TRINITY SCHOOL
CARLISLE

A CHURCH OF ENGLAND ACADEMY

E-SAFETY POLICY

Pastoral Committee
Reviewed: October 2021
Approved by the Pastoral Committee: November 2021
Ratified by the Full Governing Body: December 2021
Next review: October 2022

Review Sheet

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
Updated in light of statutory DfE guidance 'Keeping Children Safe in Education' Sept 2021 which newly references schools having an online safety policy and what it should contain, the 4Cs, and the continuing DfE expectation that all schools responsible for the provision of compulsory schooling (including independent schools with students funded by the taxpayer i.e., children looked after or children from military families attending boarding schools) will provide remote education and do it safely. Minor updates to appendices to reflect language/KCSiE updates.	September 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:

This Policy and procedures will be communicated to staff, students, and the wider community by:

- Posting it on the school website and shared staff drive
- Making a paper copy available on request from the school office and for staff in the main staff room
- Discussing school policy and procedures during induction with new staff and other relevant adults including (where relevant) the staff Acceptable Use Agreement
- Discussing Acceptable Use Agreements with students at the start of each year
- Issuing Acceptable Use Agreements to external users of school systems (e.g., Governors) usually on entry to the school
- Holding Acceptable Use Agreements in pupil and personnel files
- We share information with students and parents/carers that provide information on acceptable and safe on-line behaviour including personal safety and on-line bullying.
- We have a clear policy on the use of mobile devices in school
- Regular assemblies and "Freeze Sessions" for all year groups are used to reinforce what constitutes safe and acceptable online behaviour.

The Online Safety Policy is also referenced in other school Policies and procedures as outlined above.

The review period for this Policy and procedures is determined by the Governing Body/Proprietors and indicated on the front cover.

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. Governors will also;

- ensure a member of the Governing Body is elected to the role of Online Safety Governor who should then lead on relevant governance requirements below;
- ensure an appropriate senior member of staff from the school leadership team is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety with the appropriate status, authority, time, funding, training, resources, and support;
- ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures and to approve the Online Safety Policy and procedures, reviewing its effectiveness e.g., through Governors or a Governor Sub-committee receiving regular information about online safety incidents and monitoring reports and making use of the UK Council for Internet Safety (UKCIS) guide Online safety in schools and colleges: Questions from the Governing Board;
- ensure that the school follows all current online safety advice to keep both students and staff safe;
- support the school in encouraging parents and the wider community to become engaged in online safety activities;
- have regular reviews with the Online Safety Coordinator/Designated Safeguarding Lead (DSL) and incorporate online safety into standing discussions of safeguarding at Governors meetings (including incident logs, filtering/change control logs etc.)
- ensure that where the online safety coordinator is not the named DSL or deputy DSL, there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised;
- work with the Data Protection Officer (DPO), DSL and Head teacher to ensure a UK GDPR compliant framework for storing data, helping to ensure that child protection is always at the forefront and data protection processes support careful and legal sharing of information;
- check that school is making good use of information and support (Annex D - Online Safety which forms part of 'Keeping Children Safe in Education');
- ensure that all staff undertake regular updated safeguarding training, including online safety training in line with advice from the Local Safeguarding Children's Partnerships (LSCP), and that it is integrated, aligned, and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning;
- ensure that appropriate filters and appropriate monitoring systems are in place, but also consider how 'over-blocking' may lead to unreasonable restrictions on what students can be taught in relation to online teaching and safeguarding;
- recognise that a one size fits all educational approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed
- ensure students are taught how to keep themselves safe, including online as part of providing a broad and balanced curriculum with clear procedures on the use of mobile technology.

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);
- be the first point of contact for any concerns the wider staff and other adults working in the school may have in relation to child protection and online safety harmful behaviour e.g., sharing nude or semi-nude images/online challenges or hoaxes and refer to the UKCIS and DfE guidance on these subjects;
- 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 read and understand KCSiE Annex A unless they work in the SLT or directly with children when they must read and understand KCSiE Part one *and* Annex B;
  - all staff are aware of information relevant to their role in keeping children safe online signposted in KCSiE Annex D

- 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 Annex A of 'Keeping Children Safe in Education' unless they work in the SLT or directly with children when they must read and understand Part 1 *and* Annex B instead;

- 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 and understand the importance of reporting abuse, misuse or access to inappropriate materials including those involving hoaxes and on-line challenges 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/ know and understand school procedures on the taking/use of images and on cyberbullying/sharing nude and semi-nude images.
- 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. Teaching and Learning

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk known as the 4Cs:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial, or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Strong links between teaching online safety and the curriculum (see also Roles above) are the clearest in:

- Personal, Social and Health Education (PSHE)
- Relationships education, relationships, and sex education (RSE) and health
- Computing

It is, however, the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting subject lead staff 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, all staff will encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide students when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g., fake news), age-appropriate materials and signposting, and legal issues such as copyright, plagiarism, and data law.

We recognise that online safety and broader digital resilience must be included throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND students) are used as an opportunity to assess the key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

6.1 How internet use enhances learning

This school:

- has a clear, progressive online safety education programme as part of the ICT/PSH(RS)E curriculum. This covers the teaching of a range of skills and behaviours which are appropriate to the age and experience of the students concerned and include those to:

  - STOP and THINK before they CLICK;
  - develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - know how to narrow down or refine a search;
  - [for older students] understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - understand acceptable behaviour when using an online environment/email, i.e., be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - understand how photographs can be manipulated and how web content can attract unwanted or inappropriate attention;
  - understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs, and videos and to know how to ensure they have turned-on privacy settings;
  - understand why they must not post pictures or videos of others without their permission;
  - know not to download any files – such as music files – without permission;
  - have strategies for dealing with receipt of inappropriate materials;
  - [for older students] understand why and how some people will 'groom' young people for sexual or extremist ideology reasons;
  - understand the impact of cyberbullying, sharing inappropriate images and trolling and know how to seek help if they are affected by any form of online bullying;
  - know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e., parent, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through an end-user Acceptable Use Agreement which will be displayed throughout the school or when they log on to the school's network;
- ensures staff model safe and responsible behaviour in their own use of technology during lessons;
- ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright/intellectual property rights;
- ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying online; online gaming/gambling etc.

6.2 Students with additional needs

We use a wide range of strategies to support children with additional needs who might need extra support to keep themselves safe, especially online.

- Sensitively check pupil's understanding and knowledge of general personal safety issues using reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.
- Apply rules consistently to embed understanding.
- Communicate rules clearly to parents and seek their support in implementing school rules at home. Working with parents and sharing information with them is relevant to all children, but this group especially.
- Careful explanations about why rules might change in different situations i.e., why it is ok to give your name and address to an adult if you are lost in town, but not when using the Internet.
- Consistent use of cause and effect linking the rules to consequences teaching realistic and practical examples of what might happen if… without frightening students.

6.3 Remote Education

While the remote education temporary continuity direction which required schools to provide remote education to students where their attendance would be contrary to government guidance or legislation in force at the time has ended, the DfE expects schools to continue to maintain their capabilities to deliver high quality remote education for the next academic year.

This is because government public health advice locally or nationally may require a class, group, or a small number of students to self-isolate, and all such students not physically unwell should have access to remote education as soon as reasonably practicable, which may be the next school day.

When this school is required to provide it, remote education should be equivalent in length to the core teaching students would receive in school and should include recorded or live direct teaching time, as well as time for students to complete tasks and assignments independently. As a minimum we will provide 5 hours/day on average across the cohort for Key Stages 3 and 4.

To ensure business continuity, thorough emergency preparedness, continuity of education and safeguarding arrangements, and to prevent harms, Governors may decide to implement remote learning provision in any kind of local or national emergency situation that prevents students or staff attending to statutory schooling.

In developing our remote education provision, we have:

- Selected the 'Classcharts' and Microsoft Teams digital platform(s) to use consistently across the school to allow interaction, assessment, and feedback with procedures in place to ensure staff are trained and confident in its use. This enables us to provide online video lessons recorded by teaching staff and high-quality lessons developed by external providers as well as monitored methods of communication.
- Identified ways to discover and overcome barriers to digital access for students e.g., forms or other survey methods, distributing school-owned laptops, securing appropriate internet connectivity solutions, providing printed resources, such as textbooks and workbooks, to structure learning, supplemented with other forms of communication to keep students on track or answer questions about work.
- Ensured that school-owned devices distributed for the purpose of access to remote education will always include appropriate safeguarding controls and support to help children and families, and staff use them safely, including information about physically healthy computing e.g., posture, the teaching and learning environment, sleep.
- Ensured we can teach a planned and well-sequenced curriculum so that knowledge and skills are built incrementally.
- Published on the school website up-to-date information about what is intended to be taught and practised in each subject so that students can progress through the curriculum.
- Put systems in place for checking, daily, whether students are engaging with their work, so we can work with families to rapidly identify effective solutions where engagement is a concern.
- Identified a named senior leader Mr Hopkins with overarching responsibility for the oversight of the quality, delivery, and safety of remote education.
- Considered issues that specific individuals or groups of students may have engaging with remote education due to their age, stage of development, special educational needs, or disability e.g., where this would place significant demands on parents' help or support, ensuring that the teachers best placed to know how the pupil's needs can be most effectively met to ensure they continue to make progress, work with families to deliver an ambitious and appropriate curriculum
- Sought to demonstrate that we understand the requirement for schools under the 2014 Children and Families Act to use our best endeavours to secure the special educational provision called for by the students' special educational needs remains in place.
- Identified potential personal, professional, and children's safeguarding issues associated with the provision of remote education; put in place hardware, software, procedures, and training to reduce the risk of harm to the adults, children, and young people exposed to it; and ensured the risks are being addressed in a consistent and ongoing way through the curriculum (see below).
- Reviewed and updated as necessary relevant Policies, procedures, and supporting documents like our Acceptable Use Agreements in light of remote education provision to ensure that they remain appropriate and useful for keeping the adults, children, and young people exposed to it safe online.

In the provision of remote education this school undertakes to:

- Set meaningful and ambitious work each day in an appropriate range of subjects

- Transfer into remote education what we already know about effective teaching in live classrooms by:
  - providing frequent, clear explanations of new content, delivered by a teacher or through high-quality curriculum resources
  - providing opportunities for interactivity, including questioning, eliciting and reflective discussion
  - providing scaffolded practice and opportunities to apply new knowledge
  - enabling students to receive timely and frequent feedback on how to progress, using digitally facilitated or whole-class feedback where appropriate
  - using assessment to ensure teaching is responsive to students' needs and addresses any critical gaps in students' knowledge
  - avoiding an over-reliance on long-term projects or internet research activities
- Ensure leaders and teachers are appropriately signposted to the Get help with remote education support package, relevant peer-to-peer advice and training available through the EdTech Demonstrator programme , and guidance on supporting students and students with SEND to access remote education.
- Notify their social worker (if they have one) when a vulnerable pupil is asked to self-isolate and agree with the social worker the best way to maintain contact and offer support.
- Review and self-assess the our remote education offer regularly using the DfE review your remote education provision tool or similar.
- Continue to record attendance accurately in the register for students who are receiving remote education in line with any current government guidance on it.
- Carry out an annual review of the school's approach to online safety, supported by an annual risk assessment that considers and reflects the risks the students that attend this school face using a tool like the 360 safe website.

We recognise that there are additional safeguarding risks to students associated with them spending more time online than before the global pandemic, both in their leisure time and to be able to access remote education. There may also be risks from or to the people they live with during live video link work and staff are expected to plan accordingly and seek advice from the OSL/DSL as necessary. The pupil Acceptable Use Agreement includes expected conduct during remote education activities.

We recognise that there are additional safeguarding risks to staff as well, especially those facilitating remote learning via live video links that may also impact other people in their household or community. The Staff Code of Conduct sets out expected good remote education practice.

We will follow relevant government online safeguarding guidelines and make use of recommended technical tools and guides signposted there to help us deliver remote education safely.

In addition to the updated codes of conduct, staff, students (or due to their age and ability, the adults supporting them), parents, carers, and to some degree, virtual or in-person visitors using online technology for education purposes or school business are expected to:

Check security and privacy settings e.g.:

- Adjust privacy and safety settings on all devices, in apps and other online places to control what personal data is shared.
- Review the security settings on 'smart' devices and change any default, weak or guessable passwords.
- Set up two-factor authentication if devices are capable or available.
- Regularly update devices or apps used for school or work to improve security.
- Think about physical privacy when appearing live online e.g., adult supervision of children at home, appropriate clothing, distractions like noise and interruptions, what other people nearby can hear.

Act regarding unsuitable content e.g.:

- Prevent unwanted content from appearing i.e. set filters and parental controls on home broadband and mobile networks and not disable or bypass them (the UK Safer Internet Centre has advice on how).
- Block unsuitable contact (with support as necessary)

- Report harmful activity, to the website, platform or app, a trusted adult, and the DSL. Report Harmful Content to Safer Internet UK if not satisfied with the result of a report to a service provider.

Protect against fraud e.g.:

- Beware of fraud and scams online including phishing emails and text messages and use appropriate cyber security and "stop, challenge, protect" information to avoid becoming a victim.
- Forward suspicious emails to reportphishing@apwg.org, using the "Forward as attachment" option if possible to enhance tracking to the Anti-Phishing Working Group for analysis.
- Never give out personal information to websites or in response to emails/text messages not recognised or trusted
- Report being scammed, defrauded, or experiencing cyber-crime to Action Fraud, the UK's national reporting centre.

Check the Facts e.g.: use the SHARE checklist to make sure they are not contributing to the spread of harmful content e.g.

Stay physically and mentally healthy online e.g.:

- Take regular breaks from online activities and use tools like Apple's Screen Time, Google's Family link, Xbox One, PlayStation 4, Nintendo Switch if necessary to manage screen time, especially if feeling overwhelmed, or in physical discomfort.
- Take notice of any guidance school provides on supporting children's mental health and wellbeing or that of staff as well as practical guidance on making the home environment a good and safe one to learn in with school adopting a sensitive appreciation for people's different home circumstances and what is reasonable.

Staff are also expected to:

- Provide information about their temporary home working environment insofar as it might impact on their physical health, or the safeguarding of learners or their own household.
- Act appropriately on feedback and use any necessary online or cyber tools provided.
- Provide information about the technology they use at home to get online i.e., to ensure compatibility with school systems, especially cyber security measures involved in accessing sensitive data like medical, behaviour or performance information on school servers remotely.
- Implement relevant guidance on safe teaching and pastoral care from their home e.g., what is in the background of recorded or live streams, what is visible on shared screens, what can be heard by others in a household etc.
- Pay special attention to how they protect personal data at home.
- Report to their line manager any issues or concerns they may have either about their personal safety or that of a pupil.
- Keep talking about staying safe online, which we can do by:
  - Ensuring staff have the tools to promote a healthy balance between the positive and negative aspects of life online.
  - Signposting parents and carers to tools to explain and reduce risks and help them talk to their child.
  - Reiterating behaviour expectations and ways to handle and report problems, especially encouraging children to speak to a trusted adult if they come across content online that makes them uncomfortable.
  - Supporting critical thinking and promoting resources like Parent Zone's guide and Childnet's advice and top tips which provide ways parents and carers can help their child develop these skills.

7. Managing Information Systems

7.I 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

7.2 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.

7.3 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.

7.4 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

7.5 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;

7.6 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.

7.7 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.

7.8 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

7.9 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.

7.10 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.

7.11 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.*

7.12 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.

8. Policy Decisions

8.1 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.

8.2 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.

8.3 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			✓			
File sharing		✓				
Use of social networking sites			✓	✓		
Use of video broadcasting e.g. Youtube		✓				

8.4 Handling E–Safety Complaints

Our staff recognise that online safety is only one element of the wider safeguarding agenda as well as being a curriculum strand of ICT, PSHE/RSE.

General concerns will be handled in the same way as any other child protection concern. Early reporting to the DSL/OSL is vital to ensure that the information contributes to the overall picture or highlights what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets, and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

Procedures for dealing with online safety, concerns and incidents are detailed in the following Policies:

- Child Protection Policy and procedures
- Anti-Bullying (Peer on peer abuse) Policy
- Expectations for Learning; Behaviour Policy (includes anti-bullying procedures)
- Acceptable Use Agreements
- Prevent Risk Assessment
- Data Protection Policy, agreements, and other documentation (e.g., privacy statement, consent forms for data sharing image use etc.)

We are committed to taking all reasonable precautions to ensure online safety but recognise that incidents will occur both inside and outside school. All members of the school community are encouraged to report issues swiftly to school staff so that they can be dealt with quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the DSL/OSL on the same day wherever possible or, if out of school, the following school day.

Any concern/allegation about misuse by staff or other adult in school will always be referred directly to the Head teacher unless the concern is about the Head teacher, in which case, the complaint will be directed to the Chair of Governors. Staff may also use the NSPCC Whistleblowing Helpline. Call 0800 028 0285 or email: help@nspcc.org.uk.

The school will actively seek support from other agencies as needed (i.e., Local Authority Safeguarding Hub, UK Safer Internet Centre's Professionals' Online Safety Helpline (03443814772), NCA CEOP, Cumbria Police Prevent Officer, Cumbria Police, Internet Watch Foundation (IWF)). We will inform parents of online safety incidents involving their child and the Police where staff or students engage in or are subject to behaviour which we consider is particularly disturbing or is considered illegal. See Sections below for procedures for dealing with sharing nude and semi-nude images, upskirting and online bullying.

- In this school there is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions.
- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The Online Safety Coordinator will record all reported incidents and actions taken in the School Online Safety incident log and other in any relevant areas e.g., Bullying or Child protection log.
- The Designated Safeguarding Lead will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Child Protection Policy and procedures for dealing with concerns.
- The school will manage Online Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents of any incidents or concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Safeguarding Hub **and** escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding Hub – see Child Protection Policy and procedures.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence, and protect those carrying out the investigation. More than one member of staff should be involved in the investigation which should be carried out on a "clean" designated computer.

Incidents will be dealt with as soon as possible in a proportionate manner through normal behaviour/disciplinary procedures. It is important that, where necessary, members of the school community are made aware that incidents have been dealt with.

8.5 Sharing nude and semi-nude images

Where incidents of the sharing of nude and semi-nude images via the internet or mobile phone by those under the age of 18 are discovered , we will refer to the UK Council for (UKCIS) guidance 'Sharing nude and semi-nude images'. A copy of this document is available from the school office. Where one of the parties is over the age of 18, we will refer to it as child sexual abuse.

All staff and other relevant adults have been issued with a copy of the UKCIS overview document (Sharing nudes and semi-nudes: how to respond to an incident) in recognition of the fact that it is generally someone other than the DSL or OSL who will first become aware of an incident. Staff, other than the DSL, must not attempt to view, share, or delete the image or ask anyone else to do so but must report the incident to the DSL as soon as possible.

It is the responsibility of the DSL to follow the guidance issued by UKCIS, decide on the next steps and whether to involve other agencies as appropriate.

It is important to understand that whilst the sharing of nude and semi-nude images illegal, students should be encouraged to discuss with staff situations if they have made a mistake or had a problem with this issue.

The UKCIS advice outlines how to respond to an incident of nudes and semi-nudes being shared including:

- risk assessing situations;
- safeguarding and supporting children and young people;
- handling devices and images;
- recording incidents, including the role of other agencies.
- informing parents and carers

The types of incidents which this advice covers are:

- a person under the age of 18 creates and shares nudes and semi-nudes of themselves with a peer under the age of 18;
- a person under the age of 18 shares nudes and semi-nudes created by another person under the age of 18 with a peer under the age of 18;
- a person under the age of 18 is in possession of nudes and semi-nudes created by another person under the age of 18.

8.6 Upskirting

All staff are aware that 'upskirting' (taking a photo of someone under their clothing) is now a criminal offence, but that students should be encouraged to discuss with staff situations if they have made a mistake or had a problem with this issue. If staff or other adults become aware of an incident of 'upskirting', the issue must be reported to the DSL as soon as possible.

8.7 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.

8.8 Harmful online challenges or hoaxes

An online challenge will generally involve users recording themselves taking a challenge and then distributing the resulting video through social media sites, often inspiring or daring others to repeat the challenge. Whilst many will be safe and fun, others can be potentially harmful and even life threatening.

If staff are confident children and young people are aware of, and engaged in, a real challenge that may be putting them at risk of harm, then it would be appropriate for this to be directly addressed by either the DSL or a senior leader in school. Careful consideration will be given on how best to do this, and it may be appropriate to offer focussed support to a particular age group or individual children at risk. We will take account of the fact that even with real challenges, many children and young people may not have seen it and may not be aware of it and will carefully weigh up the benefits of institution-wide highlighting of the potential harms related to a challenge against needlessly increasing children and young people's exposure to it.

Where staff become aware of a potentially harmful online hoax or challenge, they will immediately inform the Designated Safeguarding Lead who will take the appropriate action either with the child concerned or with the wider group where the incident involves more than one child.

Where the DSL considers it necessary to directly address an issue, this can be achieved without exposing children and young people to scary or distressing content. In the response, we will consider the following questions:

- is it factual?
- is it proportional to the actual (or perceived) risk?
- is it helpful?
- is it age and stage of development appropriate?
- is it supportive?

A hoax is a deliberate lie designed to seem truthful. The internet and social media provide a perfect platform for hoaxes, especially hoaxes about challenges or trends that are said to be harmful to children and young people to be spread quickly.

We will carefully consider if a challenge or scare story is a hoax. Generally speaking, naming an online hoax, and providing direct warnings is not helpful. Concerns are often fuelled by unhelpful publicity, usually generated on social media, and may not be based on confirmed or factual occurrences or any real risk to children and young people. There have been examples of hoaxes where much of the content was created by those responding to the story being reported, needlessly increasing children and young people's exposure to distressing content.

Evidence from Childline shows that, following viral online hoaxes, children and young people often seek support after witnessing harmful and distressing content that has been highlighted, or directly shown to them (often with the best of intentions), by parents, carers, schools, and other bodies. In this respect, staff will be mindful of the advice provided by the UK Safer Internet Centre which provides guidance on dealing with online hoaxes or challenges.

In any response, reference will be made to the DfE guidance 'Harmful online challenges and online hoaxes'

8.8.1 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.

8.8.2 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.

8.9 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.

8.10 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.

8.11 Discussing the Policy with Staff

It is important that all staff feel confident meeting the demands of using ICT appropriately in teaching, administration, and all other aspects of their school and personal life and the School Online Safety Policy and procedures will only be effective if all staff subscribe to its values and methods.

Staff will be given opportunities to discuss the issues and develop appropriate teaching or other work strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an internet activity without preparation.

Any member of staff who has concerns about any aspect of their own or anyone else's ICT or internet use either on or off site, they should discuss this with their line manager. Where concerns are related to children's safeguarding, they should also be reported to the DSL who should follow the Child Protection Policy and procedure for recording and reporting allegations that meet the harm threshold and recording (and in some case reporting i.e., to a contractor's employer) low level concerns that do not.

Consideration is given when members of staff are provided with devices by the school which may be accessed outside of the school network. Staff are made aware of their responsibility to maintain the security and confidentiality of school information.

All staff have a universal duty to understand harms and protect children from them, including online. ICT use is widespread and all staff including administration, midday supervisors, facilities staff, Governors, and volunteers who use it or work with children who use it are included in awareness raising and training.

Induction of all new staff will include:

- A copy of the Online Safety Policy and procedures and a scheduled opportunity to discuss them.
- That internet traffic can be monitored and traced to the individual user, and the importance of having high professional standards and always following current policies and procedures.
- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally.
- Requirement to read, understand and sign relevant Acceptable Use Agreements.

- For staff who manage filtering systems or monitor ICT use: that they will be supervised by the Senior Leadership Team and what the procedures for reporting issues are.
- How the school will promote online tools which staff should use for work purposes, especially with children, and the procedure staff should go through if there is a new tool they want to use.
- That their online conduct out of school could have an impact on their role and reputation in school. Civil, legal, or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Volunteers will receive an online safety induction based on what staff receive but suitable for the role they have been asked to fulfil.

8.12 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

8.13 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 and Volunteer Acceptable Use Policy (E-signatures secured each September)

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 (E-signatures secured each September)

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 email, 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.

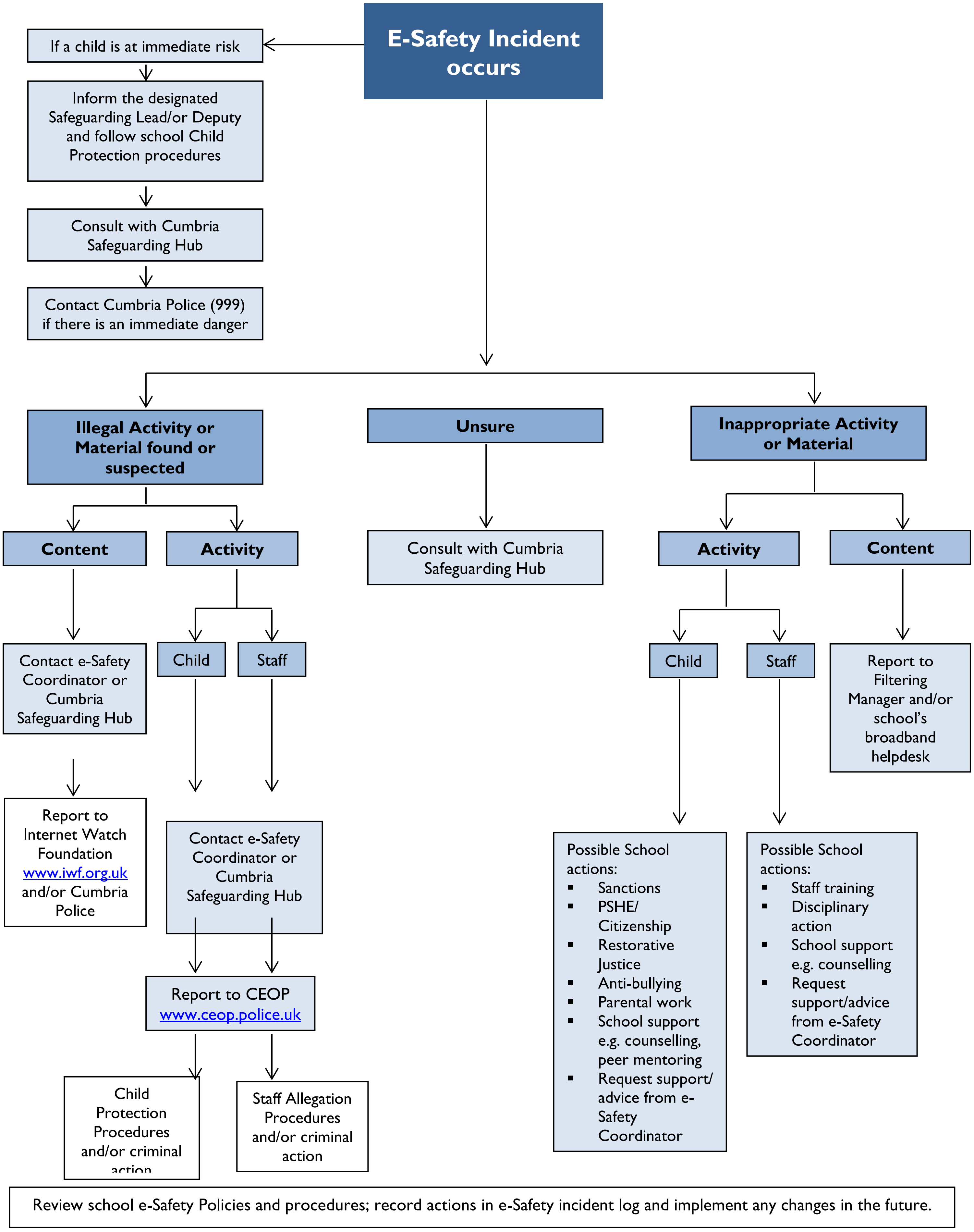
Signed ________________________________ Date ___________________

Print Name ________________________________ Form ___________________

This page is intentionally blank for photocopying purposes

Appendix 4 Incident escalation flowchart

RESPONSE TO AN INCIDENT OF CONCERN



E-Safety Incident occurs

If a child is at immediate risk

Inform the designated Safeguarding Lead/or Deputy and follow school Child Protection procedures

Consult with Cumbria Safeguarding Hub

Contact Cumbria Police (999) if there is an immediate danger

Illegal Activity or Material found or suspected

Content

Contact e-Safety Coordinator or Cumbria Safeguarding Hub

Report to Internet Watch Foundation www.iwf.org.uk and/or Cumbria Police

Activity

Child

Staff

Contact e-Safety Coordinator or Cumbria Safeguarding Hub

Report to CEOP www.ceop.police.uk

Child Protection Procedures and/or criminal action

Staff Allegation Procedures and/or criminal action

Unsure

Consult with Cumbria Safeguarding Hub

Inappropriate Activity or Material

Activity

Child

Possible School actions:

- Sanctions
- PSHE/ Citizenship
- Restorative Justice
- Anti-bullying
- Parental work
- School support e.g. counselling, peer mentoring
- Request support/ advice from e-Safety Coordinator

Staff

Possible School actions:

- Staff training
- Disciplinary action
- School support e.g. counselling
- Request support/advice from e-Safety Coordinator

Content

Report to Filtering Manager and/or school’s broadband helpdesk

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

This page is intentionally blank for photocopying purposes

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

This page is intentionally blank for photocopying purposes

Appendix 6

TRINITY SCHOOL ONLINE SAFETY AUDIT

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for Online Safety (OS). Staff that could contribute to the audit include the Designated Safeguarding Lead, Online Safety Lead, SENCO, Online Safety Coordinator, Network Manager and Head teacher.

Does school have an Online Safety Policy and procedures	**YES / NO**
Date of latest update:	
Date of future review:	
The Policy & procedures was agreed by Governors on:	
The Policy & procedures are available for staff to access at:	
The Policy & procedures are available for parents to access at:	
The responsible member of the Senior Leadership Team is:	
The Governor responsible for Online Safety is:	
The Designated Safeguarding Lead is:	
The Online Safety Coordinator is:	
The Remote Education Lead is:	
Were all stakeholders (e.g., students, staff, & parents) consulted when updating the school Policy & procedures?	**YES / NO**
Has up-to-date Online Safety training been provided for all members of staff (not just teaching staff)?	**YES / NO**
Do all members of staff sign an Acceptable Use Agreement on appointment?	**YES / NO**
Are all staff made aware of the school's expectation around safe and professional online behaviour?	**YES / NO**
Is there a clear procedure for staff, students, and parents to follow when responding to or reporting an online safety incident of concern?	**YES / NO**
Have online safety materials from CEOP, Childnet and UKCIS etc. been obtained?	**YES / NO**
Is online safety training provided for all students (appropriate to age and ability and across all Key Stages and curriculum areas)?	**YES / NO**
Are online safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	**YES / NO**
Do parents or students sign an Acceptable Use Agreement?	**YES / NO**
Are staff, students, parents, and visitors aware that network and internet use is closely monitored, and individual usage can be traced?	**YES / NO**
Has an ICT security audit been initiated by SLT?	**YES / NO**
Is personal data collected, stored, and used according to the principles of the Data Protection Act 2018?	**YES / NO**
Is internet access provided by an approved educational internet service provider which complies with DfE requirements?	**YES / NO**
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	**YES / NO**
Are members of staff with responsibility for managing filtering, network access, and monitoring systems adequately supervised by a member of SLT?	**YES / NO**

Does the school log and record all online safety incidents, including any action taken?	**YES / NO**
Are the Governing Body and SLT monitoring and evaluating the Policy and procedures regularly?	**YES / NO**