personal hand held / external devices (laptops, mobile phones, USB devices etc) in College, I will follow the rules set out in this agreement, in the same way as if I was using College equipment. I will also follow any additional rules set by the College about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses and malware.
- 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 programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant College policies.
- 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 programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- 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 programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have been given permission.
- I will not disable or cause any damage to College 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 College Data Protection Policy & in line with GDPR. Where personal data is transferred outside the secure College network, it must be password protected or encrypted where possible.
- I understand that 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 College 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 College 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 College:

- I understand that this Acceptable Use Policy applies not only to my work and use of College ICT equipment in College, but also applies to my use of College ICT systems and equipment out of College and my use of personal equipment in College or in situations related to my employment by the College.

- 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 and / or the Local Authority and in the event of illegal activities the involvement of the police.

The following are extensions of this Policy:

Form B: SIMS Permission Request
Form C: External Storage Device

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

Staff / Volunteer Name	
Signed	
Date	

Original forms will be held by the College's HR Manager on Personnel Files..

FORM B

SIMs Permissions Request Form

Name: _____ Date: _____

Job Title: _____

Department: _____

I require the access rights listed below to parts of the Torpoint Community College SIMs system to enable me to perform my role within the college. This may include sensitive and confidential data for which I will fully comply with the College's Data Protection Policy.

Signature: _____ Name: _____ Date: _____

Section 1

To fulfil my role within the College I need to access a particular part of SIMs that I currently do not have access to, this area is titled _____ and to complete my work I need Read Only / Editing (Delete as appropriate) permissions to this area.

Section 2

The permissions I need access to within SIMs are as follows (Tick all appropriate)

Permission Group	**Edit**	**Read**	**Permission Group**	**Edit**	**Read**
Admissions			Personnel		
Assessment			Registration Tutor		
Attendance			Returns Manager		
Bursar			School Administrator		
Class Teacher			SEN Coordinator		
Cover Manager			Senior Management Team		
Exams Officer			System Manager		
Pastoral Manager			Timetabler		
Others (please List)					

This Change has been checked and authorised by a member of CLT.

Name: _____

Job Title: _____ *(Members of CLT to complete this section)*

Signed: _____ Date: _____

*Authorised permissions updated in SIMs.

Signature: _____

Name: _____

Appointment: _____

Date: _____

**To be completed by a member of the ICT Team.*

FORM C

EXTERNAL STORAGE DEVICES

Torpoint Community College

Guidelines for the responsible and safe use of External Storage Devices

ROLES AND RESPONSIBILITIES

- All allocated external devices are the property of the college, and as such must be signed for before their allocation and identification details will be added to the college's inventory of ICT equipment.
- The External Storage Devices allocated are a valuable college resource; it is a condition of the loan that staff make best efforts to ensure the device remains in a good and working order.
- External Storage Devices are allocated to named individuals on long-term loan. Staff should retain the equipment for the duration that they work at the college. The device must be returned to the college for reallocation to another staff member when the original recipient ceases employment at the college.
- Staff should ensure the safety of the device and ensure it is kept secure with access only being given to those who are sanctioned to review the data held on the device.
- If the device is encrypted the password must remain secure with an enveloped copy stored in the college safe, if this step is not followed and the password is lost the data will be irretrievable.
- It is the recipient's responsibility to ensure that all information stored on the device is school property and no illegal data is held on it. If illegal data is found on the device the individual allocated the device will be held responsible and steps taken to reprimand that individual.
- Staff must ensure the device is stored safe at all times and the data on the device remains secure.

I understand and agree to the terms and conditions above.

Staff Name: _____

Staff Signature: _____

Device Make/Model: _____

Device Serial Number: _____

Date of Collection: / /

FORM D

LAPTOPS

Torpoint Community College

Guidelines for the responsible and safe use of Laptops

ROLES AND RESPONSIBILITIES

- The laptops are the property of the College, and as such details will be added to the College's inventory of ICT equipment.
- It is strongly recommended that staff update the laptops virus definition files and Windows Updates regularly. (Please consult the ICT Team for help, if required).
- The laptops allocated are a valuable educational resource; it is a condition of the loan that staff make best efforts to ensure the laptop remains in a good and working order.
- Laptops are allocated to named individuals on long-term loan. Staff should retain the equipment for the duration that they work at the College. The laptop must be returned to the College for reallocation to another staff member when the original recipient ceases employment at the College.
- Staff should ensure that regular external backups are taken (e.g. memory sticks, recordable DVD's, etc.) of all work saved on their allocated laptop. In the event of a system failure this work may be lost.
- It is the recipient's responsibility to ensure that all additional software installed or run on this laptop is legal and licensed correctly.
- Staff should also ensure they have appropriate insurance arrangements in place to cover accidental damage / loss of the equipment for which they will be liable for the replacement cost (this will be based on the cost incurred by the College to source a new like for like piece of equipment).
- College laptops / portable devices issued to staff for use off site are only to be used by the individual. Any breach of this policy may result in the item being withdrawn. Note the ICT Team can request the return of College laptops / portable devices for audit purposes, software upgrades and virus checks at any time; this may include a check of system logs to ensure appropriate usage.

I understand and agree to the terms and conditions above.

Staff Name: _____

Staff Signature: _____

Laptop Make/Model: _____

Laptop Serial Number: _____

Date of Collection: / /

Student Acceptable Use Policy

There are over 300 computers available to TCC students with a range of software including internet, e-mail, Office etc. All activity on the ICT network, including emails, user areas and internet history, are constantly monitored. Misuse of the College system will result in disciplinary action in line with current College policies. Note all relevant information can be found on your desktop.

Students are also allowed, in some circumstances, to bring electronic devices, such as mobile phones, to College. With this privilege comes the understanding that students will follow our behavioural expectations and use such devices responsibly and in line with our College expectations.

Please note that the safeguarding of young people is paramount in TCC. All staff have received training re the Prevent Duty and understand their responsibility to prevent extremism and radicalisation. Students have been advised about the issues surrounding this.

The following policy will ensure the ICT resources and privilege of technology is used safely, responsibly and appropriately.

- The taking of photographs or images or videos or recordings or other content of teachers, adults or students without consent is strictly forbidden. It is also strictly forbidden to take inappropriate images or videos or recordings or other content of students or staff.
- Students will report any computer faults they find immediately to a member of staff without attempting to fix the problem themselves.
- Students will treat the ICT resources with respect, leaving them as they would expect to find them.
- Students must ask permission from a member of staff before using ICT resources.
- Under no circumstances is food or drink to be consumed within the Colleges ICT suites.
- Students will use their own unique login to access the network and make no attempts to gain access to the network through another's login details.
- Students may use the Colleges ICT resources for educational purposes only.
- Students are strictly forbidden from accessing any form of social media or chat room style webpages whilst using the College ICT systems.
- No software or unauthorised files (i.e. files not relating to valid College activities) are to be brought in and used or installed on the network. No College software is to be copied.
- Use of e-mail is for educational purposes only. As such, it is only to be used with permission from the class teacher. All emails sent from your College email must be polite and sensible.
- Students may not disclose their personal details (such as their phone number or address), or the personal details of anyone else whilst using the internet/e-mail.
- Students should inform a teacher about any inappropriate content seen on the computer/internet/e-mail.
- Any use of the College network is monitored, the College reserves the right to copy information and disable accounts without prior warning in the event of a suspected breach of the College policy or inappropriate/unlawful use of the network.
- Students may not use the ICT facilities to use/create/distribute offensive material.
- Students must not attempt to hack into the College ICT system. This will be deemed as a malicious act to cause damage to College property and will be dealt with accordingly.
- The network is provided for educational purposes and should only be used for educational reasons, playing games is not acceptable and will be dealt with accordingly.
- When using ICT facilities you must always respect copyright and not plagiarise the work of others.

- The College reserves the right to update this policy at any time.

Photographs, videos, recordings or other content must not be taken in College unless given permission by the teacher / member of staff. All images can be subject to copyright. This should be taken into account when taking and using photos, videos recordings or other content.

Any offences relating to the above will remain on a student's record for the entire duration of their time at Torpoint Community College. Where applicable, the police or local authority may be involved.

Use of Digital/Video Images

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

Images may also be used to celebrate success through their publication in newsletters, on the College website and occasionally in the public media.

The College will comply with the Data Protection Act and request parents / carers permission before taking images of members of the College. We will also ensure that when images are published that the young people cannot be identified by the use of their names unless parental / carer consent has been given.

Parents are requested to sign the permission form below to allow the College to take and use images of their children.

Permission Form

As the parent / carer of the student names below, I agree to the College taking and using digital/video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the College.

I agree that if I take digital or video images at, or of, College events which include images of children, other than my own; I will abide by these guidelines in my use of these images.

Student Name

Parent / Carers Name

Signed

Date

The following links may help those who are developing or reviewing a College online safety policy:

SOUTH WEST GRID FOR LEARNING:
- http://www.swgfl.org.uk/products-services/esafety

Child Exploitation and Online Protection Centre (CEOP)
http://www.ceop.gov.uk/

ThinkUKnow
http://www.thinkuknow.co.uk/

CHILDNET
http://www.childnet-int.org/

BETTER INTERNET FOR KIDS
https://www.betterinternetforkids.eu

UK COUNCIL FOR CHILD INTERNET SAFETY
(UKCCIS)https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

UK Safer Internet Centre
https://www.saferinternet.org.uk/

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
Cyberbullying.org - http://www.cyberbullying.org/

East Sussex Council – Cyberbullying - A Guide for Colleges:
https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx

PARENTS GUIDES TO NEW TECHNOLOGIES AND SOCIAL NETWORKING:
http://www.iab.ie/

RESOURCES

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and College staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL E-Safety" website:

http://www.swgfl.org.uk/products-services/esafety

Links to other resource providers:

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

NCH - http://www.stoptextbully.com/

Childnet International - www.childnet.comInternet Watch Foundation: http://www.iwf.org.uk/

Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx

FORM G

Staff Acceptable Internet Use Policy – User Based Filtering (July 2016)

I understand:

- The College ICT system provides Internet access to students and staff. This Acceptable Use Policy will help protect students, staff and the College by clearly stating what is acceptable and what is not
- When accessing the internet there will be limited filtering on my account. I will therefore ensure I take the necessary steps, when teaching or presenting (if applicable), to prevent inappropriate material appearing on my computer / projected screen when conducting an internet search
- I will always ensure my computer is locked, logged off or secured upon leaving the workstation
- The authorised member of staff's account and password must not be given to any other person and, if written down, it will be stored in a secure area
- Computer and internet use during working hours must be appropriate to the student's education and or the member of staff's professional role within the College
- Copyright and intellectual property must be respected
- The ICT system must not be used for personal financial gain, gambling, political purposes or advertising.
- The Copyright, Design and Patents Act makes the unlicensed copying of software a criminal offence
- In accordance with The Regulation of Investigatory Powers Act 2000, Regulation 3.(1) authorises employers to monitor and record communications without consent for the following purposes:
    - To establish the existence of facts relevant to the business (of the College)
    - To ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the business – this would include monitoring as a means of checking that the College's business is complying with external regulatory or internal regulatory rules or guidelines
    - To prevent or detect crime – for example, monitoring to ensure employees do not breach rules or policies on use of the e-mail system or the internet
    - To ensure the effective operations of the system – this may include monitoring for viruses or other threats to the system.
- The Regulations also authorise monitoring (but not recording) without consent for the purposes of determining whether or not the communications are relevant to the College. An example is the opening of e-mail accounts in order to access College communications when a member of staff is on holiday or off sick.

Signature: ……. Date: ……..

Name: ……..

FORM H

TCC ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	