TRINITY SCHOOL CARLISLE

A CHURCH OF ENGLAND ACADEMY

E-SAFETY POLICY

Minor changes and updates to reflect introduction of GDPR and the Data Protection Act 2018	October 2018
Additional content added in response to the E-safety working group discussions/recommendations. Also changes re Co-Headteachers to Headteacher.	October 2019
Periodic Review – Updated line with Keeping Children Safe in Education 2020.	October 2020

Pastoral Committee
Reviewed: October 2020
Approved by the Pastoral Committee: November 2020
Ratified by the Full Governing Body: December 2020
Next review: October 2021

Contents

1. Background/Rationale

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 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 school E-Safety Policy helps to ensure safe and appropriate use.

The use of these exciting and innovative tools in school 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 school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images 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 risk of being targeted by extremists in order to promote and encourage radicalisation.
- The risk of being targeted by those involved in child sexual exploitation.
- The sharing/distribution of personal images 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 that may impact on the social and emotional development and learning of the young person.

2. Development/Monitoring/Review of this Policy

This E-Safety Policy has been developed through a consultative process involving the School's Senior Leadership Team, IT Services Manager and the School's E-Safety Co-Ordinator with reference to appropriate national guidelines and should be read in conjunction with other associated school polices (see appendices), and, where they exist, addendums to those Policies and procedures:

The policy is shared with staff, students, and parents/carers in a variety of ways:

- We have a clear policy on the use of mobile devices in school
- Parents/carers sign an acceptable use of ICT agreement prior to admission of their children
- We have information booklets for students and parents/carers that provide information on acceptable and safe on-line behaviour including personal safety and on-line bullying.
- Students sign an annual electronic copy of the "Acceptable Use Policy"
- Regular assemblies and "Freeze Sessions" for all year groups are used to reinforce what constitutes safe and acceptable online behaviour.

3. Scope of the Policy

This policy applies to all members of the school 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.

4. Complaints

Parents, teachers and students know how to use the school's complaints procedure. E-Safety incidents may have an impact on students. staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

Action is decided upon based on the specifics of an incident:

- A minor transgression of the school rules may be dealt with by a member of staff.
- For more serious situations a range of sanctions may be required, which will be based on the school's Behaviour Policy.
- Potential child protection or illegal issues are referred to the school Designated Safeguarding Lead. Advice on dealing with illegal use can, when deemed necessary, be discussed with the Police or Cumbria Safeguarding Hub.

CAVEAT:

- The school takes all reasonable precautions to ensure E-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable materials will never appear on a school computer or mobile device. Neither the school staff nor the Governing Body/Board of Directors can accept liability for material accessed, or any consequences of Internet access.
- Complaints about internet misuse will be dealt with under the school's Complaints procedure.
- Complaints about cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.
- Any complaints about staff misuse will be referred to the Headteacher.
- All e-safety complaints and incidents will be recorded by the school including any actions taken (see Appendix 5).

  Staff and students are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by class teacher/Head of Year/E-Safety Coordinator/Headteacher.
- Informing parents.
- Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework).
- Referral to the Police.

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

- *All members of the school community are reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community or which may bring the school into disrepute.*

5. Roles and Responsibilities

5.1 Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Pastoral Committee of the Governing Body receiving regular information about E-Safety incidents and monitoring, filtering/change reports etc.

5.2 Headteacher and Senior Leaders

The Headteacher has overall responsibility for e-safety provision. The day to day responsibility for E-Safety may be delegated to the E-Safety *Co-ordinator*.

- The Headteacher takes overall responsibility for data and data security.

- The Headteacher ensures the school uses an approved, filtered Internet Service, which complies with current statutory requirements.
- The Headteacher ensures that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher and SLT will ensure that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Headteacher and SLT will ensure that suitable processes and tools are in place to monitor on-line behaviour in school
- The Headteacher and SLT will ensure that suitable reporting procedures are in place to report incidents to themselves and to the E-Safety Coordinator
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Coordinator.
- The Headteacher and Senior Leadership Team must ensure procedures are in place in the event of a serious E-Safety allegation being made against a member of staff
- The Headteacher and Senior Leadership Team must be aware of the procedures to be followed in the event of a serious E-Safety incident or an allegation being made against a member of staff or volunteer (see flow chart on dealing with E-Safety incidents – Appendix 4, and relevant Local Authority HR/school disciplinary procedures). The procedures for dealing with allegations against staff or volunteers can be found within the school Child Protection Policy and all staff/volunteers are provided with a copy on induction.

The E-Safety Co-ordinator/Designated Safeguarding Lead will:

The DSL may delegate certain online safety duties e.g. to the OSL, but not the day-to-day responsibility; this assertion and all items below are taken from Keeping Children Safe in Education.

- take lead responsibility for safeguarding and child protection (including online safety);
- ensure an effective approach to online safety is in place that empowers the school to protect and educate the whole school community in their use of technology and establish mechanisms to identify, intervene in and escalate any incident where appropriate;
- promote an awareness and commitment to online safety throughout the school community with strong focus on parents, who are often appreciative of school support in this area, but also including 'hard-to-reach' parents;
- liaise with other agencies in line with 'Working together to Safeguard Children' statutory guidance;
- take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns;
- ensure that online safety education is embedded in line with DfE guidance 'Teaching Online Safety in schools' across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World') and beyond, in the wider school community;
- work with the Head teacher, Data Protection Officer, Governors and the school ICT technical staff to ensure a DPA compliant framework for storing data, helping to ensure that child protection is always at the fore and data protection processes support careful and legal sharing of information;
- keep up to date with the latest local and national trends in online safety;
- review and update this Policy and procedures, other online safety documents (e.g. Acceptable Use Agreements) and the strategy on which they are based (in line with Policies and procedures for behaviour and child protection) and submit for review on a regular basis to the Governors/Trustees;
- liaise with school technical, pastoral, and support staff as appropriate;
- communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident and that these are logged in the same way as any other child protection incident;

- oversee and discuss 'appropriate filtering and monitoring' with Governors (both physical and technical) and ensure staff are aware of its necessity;
- ensure the DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this as well as to bullying generally;
- facilitate training and advice for staff and others working in the school:

    - all staff must read and understand KCSiE Part one and all those working with children, Annex A;
    - it would also be advisable for all staff to be aware of Annex C (Online safety);
    - cascade knowledge of risks and opportunities throughout the organisation;

- be aware of emerging online safety issues and legislation, and of the potential for serious child protection issues to arise from:

    - sharing of personal data;
    - access to illegal/inappropriate materials;
    - inappropriate online contact with adults/strangers;
    - potential or actual incidents of grooming;
    - cyberbullying and the use of social media.

5.3 ICT Services Manager

The ICT Services Manager has the following responsibilities. To ensure that:

- report any online safety related issues that arise, to the Headteacher.
- that the school meets the online safety technical requirements outlined in the School Acceptable Use Agreements and any relevant Local Authority Online Safety Policy and guidance.
- ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices.
- the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- users may only access the school's networks through a properly enforced password protection policy, in which passwords are allocated and controlled by the ICT Services Manager.
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- 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 Coordinator/DSL for investigation/action/sanction.
- that monitoring software/systems are implemented and updated as agreed in school policies.
- that he/she keeps up to date with the school's Online Safety Policy and procedures and technical information to effectively carry out their Online safety role and to inform and update others as relevant.
- ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster and to complement the business continuity process;
- keep up-to-date documentation of the school's e-security and technical procedures.

5.4 Teaching and Support Staff

It is the responsibility of all staff to:

- understand that online safety is a core part of safeguarding; as such it is part of everyone's role. Never think that 'someone else will pick it up';
- know who the Designated Safeguarding Lead and Online Safety Lead are; [amend if the same person]
- read and understand Part 1, Annex A and Annex C of 'Keeping Children Safe in Education' statutory guidance – whilst Part 1 is statutory for all staff, Annex A for SLT and whose working directly with children, it is good practice for all staff to read all three sections;

- read, understand and help promote the school's Online Safety Policy and procedures in conjunction with the Child Protection and other related school Policies and procedures;
- read, sign and follow the school Staff Acceptable Use Agreement and staff Code of Conduct;
- be aware of online safety issues related to the use of mobile technology e.g. phones, cameras and other hand-held devices and follow school procedures in relation to these devices;
- ensure the security of their username and password for the school system, 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. Passwords will be changed on a regular basis and at least every 6 months; [school to amend if timescales differ]
- record online safety incidents in the same way as any child protection incident and report incidents to the DSL/OSL in accordance with school procedures;
- notify the DSL/OSL if policy does not reflect practice in the school and follow escalation procedures if concerns are not promptly acted upon;
- identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise;
- whenever overseeing the use of technology (devices, the Internet, new technology such as augmented reality, etc.) in school or setting as homework tasks, encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites (check what appropriate filtering and monitoring processes are in place);
- carefully supervise and guide students when engaged in learning activities involving online technology, supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law;
- prepare and check all online source and resources before using in the classroom;
- encourage students to follow their Acceptable Use Agreement, regularly remind them about it and enforce school sanctions where there is a breach of the Agreement;
- notify the DSL/OSL of new trends and issues before they become a problem;
- take a zero-tolerance approach to bullying and low-level sexual harassment either offline or online;
- receive and act upon regular updates from the DSL/OSL and have a healthy curiosity for online safety issues;
- model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and the professional reputation of all staff;
- ensure that any digital communications with students are on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones or social media messaging or posts.

5.5 Designated Safeguarding Lead

This individual is fully conversant with E-Safety issues and 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.
- potential or actual incidents of grooming.
- Cyber-bullying.

5.6 Data Manager

It is the responsibility of the Data Manager to ensure that all data held on students on school office machines have appropriate access controls in place and that systems and procedures comply with the General Data Protection Regulations.

5.7 E-Safety Committee

The key responsibility of this group comprising Senior Leadership, the ICT Services Manager (or delegated colleague) and E-Safety Coordinator is the production, review and monitoring of the school E-Safety Policy and associated documents.

5.8 Students

Students of all age groups are:

- responsible for using the school ICT systems in accordance with Acceptable Use Policy have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- taught the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- 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 and use of images and on cyber-bullying.
- taught the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- help the school in the creation/review of the E-Safety Policy and procedures.

5.9 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.

- School takes every opportunity to help parents understand these issues through tutor evenings, newsletters, information packs, and published information on the website and providing guidelines on safe and acceptable use of social networking and internet sites (appendix 2).

Parents and carers will be responsible for:

- endorsing the school's Acceptable Use Policy through signature of the Home School Agreement.
- accessing the school website and VLE(s) in accordance with the relevant school Acceptable Use Policy.

Staff and Governor Training

As a School we endeavour to develop competencies to maintain pace with ever changing technologies. We aim to:

- ensure that staff know how to send or receive sensitive and personal data in accordance with GDPR and understand the requirement to encrypt data where the sensitivity requires data protection.
- make regular training available to staff on online safety issues. This may be e-training, monthly bulletins, or alerts to articles posted on the School website.
- provide, as part of the induction process, all new staff (including those on university/college placements and work experience) and volunteers with information and guidance on the Online Safety Policy and procedures the school's Acceptable Use Agreements.

Parent Awareness and Training

We also recognise the importance of alerting parents/carers to e-safety matters. We operate a rolling programme of advice, guidance and training for parents/carers, including:

- the introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear.
- the provision of information leaflets, articles in the school newsletter and on the school website in a dedicated e-safety section.
- suggestions for safe Internet use at home.
- the provision of information about national support sites for parents.

6. Managing Information Systems

6.1 Maintaining Information Systems Security

School ensures the security of ICT systems, information and personal data in a variety of ways:

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without an anti-virus/malware scan.
- Staff Devices and portable media will always be encrypted.
- Unapproved software will not be allowed on the school network.
- Files held on the school's network will be regularly checked.
- The Network Manager will review system capacity regularly.
- Use of user logins and passwords to access the school network will be enforced
- The school broadband and online suppliers are Virtue Technologies

6.2 Password Security

The school is responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access;
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's procedures);
- access to personal data is securely controlled in line with the school's personal data procedures;

The management of password security will be the responsibility of ICT Services Manager.

Responsibilities:

All users (adults and young people) will have responsibility 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.

Passwords for new users, and replacement passwords for existing users can be allocated by the ICT Services Team. Any changes carried out must be notified to the member of staff responsible for issuing and coordinating password security.

Training/Awareness:

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the school's password security procedures:

- through the school's Online Safety Policy and procedures;
- through the Acceptable Use Agreement;

Students will be made aware of the school's password security procedures:

- in KS3 ICT lessons and during specially organised online safety activities, including external agency presentations/workshops as part of the Personal Development additionality curriculum
- through the Acceptable Use Agreement

The following rules apply to the use of passwords:

- The Initial password will be a minimum of 5 characters long and will take the format of XX1x1 (CapitalCapitalNumberLowerCaseNumber).
- Future passwords *should* be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special character;
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption);
- requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine

The Administrator passwords for the school ICT system, used by the ICT Services Team must also be available to the Headteacher or other nominated senior leader. These are Kept electronically in a secure location.

Audit/Monitoring/Reporting/Review:

The ICT Services Manager will ensure that full records are kept of:

- User log-ons;
- Security incidents related to this Policy and procedures.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

6.3 Managing Email

School's policy is based on the principles below:

- Students may only use approved email accounts for school purposes.
- Students must immediately tell a designated member of staff if they receive an offensive email or one which upsets or worries them.
- Students must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with students and parents, as approved by the Senior Leadership Team.
- Email sent to external organisations should be written carefully. Very sensitive mail should be cross checked before sending.
- The forwarding of chain messages is not permitted.
- Schools will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school Policy and procedures, 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 (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be

reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Spam, phishing and virus attachments can make email dangerous. The school ensures mail is virus checked (ingoing and outgoing), includes spam filtering.

6.4 Emailing personal, sensitive, confidential or classified information

- Assess whether the information can be transmitted by other secure means before using email - emailing confidential data is not recommended and should be avoided where possible;
- The use of personal webmail services for sending email containing sensitive information is not permitted;
- Where your conclusion is that email must be used to transmit such data:
- Exercise caution when sending the email and always follow these checks before releasing the email:
    - Verify the details, including accurate email address, of any intended recipient of the information; do not copy or forward the email to any more recipients than is necessary.
    - Send the information as an encrypted document **attached** to an email;
    - Provide the encryption key or password by a **separate** contact with the recipient(s);
    - Do not identify such information in the subject line of any email;
    - Request confirmation of safe receipt

6.5 Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left;
- Prompt action on disabling accounts will prevent unauthorised access;

6.6 Managing Published Content

- The contact details on the website are the school address, email and telephone number only.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy procedures and copyright.

6.7 Use of Digital and Video Images

- School teaches and informs staff, students and parents/carers about the risks and legal issues associated with the taking, use, sharing, publication and distribution of images.

6.8 Managing Social Networking, Social Media and Personal Publishing Sites

School's policy encompasses the principles below:

- The school will control access to social media and social networking sites.
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for student use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Student will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding a student's use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents, particularly when concerning the underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and outlined in the school Staff Acceptable Use Agreement

6.9 Managing Filtering

The school's broadband access includes:

- The school's broadband access will include filtering appropriate to the age of students.
- The school will work with Virtue Technologies to ensure that filtering procedures are continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all students) will be aware of this procedure.
- If staff or students discover unsuitable sites, the URL will be reported to the School Online Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list
- Changes to the school filtering procedures will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Cumbria Police or CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers.

6.10 Webcams and CCTV

The school uses CCTV for security and safety. The only people with access to this are The Premises Manager, Network Support Staff and Senior Leadership Team. Notification of CCTV use is displayed at the front of the school. All CCTV data is securely stored in accordance with the school CCTV policy. It is important to also note that we do not use publicly accessible webcams in school.

6.11 Emerging technologies

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections that can be highly beneficial educationally.

We aim to keep up to date with new technologies, including those relating to mobile phones and handheld devices, and to adopt appropriate strategies.

School will undertake the following:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- *Students will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.*

6.12 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and GDPR which states that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals.
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up to date.
- kept for no longer than is necessary.
- processed in a manner that ensures appropriate security of it.

7. Policy Decisions

7.1 Authorising Internet Access

- The school maintains a current record of all staff and students who are granted access to the school's electronic communications.
- Everyone will read and sign the Acceptable Use Agreement before using any school ICT resources. This is done electronically at First log on and will be re-signed periodically.
- Use of ICT is monitored and logs maintained. any misuse incurs sanctions including temporary or permanent bans.
- Reports of incidences of ICT/internet misuse can be electronically produced as needs.
- Students will apply for Internet access individually by agreeing to comply with the School Acceptable Use Policy.

7.2 Assessing Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Virtue Technologies can accept liability for the material accessed, or any consequences resulting from Internet use.

The school will audit ICT use to establish if the filtering procedures are adequate
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Cumbria Police.

7.3 Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and users, as defined below, should not engage in these activities in school or outside

school when using school equipment or systems. The school Policy and procedures 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					✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	Pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
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					✓	
Online gaming (educational)			✓			
Online gaming (non-educational)					✓	
Online gambling					✓	
Online shopping/commerce			✓			

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
File sharing	✓				
Use of social networking sites		✓	✓		
Use of video broadcasting e.g. Youtube	✓				

7.4 Handling E–Safety Complaints

- Complaints about Internet misuse are dealt with under the School's complaints procedure and behaviour policies.
- Any complaint about staff misuse is referred to the Headteacher.
- All e–safety complaints and incidents are recorded by the school, including any actions taken.

7.5 Managing Cyber-bullying

- Cyber-bullying (along with all other forms of bullying/peer on peer abuse) of any member of the school community is not tolerated. Full details of our stance on and response to cyber-bullying are included in the school Anti-Bullying (Peer on Peer abuse) Policy.
- There are clear procedures in place to support anyone in the school community affected by cyber-bullying.
- All incidents of cyber-bullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of Cyber-bullying.
- The Police will be contacted if a criminal offence is suspected.

7.5.1 Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in 'Keeping Children Safe in Education' and separate guidance exists on this issue 'Sexual violence and sexual harassment between children in schools and colleges'. All staff are aware of this guidance.

We take all forms of sexual violence and harassment seriously and will act appropriately on information which suggests inappropriate behaviour regardless of the considered seriousness. Any incident of sexual harassment or violence (online or offline) must be reported to the DSL at the earliest opportunity. The DSL will follow the guidance as outlined in the Child Protection Policy and procedures.

7.5.2 Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern student and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These rules are defined in the relevant Acceptable Use Agreements as provided to students, staff and Governors.

Where students contravene these rules, the Whole School Behaviour Policy and procedures will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct and, where necessary, the school disciplinary procedures.

The school reserves the right to withdraw, temporarily or permanently, any or all access to such technology or the right to bring mobile technology devices onto school property.

7.6 Managing Learning Environment/Platforms

We are committed to the use of VLE's as an embedded aspect of the school's teaching and learning practice and we ensure appropriate safeguards are in place surrounding their usage:

- Only members of the current student, parent and staff community will have access to the VLE.
- All users will be mindful of copyright issues and will only upload appropriate content onto the VLE.
- When staff, students etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

Any concerns about content on the VLE may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the VLE for the user may be suspended.
- The user will need to discuss the issues with a member of SLT before reinstatement.
- A student's parent may be informed.
- A visitor may be invited onto the VLE by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

7.7 Managing Mobile Phones and Personal Devices

We recognise the widespread use of personal devices makes it essential that schools take steps to ensure mobile phones and devices, including wearable or "smart" technologies like health or fitness trackers, are used responsibly at school and it is essential that student use of their devices does not impede teaching, learning and good order in classrooms. Staff will be given clear boundaries on professional use.

Students are not allowed networked file access via personal devices. However, 6th Form are permitted to access the school wireless internet network for school-related internet use/limited personal use within the framework of the Acceptable Use Agreement. All such use is monitored.

Student Use

- The use of mobile phones and other personal devices by students and staff in school is covered in the Trinity Handbook, available via the website.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- Students may not use such devices in school to take photographs or to record voice or video unless specific permission has been given by a member of school staff.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or bullying policy.
- The phone or device might be searched by the Senior Leadership Team.
- Suspected abuse may be reported to the Police.
- Electronic devices of all kinds that are brought into school are the responsibility of the user and School accepts no responsibility for loss, theft or damage nor for any adverse health effects caused by such devices, these potential or actual.

Staff Use

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

- Where members of staff are required to use a mobile phone for school duties, a school mobile phone will be provided and used.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

7.8 Discussing the Policy with Staff

- The E–Safety Policy is available to all members of staff.
- To protect all staff and students, the school implements Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user and that discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, is provided for all members of staff**.**

7.9 Discussing the policy with students

All students are made fully aware of the School's E-Safety Policy. Where appropriate they can also be guided to useful published resources that offer valuable information about safe and responsible online behaviour:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk

7.10 Enlisting Parents' Support

- Parents/carers attention is drawn to the school e–safety Policy in newsletters, information packs, the school prospectus and on the school website.

Appendices

Appendix 1 Staff Acceptable Use Policy

INFORMATION AND COMMUNICATION TECHNOLOGY:
POLICY FOR ACCEPTABLE USAGE BY STAFF

Aim
The aim of this policy is to ensure that all staff employed to work at Trinity School understand what is acceptable and what is not when it comes to using the ICT network of the school.

Given that this is an increasingly important feature of the working life of most staff in a school, we need to make sure that everyone can use the system and its wider links safely and effectively, in ways that support individual work and sit within the values and procedures of the school.

Trinity School is committed to protecting the rights and privacy of individuals – students, staff, and others, in accordance with the Data Protection Act. This policy on Acceptable Usage should be read alongside the Data Protection Policy.

Purposes
For each area of likely use of ICT by staff of the school, this policy will aim to explain what acceptable use is, and what is not acceptable, and where any exceptions may lie.

These areas are:

- Passwords
- Uses of E-mail
- Uses of the Internet
- Use of telephone services, including landlines and all mobile devices
- Uses of all computers of the school, including desktops and laptops, and servers

The policy will also cover in brief the legal framework in which ICT usage operates, and it will seek to explain the monitoring of use of our ICT system by the school.

Compliance
This policy applies to all staff and students of Trinity School. Any breach of this policy, or of the Act itself, will be considered an offence and the school's disciplinary procedures could be invoked.

Passwords
The school is responsible for establishing and enforcing a password policy for its use of ICT in order to ensure that matters of privacy and acceptable uses are maintained, and to prevent the unacceptable.

The Headteacher is responsible for establishing and enforcing a password policy on our systems based on the level of security required. This responsibility is delegated in practice to the Deputy Headteacher (Curriculum) and to the manager of our ICT Services.

Passwords are assigned to individual users of ICT systems to maintain security and the data that they contain.

Acceptable uses:
- Using your own personal user account to carry out day to day work.
- Providing your password on request, to the Headteacher or a person nominated by them for, example if access was required should you be absent.
- Compliance with the password policy for our ICT network.
- Taking reasonable precautions to protect the password from disclosure and misuse.

Unacceptable uses:
- Installing or using any other encryption software without the written permission of the Headteacher or a person nominated by her/him.
- Requesting passwords of any other members of staff.

- Using a session via another member of staff's password.
- Sharing passwords with other users.

If a member of staff thinks that their username or password has been used without their permission, they must change the password and inform the Headteacher or ICT Network Manager as soon as practically possible.

The Headteacher will ensure that new members of staff/authorised users are issued with usernames and passwords.

When a member of staff/authorised user leaves their job, whether leaving the school or not, the Headteacher will ensure that all usernames and passwords for that employee are suspended or removed as necessary, through the IT Services Manager.

Uses of Email

Acceptable uses:
- Communication via e-mail in connection with your day to day work.
- Occasional personal use during breaks, lunch hours, before or after the working day in your own time.
- Management access to a member of staff's/authorised user's mail boxes, records etc., where there is a legitimate need authorised by the Headteacher.
- Receipt of unsolicited e-mails (spam) to a member of staff's/authorised users account, so long as they inform their line manager/Headteacher on receipt of such material.

It is vital that all communications with students should be via the systems approved by the school (Office 365 and School Comms etc.).

Unacceptable uses:
- Using e-mail for personal non-work-related communication during the working day, outside of break times.
- Forwarding chain e-mails.
- Subscribing to non-work-related mailing lists.
- Sending files with non-work-related attachments (e.g. video streams, audio streams or graphics).
- Sending e-mails or files which contain discriminatory, abusive, pornographic, obscene, illegal, offensive, potentially libelous or defamatory content.
- Sending any sensitive or confidential e-mails or files to unauthorised internal or external recipients.
- Sending e-mails from another user's account.
- Sharing personal e-mail addresses with students, or communicating with them to their private, non-school addresses, or e.g. Facebook accounts.
- Participation in forwarding or passing on messages or images designed to humiliate others, often known as 'cyber bullying'.

USE OF THE INTERNET

Acceptable uses:
- Accessing work related websites as additional tools to carry out your day to day duties.
- Accessing non-work-related websites for personal use during breaks, lunch hours, before or after the working day in your own time, with the exception of websites containing pornographic, offensive or obscene material.

Unacceptable uses:
- Accessing non-work-related websites for personal use during the working day, including accessing social networking sites.
- Making your personal internet access password available to others.
- Downloading copyright material without the owner's permission.
- Making repeated attempts to access websites which have been automatically blocked by the school.
- Downloading images, video or audio streams for non-work-related purposes.
- Downloading or deliberately accessing sites displaying pornographic offensive or obscene material.
- Accessing live internet feeds and leaving them open for example to collect news or sports results.

- Accessing the internet via another user's password.
- Revealing or publicising confidential information.
- Representing personal opinions as those of the school.
- Soliciting for personal gain or profit.
- Online gambling.
- Participation in forwarding or passing on messages or images designed to humiliate others, often known as 'cyber bullying'.
- Adding students as 'friends' on social networking sites.
- Attempting to bypass security systems.

Outside of the workplace:
The Internet provides members of staff/authorised users with access to worldwide information services, bringing new opportunities for communication. With the increasing popularity of social networking sites thought should be given when publishing information about yourself. Members of staff/authorised users should ask themselves if they would feel comfortable about an employer, colleague, student or parent viewing their content on a social networking site. Profiles should be made private and consideration given as to who is added as 'friends'. Consideration should also be given as to making 'tweets' available for public viewing and how employees would feel about an employer, colleague, student or parent viewing comments made on Twitter.

USE OF TELEPHONES (INCLUDING LANDLINE & MOBILE & DEVICES)

Acceptable uses:
- Personal calls, with the approval of a line manager/the Headteacher.
- Use of the telephone for work-related business.

Unacceptable uses:
- Allowing use of the telephone by unauthorised users.
- Personal calls made without the approval of a line manager/Headteacher.
- Personal use of mobile phones and Portable Electronic Devices during lesson times.
- Use of telephones that could bring the school into disrepute.
- Use of telephones to promote external private business.
- Use of telephones to premium rate numbers.
- Use of a hand-held telephone whilst driving.
- Participation in forwarding or passing on messages or images designed to humiliate others, often known as 'cyber bullying'.

USE OF ICT EQUIPMENT

Acceptable uses:
- Storing school data.
- Loading text, images, video or audio streams in connection with day to day work activities.
- Storing limited amounts of personal data (where agreed by the Headteacher).

Unacceptable uses:
- Loading unauthorised or untested software.
- Allowing unauthorised users to access laptops used away from school.
- Failure to keep laptops secure when used away from school.
- Storing confidential or personal data or information on removable media without adequate protection or encryption.
- Deliberate, reckless or negligent introduction of viruses.
- Storing personal material protected by copyright which has not been purchased.
- Loading files containing pornographic offensive or obscene material.
- Unauthorised use of Spyware.

THE LEGAL FRAMEWORK

Computer use in school is legally regulated. This includes the content of e-mail, or sites downloaded from the Internet. privacy issues, monitoring of communications and surveillance at work; and employment relations. The school may seek further legal advice, if appropriate.

The school does monitor emails and other Internet uses for profanity/inappropriate content. Members of staff are hereby advised of this monitoring.

Appendix 2 – Guidelines for Parents and carers

POLICY ON PARENTAL USE OF SOCIAL NETWORKING AND INTERNET SITES

Overview

Social networking sites such as Facebook and Twitter are now widely used and these types of media allow people to communicate in ways that were not previously possible. Unfortunately, such sites can be used inappropriately by some as a means of expressing negative or offensive views about schools and their staff. This document sets out this school's approach to parental use of such sites and sets out the procedures that will be followed and action that may be taken when it is considered that parents have used such facilities inappropriately. Where there is reference to "parent" in this document this also include carers, relatives or anyone associated with the school.

Objectives

The purpose of this policy is to:

- Encourage social networking sites to be used in a beneficial and positive way by parents
- Safeguard students, staff and anyone associated with the school from the negative effects of social networking site
- Safeguard the reputation of the school from unwarranted abuse on social networking sites
- Clarify what the school considers to be appropriate and inappropriate use of social networking sites by parents
- Set out the procedures the school will follow where it is considered that parents have inappropriately or unlawfully used social networking sites to the detriment of the school, staff, students or anyone else associated with the school
- Set out the action the school will consider taking if parents make inappropriate use of social networking sites

Appropriate use of social networking sites by parents

Social networking sites have potential to enhance the learning and achievement of students and enable parents to access information about the school and provide feedback efficiently and easily. In addition, the school recognises that many parents and other family members will have personal social networking accounts which they might use to discuss/share views about school issues with friends and acquaintances. As a guide, individuals should consider the following prior to posting any information on social networking sites about the school, staff, students or anyone else associated with the school:

- Is the social networking site the appropriate channel to raise concerns, give this feedback or express these views?
- Would a private and confidential discussion with someone in the school be more appropriate? If there are serious allegations being made/concerns being raised, social media or internet sites should not be used to name individuals and make abusive comments. Please contact the school to discuss any concerns you may have
- Are such comments likely to cause emotional or reputational harm which would not be justified, particularly if the school has not yet had a chance to investigate a complaint?
- The reputational impact that the posting of such material may have to the school, any detrimental harm that the school may suffer as a result of the posting and the impact that such a posting may have on students' learning.
- Trinity School will always work with parents to attempt to resolve issues. If parents are dissatisfied with our first response at any time the Complaints Policy is available on the website as are contact details for the Headteacher and the Chair of Governors.

Inappropriate use of social networking sites by parents

Although social networking sites may appear to be the quickest and easiest way to express frustrations or concerns about the school and those associated with it, it is rarely appropriate to do so. Other channels such as a private and confidential discussion with the Headteacher or member of the Governing Body, or using the school's formal complaints process are much better suited to this. The School considers the following examples to be inappropriate uses of social networking sites. (This list is non-exhaustive and intended to provide examples only):

- Naming children or posting any comments about children who attend Trinity School

- Making allegations about staff or anyone else connected with the school
- Making any posts that could be deemed to be cyber-bullying
- Making complaints about the school or staff at the school
- Making defamatory statements about the school or staff at the school
- Posting negative or offensive comments about staff or any other individual connected to the school
- Posting racist comments
- Posting comments which threaten violence

Parents should also ensure that their children are not using social networking and other internet sites in an inappropriate manner. It is expected that parents/carers explain to their children what is acceptable to post online. Parents/carers are also expected to monitor their children's online activity, including in relation to their use of social media. Please note that most social networking sites require the user to be at least 13 years old but some only allow access to those aged 13-18 with parental consent.

Procedure the school will follow if inappropriate use continues

The School will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step the school will usually discuss the matter with the parent to try and resolve it and to ask that the relevant information be removed from the social networking site in question. If the parent refuses to do this and continues to use social networking sites in a manner the school considers inappropriate, the school will consider taking the following action:

- Take legal advice and/or legal action where the information posted is defamatory in any way or if the circumstances warrant this
- Set out the school's concerns to you in writing, giving you a warning and requesting that the material in question is removed
- Contact the police where the school feels it appropriate – for example, if it considers a crime (such as harassment) has been committed or in cases where the posting has a racial element, is considered to be grossly obscene, grossly offensive or is threatening violence
- If the inappropriate comments have been made on a school website or online forum, the school may take action to block or restrict that individual's access to that website or forum
- Contact the host/provider of the social networking site to complain about the content of the site and ask for removal of the information
- Take other legal action against the individual

Appendix 3 Student Acceptable Use Agreement Form

The computer system is owned by the school. This Responsible Use policy helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not. This is a summary of the full school Acceptable Use policy.

- Irresponsible use will result in the loss of computer access to all school ICT resources.
- Network access must be made via the user's authorised account and password, which must not be given to another person. You will be responsible for any computer activity done on your password.
- School computer and internet use must be appropriate to your education.
- Copyright and intellectual property rights must be respected.
- E mail should be written carefully and politely, particularly as messages may be forwarded or printed to be seen by unexpected readers.
- Users are fully responsible for e mail they send and for contacts made.
- Personal contact information (e.g. phone numbers and addresses) must not be typed into web pages or e mail.
- Anonymous messages and chain letters are not permitted.
- The use of chat rooms and messaging services is not allowed.
- You are not allowed to download any programs or games from the internet. If in doubt you should check with the ICT Services Manager in Creighton building.
- The use of proxy sites is expressly forbidden.
- The school ICT systems including printers may not be used for personal purposes.
- The ICT system and system security must be respected
- No food or drink should be brought near any of the ICT resources

The school will exercise its right to monitor the use of the school computer systems, including access to web sites, the interception of e mail, and the deletion of inappropriate materials where it believes unauthorised use of the school system is or may be taking place.

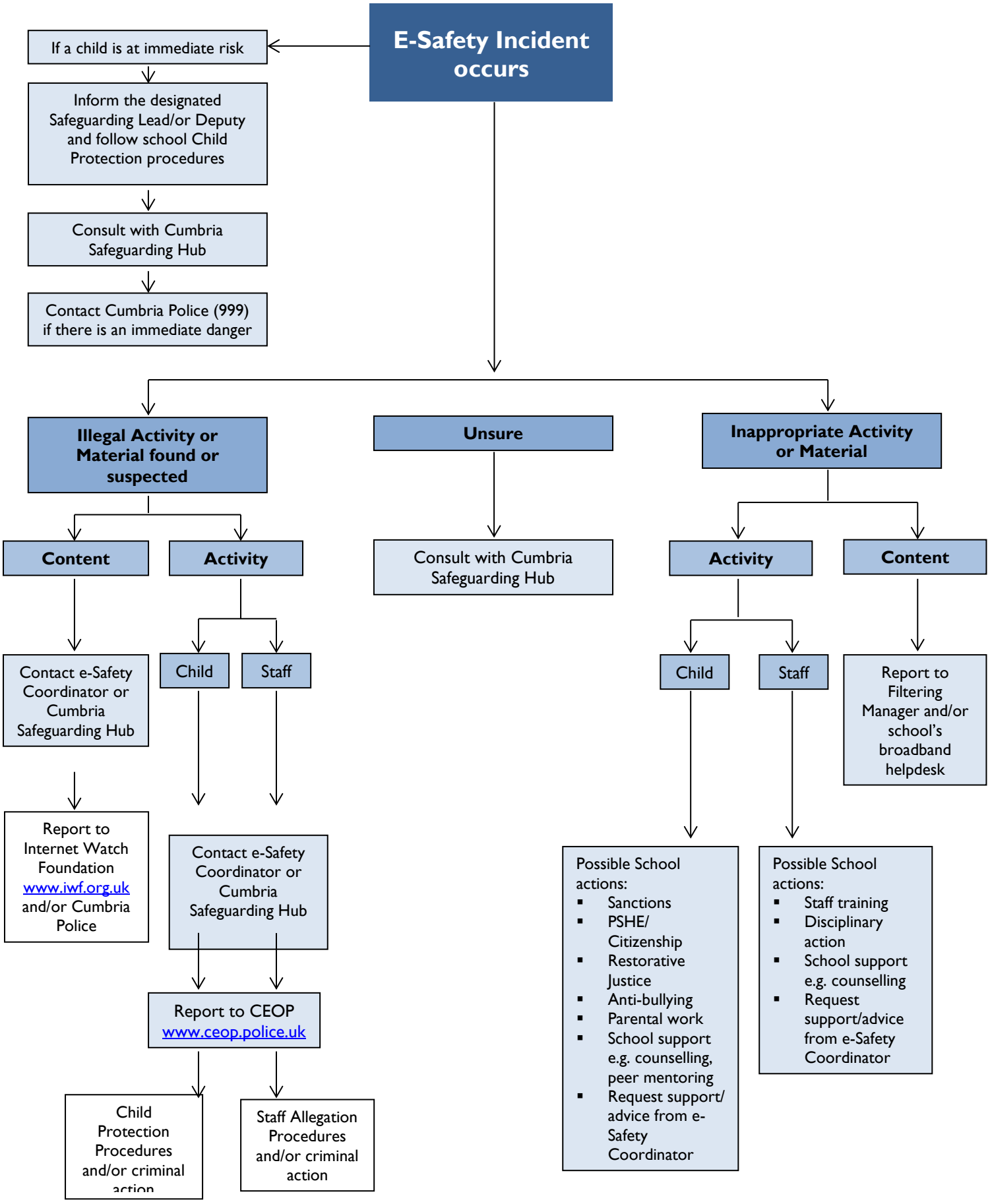
I agree to abide by the conditions of the ICT Responsible Use Policy and understand the implications if I do not.

Signed _____ Date _____

Print Name _____ Form _____

Appendix 4 Incident escalation flowchart

RESPONSE TO AN INCIDENT OF CONCERN



Review school e-Safety Policies and procedures; record actions in e-Safety incident log and implement any changes in the future.

Appendix 5 E-SAFETY INCIDENT LOG

Details of E-Safety incidents to be recorded by the E-Safety Coordinator. This incident log will be monitored termly by the Head teacher, member of SLT or Chair of Governors.

Date	Time	Name of Student or Staff Member	Male or Female	Room and Computer/ Device No.	Details of Incident (including Evidence)	Actions and Reasons