Policy Reference H05
ICT Acceptable Use and Online Safety Policy

Every school within Cumbria Futures Federation aims to provide a safe and hardworking environment where every child can be successful, whatever their abilities.

Our Values

- Courage and Compassion
- Inclusion and Equality
- Respect and Courtesy
- Optimism and Perseverance
- Forgiveness and Tolerance
- Ambition and Achievement

Version No	Author/Owner	Date Written	Note of amendments made	Authorised by	Date
01-2018	JR	August 2018	New policy created from model policy plus elements from Beacon Hill and Solway's existing policies		
01-2019	JR	Jan 2019	Updates related to GDPR		22/1/19

REVIEW SHEET

Contents

POLICY

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 requirement to ensure that children and young people are able to use online and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school Online Safety Policy and procedures will help to ensure safe and appropriate use. The development and implementation of such a strategy will involve all the stakeholders in a child's education from the Head teacher and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil 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 which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety Policy and procedures is used in conjunction with other school Policies including the Overarching Safeguarding Statement, Child Protection, Data Protection and Whole School Behaviour.

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

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

2. Definitions

For the purposes of this document a child, young person, pupil or student is referred to as a 'child' or a 'pupil' and they are normally under 18 years of age.

Wherever the term 'parent' is used this includes any person with parental authority over the child concerned e.g. carers, legal guardians etc.

Wherever the term 'Head teacher' is used this also refers to any Manager with the equivalent responsibility for children.

Wherever the term 'school' is used this also refers to all the schools with our Federation as well as the Federation itself.

Associated School Policies and procedures
This Policy should be read in conjunction with the following school Policies/procedures:

- Overarching Safeguarding Statement
- Child Protection Policy and procedures
- Data Protection Policy including procedures for CCTV
- Health and Safety Policy and procedures
- Whole School Behaviour Policy
- Procedures for Using Students Images
- Code of Conduct for staff and other adults

3. Communication/Monitoring/Review of this Policy and procedures

This Policy and procedures will be communicated to staff, students and the wider community in the following ways:

- Posted on the school website/Learning Platform/staffroom/shared staff drive
- Policy and procedures to be discussed as part of the school induction pack for new staff and other relevant adults including (where relevant) the staff Acceptable Use Agreement
- Acceptable Use Agreements discussed with students at the start of each year
- Acceptable Use Agreements to be issued to external users of the school systems (e.g. Governors) usually on entry to the school
- Acceptable Use Agreements to be held in pupil and personnel files

The Online Safety Policy is referenced from within other school Policies and procedures as outlined above.

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

4. Schedule for Development / Monitoring / Review

This Online Safety Policy and procedures was approved by the *Governing Body/Governing Body Committee on:*	*August 2018*
The implementation of this Online Safety Policy and procedures will be monitored by the:	*Senior Leadership Team, Pastoral team, Governors*
Monitoring will take place at regular intervals:	*Once a year*
The *Governing Body/Governing Body Committee* will receive a report on the implementation of the Online Safety Policy and procedures generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*At least once a year or as requested*
The Online Safety Policy and procedures will be reviewed in accordance with the Governors decision on frequency, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*August 2019*
Should serious Online safety incidents take place, the following external persons/agencies will be informed:	*LA ICT Manager, DO, Police, Information Commissioner's Office, Cumbria LSCB Hub*

The school will monitor the impact of the Policy and procedures using l*ogs of reported incidents.*

5. Scope of the Policy

This Policy and procedures applies to all members of the school community (including staff, students, volunteers, parents, visitors, community users) who have access to and are users of School ICT systems, both in and out of School.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety related incidents covered by this Policy and procedures, which may take place out of school, but is linked to membership of the School. The 2011 Education Act increased these powers with regard to the searching for, and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken with regard to issues covered by the published Whole School Behaviour Policy.

The School will deal with such incidents within this Policy and procedures and the Whole School Behaviour Policy which includes anti-bullying procedures and will, where known, inform parents of incidents of inappropriate on-line safety behaviour that take place out of school.

PROCEDURES

1. Roles and Responsibilities

The following section outlines the roles and responsibilities for on-line safety of individuals and groups within the school:

1.1 Governors

The role of the Governors/online safety Governor is to:

- ensure that the school follows all current online safety advice to keep the children and staff safe;
- approve the Online Safety Policy and procedures and review its effectiveness. This will be carried out by the Governors/Governors Sub-committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor
- support the school in encouraging parents and the wider community to become engaged in online safety activities;
- regular review with the Online Safety Coordinator (including incident logs, filtering/change control logs etc.)

1.2 Head teacher

The Head teacher has overall responsibility for online safety provision. The day to day responsibility for online safety may be delegated to the Online Safety *Coordinator*.

The Head teacher will:

- take overall responsibility for data and data security;
- ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements;
- ensure that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant;
- ensure 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;
- receive regular monitoring reports from the Online Safety Coordinator.
- be aware of the procedures to be followed in the event of a serious online safety incident or an allegation being made against a member of staff or volunteer (see flow chart on dealing with online safety incidents – Appendix I, 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.

1.3 Online Safety Coordinator/Designated Safeguarding Lead

The Online Safety Coordinator/Designated Safeguarding Lead will:

- take day-to-day responsibility for online safety issues and take a lead role in establishing and reviewing the school online safety procedures and documents;
- promote an awareness and commitment to e-safeguarding throughout the school community;
- ensure that online safety education is embedded across the curriculum;
- liaise with the school ICT technical staff
- ensure students internet goes through appropriate filtering. There is the understanding this can never be 100% secure due to the nature of the internet
- communicate regularly with SLT and the designated online safety governor/committee to discuss current issues, 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 or allegation against a member of staff or volunteer;
- ensure that an online safety log is kept up to date;
- facilitate training and advice for staff and others working in the school;

- 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

1.4 Network Manager/Technical staff

The Network Manager/Systems Manager/ICT Technician/ICT Coordinator will:

- report any online safety related issues that arise, to the Online Safety Coordinator;
- ensure that users may only access the school's networks through an authorised and properly enforced password protection procedures, in which passwords are regularly changed;
- ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack e.g. keeping virus protection up to date;
- 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;
- the school's procedures on web filtering, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices;
- that he/she keeps up to date with the school's Online Safety Policy and procedures and technical information in order to effectively carry out their Online safety role and to inform and update others as relevant;
- that the use of the network/Virtual Learning Environment (VLE)/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Coordinator/Head teacher/Senior Leader/ (as in the section above) for investigation/action/sanction;
- ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster and in order to complement the business continuity process;
- keep up-to-date documentation of the school's e-security and technical procedures.

1.5 Learning Platform Leader

It is the responsibility of the Learning Platform Leader to ensure that all data held on students on the Learning Platform is adequately protected.

1.6 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.

1.7 All Staff

It is the responsibility of all staff to:

- read, understand and help promote the school's Online Safety Policy and procedures
- read, understood and adhere to the school Staff Acceptable Use Agreement;
- be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school procedures with regard to these devices;
- report any suspected misuse or problem to the Online Safety Coordinator;
- maintain an awareness of current online safety issues and guidance e.g. through CPD opportunities;
- model safe, responsible and professional behaviours in their own use of technology;
- 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.

Teachers must:

- ensure that online safety issues are embedded in all aspects of the curriculum and other school activities;
- monitor, supervise and guide students carefully when engaged in ICT activity in lessons, extra-curricular and extended school activities;
- ensure that students are fully aware of research skills and are made aware of legal issues relating to electronic content such as copyright laws.
- ensure that during lessons where internet use is pre-planned students are guided to sites checked as suitable for their use and that processes are known and used when dealing with any unsuitable material that is found in internet searches.

1.8 Students

Taking into account the age and level of understanding, the key responsibilities of students are to:

- use the school ICT systems in accordance with the Pupil Acceptable Use Agreement – see Appendix D or E, which they and/or their parents will be expected to sign before being given access to school systems;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- know and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- know what action to take if they or someone they know feels worried or vulnerable when using online technology;
- know and understand school procedures on the use of mobile phones, digital cameras and hand-held devices.
- know and understand school procedures on the taking/use of images and on cyber-bullying;
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy and procedures 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 Online Safety Policy and procedures.

1.9 Parents

Parents 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 do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/VLE and information about national/local online safety campaigns/literature.

The key responsibilities for parents are to:

- support the school in promoting online safety which includes the students' use of the Internet and the school's use of photographic and video images;
- endorsing (by signature) the Pupil Acceptable Use Agreement – see Appendix D or E;
- access the school website/VLE/online pupil records in accordance with the relevant school Acceptable Use Agreement;
- consult with the school if they have any concerns about their children's use of technology;
- ensure that they themselves do not use the internet/social network sites/other forms of technical communication in an inappropriate or defamatory way;
- support the school's approach to online safety by not uploading or posting to the Internet any pictures, video or text that could upset, offend or threaten the safety of any member of the school community or bring the school into disrepute.

2. Training

2.1 Staff and Governor Training

This school:

- ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- makes regular training available to staff on online safety issues and the school's online safety education programme; through staff inset and training time.
- provides, 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.

2.2 Parent Awareness and Training

This school operates a rolling programme of advice, guidance and training for parents, including:

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

3. Teaching and Learning

3.1 Why Internet use is Important

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

3.2 How Internet Use Benefits Education

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between students worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DfE;
- access to learning wherever and whenever convenient.

3.3 How Internet Use Enhances Learning

Increased computer numbers and improved Internet access may be provided, but its impact on students learning outcomes should also be considered.

Developing effective practice in using the Internet for teaching and learning is essential. Students need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet.

Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be developed.

This school:

- Has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE 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 the wrong sort of 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 reasons;
    - Understand the impact of cyberbullying, sexting 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 will model safe and responsible behaviour in their own use of technology during lessons;
- ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online, online gaming/gambling etc.

3.4 Students with Additional Needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' online safety rules. However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities need to be planned and well managed for these children and young people.

Here are some considerations regarding possible ways to support a generic group of children who may require additional support to move forward in safeguarding

A fundamental part of teaching online safety is to check pupil's understanding and knowledge of general personal safety issues. Some students may need additional teaching that includes 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.

- *Rules are very helpful to all students and it is important to achieve consistency of how rules can be applied.*
- *This is a difficult area for some students who will usually learn rules within certain contexts, but who will find it difficult to transfer these rules across environments, lessons or teachers.*
- *As consistency is so important for these students, there is a need to establish online safety rules for school that are similar to those which should be in place at home. It is not always the case that these are in place, or understood, so they need reinforced regularly at school.*
- *Working with parents and sharing information with them would be relevant to all children, but this group especially.*
- *There will always be exceptions to rules and if this is the case, then these students will need to have additional 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.*
- *It might be helpful to consider presenting the rules as being linked to consequences such that you are teaching cause-effect rather than a list of procedures. This needs to be achieved carefully so as to use realistic and practical examples of what might happen if… without frightening students.*

How rules are presented could be vital to help these students understand and apply some of the rules they need to learn:

- *Visual support is usually important to help most students' understanding but some areas of this topic are quite abstract in nature and difficult to represent visually i.e.*

    - *Uncomfortable*
    - *Smart*
    - *Stranger*
    - *Friend*

    It might be helpful to ask students to produce a drawing or write a mini-class dictionary that describes and defines these words in their own terms.

- *Visual support can be useful but it is more likely that the students will respond to multi-media presentations of the rules such as interactive power-point slides, screensavers, spoken recordings of the main rules or sounds that they can associate with decisions they make while using the internet. The really useful thing about these is the repetition and practice that students can have with these which may not be so easy if spoken language were used.*
- *If visual prompts are used to help remember the rules, the picture or image support needs to give the students some improved understanding of what the rule is about. It is quite easy to find attractive pictures that link to other abstract ideas not related to internet use i.e. use of a compass to show "lose track" of a search when a head looking confused is more like what happens.*
- *This group of students are vulnerable to poor social understanding that may leave them open to risks when using the internet individually, but also when with peers.*
- *It can be common for peers to set up scenarios or "accidents" regarding what they look for on the internet and then say it was someone else who has done so. Adults need to plan group interactions carefully when raising awareness of internet safety.*
- *Some students in this group may choose recreational internet activities that are perhaps simpler or aimed at students younger than themselves. By their very nature, these activities tend to be more controlled and less open to naïve mistakes. Staff need to plan how to manage students who may want to do the same as other peers but who may need small step teaching due to limited experiences with internet use.*
- *For various reasons, students with additional needs may find it difficult to explain or describe events when using the internet.*

- *Some students might find it easier to show adults what they did i.e. replay which will obviously have its own issues for staff regarding repeating access.*
- *Some students are very quick to click with the mouse and may not actually know what they did or how something happened. Gentle investigation will be more productive than asking many questions.*
- *Some students may not be able to ask for help. Staff will need to know specific students well so that this can be addressed.*
- *Students may need a system or a help sound set up on computers which will help them to get adult attention. If students don't recognise that they need help, then adult supervision is the safe way to improve their recognition of this.*

4. Managing Information Systems

4.1 Maintaining Information Systems Security

Discussion:

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and students.

ICT security is a complex issue which cannot be dealt with adequately within this document. A number of agencies can advise on security including network suppliers.

Local Area Network (LAN) security issues include:

- Users must act reasonably e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For staff, flouting the school Acceptable Use Agreement may be regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

- Broadband firewalls and local CPEs (Customer Premises Equipment) are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between schools and the network provider.

- **The security of the school information systems and users will be reviewed regularly.**
- **Virus protection will be updated regularly.**
- *Unapproved software will not be allowed in work areas or attached to email.*
- *Files held on the school's network will be regularly checked.*
- *The ICT coordinator/network manager will review system capacity regularly.*
- *Use of user logins and passwords to access the school network will be enforced – see Section 6.2 below.*

The school broadband and online suppliers are CLEO Broadband and Cumbria Schools ICT Support

4.2 Password Security

Schools are 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 is 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; logs are maintained of access by users and of their actions while users of the system.

The school will be responsible for ensuring that the school infrastructure/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;**
- **logs are maintained of access by users and of their actions while users of the system.**

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE).

The management of password security will be the responsibility of The Network 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 Network Manager.

Any changes carried out must be notified to the member of staff responsible for issuing and coordinating password security (above).

Users will change their passwords at intervals decided by the person responsible for the overall security of the system.

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:

- *at induction;*
- *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 ICT and/or Online Safety lessons*
- *through the Acceptable Use Agreement*

The following rules apply to the use of passwords:

- *the password should be a minimum of **4** Characters long and must include three of – uppercase character, lowercase character, number, special character;*

- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on;*
- *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 user. We need to ensure that the person asking for the password change is indeed the user who's password is being changed.*

The "master/administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe). (Alternatively, where the system allows more than one "master/administrator" log-on, the Head teacher or other nominated senior leader should be allocated those master/administrator rights.

Audit/Monitoring/Reporting/Review:

The responsible person will ensure that full records where appropriate are kept of:

- *User Ids and requests for password changes;*
- *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.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed by (Online Safety Coordinator/Online Safety Committee/Online Safety Governor) at regular intervals ,annually.

4.3 Managing Email

Discussion:

Email is an essential means of communication for both staff and students. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents can be created, for example.

The implications of email use for the school and students need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to students that bypass the traditional school boundaries.

A central question is the degree of responsibility that can be delegated to individual students as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible.

In the school context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of students and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents, students and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

Secondary schools should limit students to email accounts approved and managed by the school. For EYFS and primary schools, whole-class or project email addresses should be used. When using external providers to provide students with email systems, schools must pay close attention to the sites terms and conditions as some providers have restrictions of use and age limits for their services.

Spam, phishing and virus attachments can make email dangerous. The school provider uses industry leading email relays to stop unsuitable mail using robust filtering.

Possible statements:

- **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.**
- **Whole-class or group email addresses will be used in primary schools for communication outside of the school.**
- **Staff will only use official school provided email accounts to communicate with students and parents, as approved by the Senior Leadership Team.**
- **When emailing more than one external individual or group (i.e. not staff or governors) then BCC MUST be used to ensure data protection requirements are met – i.e. that personal or business email addresses that the school holds are not shared with anyone else.**
- *Access in school to external personal email accounts may be blocked.*

- *Excessive social email use can interfere with learning and will be restricted.*
- *Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.*
- *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. Staff should email Safeguarding Leads.*
- **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 ICT provider ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.*

4.4 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 Hotmail, BTInternet, G-mail or any other Internet based webmail service for sending email containing sensitive information is not permitted;
- Where your conclusion is that email must be used to transmit such data:
    - Obtain express consent from your manager to provide the information by email;
    - 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;
        - Verify (by phoning) the details of a requestor before responding to email requests for information;
        - Do not copy or forward the email to any more recipients than is absolutely necessary.
    - Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
    - 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.

4.5 Zombie Accounts

Possible statements:

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;
- Regularly change generic passwords to avoid unauthorised access (Microsoft© advise every 42 days).

Further advice is available at IT Governance Click here to access.

4.6 Managing Published Content

Discussion:

Many schools have created excellent websites and communication channels, which inspire students to publish work of a high standard. Websites can celebrate students' work, promote the school and publish resources for projects. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

Sensitive information about schools and students could be found in a newsletter but a school's website is more widely available. Publication of any information online should always be considered from a personal and school security viewpoint. Material such as staff lists or a school plan may be better published in the school handbook or on a secure part of the website which requires authentication.

- **The contact details on the website are the school address, email and telephone number. Staff or students' personal information are not published.**
- *Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)*
- *The head teacher 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.*

4.7 Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, students and parents need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement procedures to reduce the likelihood of the potential for harm:

Possible Statements:

- **We gain parental permission for the use of digital photographs or video involving their child as part of the school agreement form when their child joins the school. This is a once in a school lifetime consent. Parents are required to inform the school if their consent changes.**
- **We do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials/DVDs.**
- **When using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.**
- *Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones/personal equipment for taking pictures of students;*
- *The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;*
- *Staff are allowed to take digital/video images to support educational aims, but must follow school procedures concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*

- *Students are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;*
- *Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.*
- *If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use.*
- *Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Pupil's work can only be published with the permission of the pupil and parents.*

4.8 Managing Social Networking, Social Media and Personal Publishing Sites

Discussion:

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control. For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

Possible Statements:

- **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 wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.**
- *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 pupil 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.*
- *Pupil 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 pupil'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 – see Appendix F.*
- **Further guidance can be found in the document 'Safe Use of Facebook and Other Social Networking Sites' on the KAHSC website**.
- *A sample advice leaflet for parents on Social Networking Sites, in particular, Facebook, can be found at Appendix H.*

4.9 Managing Filtering

Levels of Internet access and supervision will vary according to the pupil's age and experience. Access profiles must be appropriate for all members of the school community. Older secondary students, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. Systems to adapt the access profile to the pupil's age and maturity are available.

Access controls fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit students' access to a narrow range of content.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil access.
- Key loggers record all text sent by a workstation and analyse it for patterns.
- Schools installing or managing their own filtering systems and procedures must be aware of the responsibility and demand on management time. Thousands of inappropriate sites are created each day and many change URLs to confuse filtering systems. It is the Senior Leadership Team's responsibility to ensure appropriate procedures are in place and all members of staff are suitably trained to supervise Internet access.

It is important that schools recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone). Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access and that Acceptable Use Agreements are in place. In addition, Internet Safety rules should be displayed, and both children and adults should be educated about the risks online. There should also be an Incident Log to report breaches of filtering or inappropriate content being accessed. Procedures need to be established to report such incidents to parents and the LA where appropriate. Any material that the school believes is illegal must be reported to appropriate agencies such as Internet Watch Foundation (IWF), Cumbria Police or CEOP (see online safety contacts and references).

Websites which schools believe should be blocked centrally should be reported to the Schools Broadband Service Desk. Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the students. Often this will mean checking the websites, search results etc. just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- *The school's broadband access will include filtering appropriate to the age and maturity of students.*
- *The school will work with the Schools Broadband team CLEO to ensure that filtering procedures are continually reviewed.*
- *The network administrator is to be made aware of all breaches of filtering.*
- *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 Click here to access.*
- *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 Click here to access, Cumbria Police or CEOP Click here to access.*
- *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.*

4.10 Managing Video conferencing

Video conferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education.

Equipment ranges from small PC systems (web cameras) to large room-based systems that can be used for whole classes or lectures.

The National Educational Network (NEN) is a private broadband, IP network interconnecting the 13 regional schools' networks across England with the Welsh, Scottish and the Northern Ireland networks.

Schools with full broadband have access to services such as gatekeepers and gateways to enable schools to communicate with external locations. Schools may also decide to use conferencing services such as Skype and Flashmeeting. If Flashmeeting is used, conferences should always be booked as private and not made public. The conference URL should only be given to those who you wish to take part. Check who has signed into your conference; as a guest without a camera would not be visible.

Possible Statements:

- **All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.**
- *Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.*
- *External IP addresses will not be made available to other sites.*
- *Video conferencing contact information will not be put on the school Website.*
- *The equipment must be secure and if necessary locked away when not in use.*
- *School video conferencing equipment will not be taken off school premises without permission.*
- *Responsibility for the use of the video conferencing equipment outside school time will be established with care.*
- *Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference*

Users:

- **Students will ask permission from a teacher before making or answering a videoconference call.**
- **Videoconferencing will be supervised appropriately for the students' age and ability.**
- **Parent's consent should be obtained prior to children taking part in videoconferences, especially those with end-points outside of the school.**
- *Only key administrators should be given access to videoconferencing administration areas or remote control pages.*
- *Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.*

Content:

- *When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.*
- *Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.*
- *If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.*
- *Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.*

4.11 Webcams and CCTV

- *The school uses CCTV for security and safety. The only people with access to this are Office staff where the screens are located and the Site Manager / ICT Manager.*
- *Notification of CCTV use is displayed at the front of the school. Please refer to the Information Commissioners Office (ICO) for further guidance and the school CCTV procedures.*
- *We do not use publicly accessible webcams in school.*
- *Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.*
- *Misuse of the webcam by any member of the school community will result in sanctions.*
- *Consent is sought from parents and staff on joining the school, in the same way as for all images*

4.12 Managing Emerging Technologies

Discussion:

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible. Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation.

Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many students and families; this could be used to communicate a pupil's absence or send reminders for exam coursework. There are dangers for staff however if personal phones are used to contact students and therefore a school owned phone should be issued or made available.

The inclusion of inappropriate language or images is difficult for staff to detect. Students may need reminding that such use is inappropriate and conflicts with school Policy and procedures. Abusive messages should be dealt with under the Whole School Behaviour Policy.

- **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 Agreement/Mobile Phone procedures.*

4.13 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- **Fairly and lawfully processed;**
- **Processed for limited purposes;**
- **Adequate, relevant and not excessive;**
- **Accurate;**
- **Kept no longer than is necessary;**
- **Processed in accordance with the data subject's rights;**
- **Secure;**
- **Only transferred to others with adequate protection.**

More detailed information can be found in the School Data Protection Policy.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. The management of Data should be included within the school Data Protection Policy. Schools should also ensure that they take account of relevant local authority Policy and guidance as it applies to the individual school.

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

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

- *the data must be encrypted and password protected;*
- *the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected);*
- *the device must offer approved virus and malware checking software;*
- *the data must be securely deleted from the device, in line with school procedures (below) once it has been transferred or its use is complete.*

4.14 Disposal of Redundant ICT Equipment

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to:
  - The Waste Electrical and Electronic Equipment Regulations 2006
  - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  - Environment Agency Guidance (WEEE) Click here to access

- ICO Guidance - Data Protection Act 1998 Click here to access
- Electricity at Work Regulations 1989

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- The school's disposal record will include:
  - Date item disposed of;
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? *
  - How it was disposed of e.g. waste, gift, sale
  - Name of person and/or organisation who received the disposed item

  *** if personal data is likely to be held the storage media will be over written multiple times or 'scrubbed' to ensure the data is irretrievably destroyed.**
- Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

5. Policy Decisions

5.1 Authorising Internet Access

The school should allocate Internet access to staff and students on the basis of educational need. It should be clear who has Internet access and who has not. Authorisation is generally on an individual basis in a secondary school. In a primary school, where pupil usage should be fully supervised, all students in a class could be authorised as a group. Normally most students will be granted Internet access; it may be easier to manage lists of those who are denied access. Parental permission should be encouraged for Internet access in all cases - a task that may be best organised as new students join the school. If schools do request parental consent for internet access it is essential to record this data. Schools must be aware that students should not be prevented from accessing the internet unless the parents have specifically denied permission or the child is subject to a sanction as part of the Whole School Behaviour policy.

- **The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.**
- **All staff will read and sign the Staff Acceptable Use Agreement before using any school ICT resources.**
- *Parents will be asked to read and sign the School Acceptable Use Agreement for pupil access and discuss it with their child, where appropriate.*
- *Parents will be informed that students will be provided with supervised Internet access appropriate to their age and ability.*
- *When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).*

5.2 Assessing Risks

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will need to address the fact that it is not possible to completely remove the risk that students might access unsuitable materials via the school system.

Risks can be considerably greater where tools are used which are beyond the schools control such as most popular social media sites.

- **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 the LA can accept liability for the material accessed, or any consequences resulting from Internet use.**

- **The school will audit ICT use to establish if the Online Safety Policy and procedures is adequate and that the implementation of the Online Safety Policy is appropriate – see Appendix A for a sample Online Safety Audit.**
- *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.*
- *Methods to identify, assess and minimise risks will be reviewed regularly.*

5.3 Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and obviously banned from school and all other ICT systems. Other activities e.g. Cyber-bullying are against the rules and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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					x
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					x
	adult material that potentially breaches the Obscene Publications Act in the UK					x
	criminally racist material in UK					x
	pornography				x	
	promotion of any kind of discrimination				x	x
	promotion of racial or religious hatred				x	x
	threatening behaviour, including promotion of physical violence or mental harm				x	x
	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				x	
Using school systems to run a private business					x	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					x	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					x	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer / network access codes					x	

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
and passwords)					
Creating or propagating computer viruses or other harmful files				x	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				x	
Online gaming (educational)		x			
Online gaming (non-educational)		x			
Online gambling				x	
Online shopping/commerce				x	
File sharing				x	
Use of social networking sites				x	
Use of video broadcasting e.g. Youtube		x			

5.4 What are the risks?

The risks that can be posed to young people and adults when online have been identified by the EUKids online project, which was later referenced in paragraph 1.3 of Dr Tanya Byron in "Safer Children in a Digital World" (2008).

	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	Adverts Spam Sponsorship Personal Info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias, Racist or Misleading info or advice
Contact (Child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers, Being groomed	Self-harm, Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading information/advice

Byron Review (2008): Click here to access

5.5 Responding to Incidents of Concern

Discussion:

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However it is also important to consider the risks associated with the way these technologies can be used. This Online Safety Policy and procedures recognises and seeks to develop the skills that children and young people need when communicating and using technologies enabling them to keep safe and secure and act with respect for others. Online safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about students and in developing trust so that issues are reported.

Staff should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the school Designated Safeguarding Lead.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, schools should determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible, after contacting Children's Services if the offence is deemed to be out of the remit of the school to deal with.

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

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **extremism or radicalisation of individuals**
- **other criminal conduct, activity or materials - school should refer to the Flow Chart found at Appendix I.**

- *In this school there is monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions*
- *All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyber-bullying, illegal content etc.).*
- *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 of 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.

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

incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows DEPENDING ON THE EXACT NATURE AND CIRCUMSTANCES OF THE TRANSGRESSION.

Students **Possible Actions / Sanctions**

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

The below are suggestions and would depend upon the exact nature and circumstance of the identified transgression.

Staff **Actions / Sanctions**

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

5.6 Managing Cyber-bullying

Cyber-bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF (now DfE) 2007.

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobile phones, gaming or the Internet, they can often feel very alone, particularly if

the adults around them do not understand cyber-bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents understand how cyber-bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst students. These measures should be part of the school's Behaviour Policy which must be communicated to all students, school staff and parents;
- gives Head teachers the ability to ensure that students behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police or Pastoral Staff in the first instance.

For more information please read "Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies" Click here to access.

DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyber-bullying: Click here to access.

- **Cyber-bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the Whole School Behaviour 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 will be clear procedures in place to investigate incidents or allegations of Cyber-bullying.**
- *Students, staff and parents will be advised to keep a record of the bullying as evidence.*
- *The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.*
- *Students, staff and parents will be required to work with the school to support the approach to cyber-bullying and the school's online safety ethos.*
- *Sanctions for those involved in cyber-bullying may include:*
  - *The bully will be asked to remove any material deemed to be inappropriate or offensive.*
  - *A service provider may be contacted to remove content if the bully refuses or is unable to delete content.*
  - *Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance with the Whole School Behaviour Policy, Acceptable Use Agreement and Disciplinary Procedures.*
  - *Parents of students will be informed.*
  - *The Police will be contacted if a criminal offence is suspected.*

5.7 Managing Learning Environment/Platforms

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, students and parents, as well as support for management and administration. It can enable students and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and students can develop online and secure e-portfolios to showcase examples of work.

The Virtual Learning Platform/Environment (VLE) must be used subject to careful monitoring by the Senior Leadership Team (SLT). As usage grows throughout the school then more issues could arise regarding content, inappropriate use and behaviour online by users. The SLT has a duty to annually review and update the Policy and procedures

- **SLT and staff will regularly monitor the usage of the VLE by students and staff in all areas, in particular message and communication tools and publishing facilities.**
- **Students/staff will be advised about acceptable conduct and use when using the VLE.**
- **Only members of the current pupil, 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 pupil'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 pupil to fulfil a specific aim and may have a limited time frame.*

5.8 Managing Mobile Phones and Personal Devices

Mobile phones and other personal devices such as Games Consoles, Tablets, PDA, MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet access all common features. Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school should carefully consider how this is managed on their premises.

Mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render students or staff subject to cyber-bullying;
- Internet access on phones and personal devices can allow students to bypass school security settings and filtering;
- They can undermine classroom discipline as they can be used on "silent" mode;
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of students or staff.

Procedures which prohibit students from taking mobile phones to school could be considered to be unreasonable and unrealistic for schools to achieve. Many parents would also be concerned for health and safety reasons if their child were not allowed to carry a phone and many staff also use mobile phones to stay in touch with family.

Due to the widespread use of personal devices it is essential that schools take steps to ensure mobile phones and devices are used responsibly at school and it is essential that pupil use of mobile phones does not impede teaching, learning and good order in classrooms. Staff should be given clear boundaries on professional use.

The use of mobile phones and personal devices is a school decision – we allow students to carry a mobile device on the proviso it is not seen, used or heard during the school day. There are procedures in place for any transgression of this.

- **The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use Agreement.**
- **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.**
- **The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable materials, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.**
- **School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour Policy or bullying procedures.**
- *If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.*
- *Mobile phones and personal devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. They should be switched off (not placed on silent) and stored out of sight on arrival at school. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent whilst in the school.*
- *The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the Head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head teacher is authorised to withdraw or restrict authorisation for use at any time if it is deemed necessary. Where permission is given by the Head teacher, no images or videos are to be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people in the image.*
- *The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.*
- *Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.*
- *Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break time.*
- *Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.*

Students use of personal devices:

- *The school strongly advices that pupil mobile phones should not be brought into school. However, the school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. If this is the case, the circumstances should be discussed with the class teacher/Head of Year and the normal rules regarding use during the school day will apply.*
- *If a pupil breaches the school procedures then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or students as appropriate in accordance with the school procedures.*

- *Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.*
- *If a pupil needs to contact his/her parents they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.*
- *Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.*
- *Students will be provided with school mobile phones or other hand-held personal devices to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.*

Staff use of personal devices:

- *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.*
- *Staff will be issued with a school phone where contact with students or parents is required.*
- *Mobile phones and personally owned devices will be switched off or switched to 'silent' mode; Bluetooth communication should be "hidden" or switched off and mobile phones or personally owned devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.*
- *If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.*
- *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.*
- *Where members of staff are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. 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.*
- *If a member of staff breaches the school Policy and procedures then disciplinary action may be taken.*

	Staff & other adults				**Students**			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X				x			
Use of mobile phones in lessons		X				x	x	
Use of mobile phones in social time	x					x		
Taking photos on mobile phones or other camera devices		X						x
Use of hand held devices e.g. PDAs, PSPs	x						x	
Use of personal email addresses in school, or on school network	x							x

Use of school email for personal emails		x						x
Use of chat rooms/facilities			X					X
Use of instant messaging		X						X
Use of social networking sites		X						X
Use of blogs		X					X	

6. Communicating Policy and procedures

6.1 Introducing the Policy and procedures to Students

Many students are very familiar with the culture of mobile and Internet use and it is wise to involve them in designing the School Online Safety Policy, possibly through a pupil council. As students' perceptions of the risks will vary, the online safety rules may need to be explained or discussed.

Posters covering online safety rules should be displayed in every room with a computer to remind students of the rules at the point of use.

The pupil and parent agreement form should include a copy of the school online safety rules appropriate to the age of the pupil.

Consideration must be given as to the curriculum place for teaching online safety. This could be as an ICT lesson activity, part of the pastoral programme or part of every subject whenever students are using the internet.

Useful online safety programmes include:

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

- **All users will be informed that network and Internet use will be monitored.**
- **An online safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst students.**
- *Pupil instruction regarding responsible and safe use will precede Internet access.*
- *An online safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.*
- *Online safety training may be part of the transition programme across the Key Stages and when moving between establishments. It will form part of the curriculum upon entry.*
- *Online Safety rules or copies of the pupil Acceptable Use Agreement will be posted in all rooms with Internet access.*
- *Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.*
- *Particular attention to Online Safety education will be given where students are considered to be vulnerable.*

6.2 Discussing the Policy and procedures with Staff

It is important that all staff feel confident to use new technologies in teaching and the School Online Safety Policy and procedures will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

All staff must understand that the rules for information systems misuse for school employees are specific and that instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager to avoid any possible misunderstanding.

Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside of the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.

ICT use is widespread and all staff who will access the system, including administration, midday supervisors, caretakers, governors and volunteers should be included in awareness raising and training. Induction of new staff should include a discussion about the school Online Safety Policy and procedures.

- **The Online Safety Policy and procedures will be formally provided to, and discussed, with all members of staff.**
- **To protect all staff and students, the school will implement Acceptable Use Agreements.**
- **Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.**
- **Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.**
- *Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.*
- *The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the students.*
- *All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within 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.*

6.3 Enlisting Parents' Support

Internet use in students' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, students may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is covered by an appropriate use policy.

- **Parents' attention will be drawn to the school Online Safety Policy and procedures in newsletters, and on the school website.**
- *A partnership approach to online safety at home and at school with parents will be encouraged. This may include highlighting online safety at other attended events e.g. parent evenings and sports days.*
- *Parents will be encouraged to read and sign the school Acceptable Use Agreement for students and discuss its implications with their children.*
- *Information and guidance for parents on online safety will be made available to parents in a variety of formats.*

- *Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.*
- *Interested parents will be referred to organisations listed in the "online safety Links" at Appendix K.*

7. Complaints

Parents, teachers and students should know how to use the school's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. Online 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.

A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the school's Behaviour Policy. Potential child protection or illegal issues must be 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.

The school will take all reasonable precautions to ensure online 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 the misuse of on-line systems will be dealt with under the school's Complaints procedure.
- Complaints about cyberbullying are dealt with in accordance with our Anti-bullying procedures.
- Complaints related to child protection are dealt with in accordance with school/LA Child Protection Policy and procedures.
- Any complaints about staff misuse will be referred to the Head teacher.
- All online safety complaints and incidents will be recorded by the school including any actions taken (see Appendix J).

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

- Interview/counselling by class teacher/Head of Year/Online Safety Coordinator/Head teacher;
- 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 Online Safety Coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

- *Parents and students will need to work in partnership with the school to resolve issues.*
- *All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.*
- *Reference will be made to the local Police and/or the Safeguarding Hub procedures for handling potentially illegal issues.*
- *Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.*
  All members of the school community will be 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.

8. Acknowledgements

With thanks to Jeff Haslam (E-Safety Consultant), Hertfordshire County Council, Kent County Council, the South West Grid for Learning, Cumbria LSCB, CEOP, UKCCIS, Childnet and the DfE whose guidance and information has contributed to the development of this Policy and procedures.

Appendix A

Cumbria Future Federation ONLINE SAFETY AUDIT

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

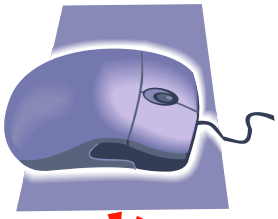
Does the school have an Online Safety Policy and procedures	**YES**
Date of latest update:	May 2017
Date of future review:	May 2020
The school Online Safety Policy and procedures was agreed by governors on:	23 May 2017
The Policy and procedures is available for staff to access at:	Policies folder
The Policy and procedures is available for parents to access at:	The School Website
The responsible member of the Senior Leadership Team is:	J Rowlands
The Governor responsible for Online Safety is:	
The Designated Safeguarding Lead is:	G Wigginton
The Online Safety Coordinator is:	J Gribbon
Were all stakeholders (e.g. students, staff and parents) consulted when updating the school Online Safety Policy and procedures?	**NO**
Do all members of staff sign an Acceptable Use Agreement on appointment?	**YES**
Are all staff made aware of the schools expectation around safe and professional online behaviour?	**YES**
Is there a clear procedure for staff, students and parents to follow when responding to or reporting an online safety incident of concern?	**YES**
Have online safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	**YES**
Is online safety training provided for all students (appropriate to age and ability and across all Key Stages and curriculum areas)?	**YES**
Are online safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	**YES**
Do parents or students sign an Acceptable Use Agreement?	**YES**
Are staff, students, parents and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**YES**
Has an ICT security audit been initiated by SLT?	**YES**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**YES**
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements?	**YES**
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	**YES**
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	**YES**
Does the school log and record all online safety incidents, including any action taken?	**YES**
Are the Governing Body and SLT monitoring and evaluating the school Online Safety Policy and procedures on a regular basis?	**YES**

This page is intentionally blank for printing purposes

These rules help us to stay safe on the Internet.

Think then Click

We only use the Internet when an adult is with us.



We can click on the buttons or links when we know what they do

We can search the internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Think then Click

We ask permission before using the Internet.

We only use websites that our teacher has chosen.

We immediately close any webpage we don't like.

We only email people our teacher has approved.

We send emails that are polite and friendly.

We never give out a home address or phone number.

We never arrange to meet anyone we don't know.

We never open emails sent by anyone we don't know.

We never use Internet chat rooms.

We tell the teacher if we see anything we are unhappy with.

RESPONSIBLE INTERNET USE

SECONDARY SCHOOLS

Rules for Staff and Students

The computer system is owned by the school. This Responsible Internet Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the pupil's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- Email should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for email they send and for contacts made.
- Anonymous messages and chain letters are not permitted.
- The use of chat rooms is not allowed.
- The school ICT systems may not be used for private purposes, unless the head teacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted.
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

The school may exercise its right to monitor the use of the school's 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's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix E

PUPIL ACCEPTABLE USE AGREEMENT

Solway Community School and Beacon Hill Community School

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc. for educational purposes.
- I will only log on to the school network/Learning Platform, other systems and resources with my own user name and password. I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username or password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address for educational purposes. I will check my email regularly and carry out routine "housekeeping" of my email messages.
- I will not give out my personal information or that of others such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I will make sure that all ICT communications with students, teachers or others is responsible, polite and sensible. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will 'log off' when leaving a computer.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will only save files to the network that are related to schoolwork. I will not use filenames that could be considered offensive.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I am aware that when I take images of students and/or staff, that I must only store and use these for school purposes and in line with school procedures and must never distribute these outside the school network without the permission of all parties involved, including in school breaks and all occasions when you are in school uniform or when otherwise representing the school.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts.
- I understand that I am responsible for my actions, both in and out of school and that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement when I am out of school and where they involve my membership of the school community (e.g. cyberbullying, use of images or personal information etc.)
- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- When I am using the internet to find information, I should take care to check that the information that I access is accurate as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I will respect the privacy and ownership of others' work online at all times and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission. Where work is protected by copyright, I will not try to download copies (including music and videos).
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will only use my personal hand-held/external devices (USB devices) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails unless I know and trust the person or organisation that sent the email due to the risk of the attachment containing a virus or other harmful programme.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent may be contacted and any illegal activities will be reported to the Police.

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

✂----------

Beacon Hill and Solway Community School

Pupil Acceptable Use – Pupil and Parent Agreement

Dear Parent,

ICT including the internet, learning platforms, email and mobile technologies and online resources have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of online safety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or P Esslemont

I have read, understood and agree to follow the terms of this Acceptable Use Agreement when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. camera, PDA, USB stick, etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil: _____ Class/Year Group: _____

Parent Signature		**Date**	
Pupil Signature		**Date**	

STAFF & VOLUNTEER
ACCEPTABLE USE POLICY AGREEMENT

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This Agreement is designed to ensure that all staff and volunteers (including Governors) are aware of their responsibilities when using any form of ICT. This applies to ICT used in school and also applies to use of school ICT systems and equipment out of school and use of personal equipment in school or in situations related to their role within the school. All staff and volunteers (where they are using technology in school) are expected to sign this Agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.
This Acceptable Use Agreement is intended to ensure that:

- staff and volunteers are responsible users and stay safe while using technologies for educational, personal and recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- staff are protected from potential risk from the use of ICT in their everyday work and work to ensure that young people in their care are safe users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

Keeping Safe

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will only use my own user names and passwords which I will choose carefully so they cannot be guessed easily. I will also change the passwords on a regular basis.
- I will not use any other person's user name and password.
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to students.
- I will ensure that my data is regularly backed up.
- I will ensure that I 'log off' after my network session has finished.
- If I find an unattended machine logged on under another user's username, I will **not** continue using the machine – I will 'log off' immediately.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will not accept invitations from school students to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.

  As damage to professional reputations can inadvertently be caused by quite innocent postings or images, I will also be careful with who has access to my pages through friends and friends of friends, especially with those connected with my responsibilities at the school, such as parents and their children.
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when it is deemed necessary that I am required by law or by school procedures to disclose it an appropriate authority.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the school personal data guidelines. I will not send personal information by email as it is not secure.
- Where personal data is transferred outside the secure school network, it must be encrypted or password protected. Personal data can only be taken out of school or accessed remotely when authorised, in advance, by the Head teacher or Governing Body. Personal or sensitive data taken off site in an electronic format must be encrypted, e.g. on a password secured laptop, memory stick or individual documents password protected. Staff leading a trip are expected to take relevant pupil information with them but this must be held securely at all times.

- I will ensure that any private social networking sites/blogs etc. that I create, or actively contribute to:

- do not reveal confidential information about the way the school operates
- are not confused with my school responsibilities in any way.

- I will not try to bypass the filtering and security systems in place.
- I will only use my personal ICT in school for permissible activities and I will follow the rules set out in this agreement. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

Promoting Safe Use by Learners

- I will support and promote the school's Online Safety, Data Protection and Behaviour Policies and help students to be safe and responsible in their use of ICT and related technologies.
- I will model safe use of the internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school procedures if an issue arises in school that might compromise a learner, user or school safety or if a pupil reports any concerns.

Communication

- I will only use the school's email/Internet/Intranet/Learning Platform and any related technologies for professional purposes or for uses deemed 'acceptable' by the Head teacher or Governing Body.
- I will communicate on-line in a professional manner and tone, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. Anonymous messages are not permitted.
- I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- I will only communicate with students and parents using the school's approved, secure email system(s). Any such communication will be professional in tone and manner.
- I am aware that any communication could be forwarded to an employer or governors.
- I will only use chat and social networking sites that are approved by the school.
- I will not use personal email addresses on the school ICT systems unless I have permission to do so.

Research and Recreation

- I will not browse, upload, download, distribute or otherwise access any materials which are illegal, discriminatory or inappropriate or may cause harm or distress to others.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity.
- I know that all school ICT is primarily intended for educational use and I will only use the systems for personal or recreational use if this is allowed by the school.

Sharing

- I will not access, copy, remove or otherwise alter any other user's file, without their permission.
- I will respect the privacy and ownership of others' work online at all times and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission, and will credit them if I use it.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos). If I am unsure about this, I will seek advice.
- Images of students and/or staff will only be taken, stored and used for professional purposes using school equipment in line with school procedures.
- I will only take images/video of students and staff where it relates to agreed learning and teaching activities and will ensure I have parent/staff permission before I take them.
- If images are to be published on-line or in the media I will ensure that parental/staff permission allows this.
- I will not use my personal equipment to record images/video unless I have permission to do so from the Head teacher or other Senior Manager.
- I will not keep images and/or videos of students stored on my personal equipment unless I have permission to do so. If this is the case, I will ensure that these images cannot be accessed or copied by anyone else or used for any purpose other than that for which I have permission.

- Where these images are published by the school (e.g. on the school website/prospectus/social media), I will ensure that it is not possible in our initial publication to identify the people who are featured by full name or other personal information.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

Buying/Selling/Gaming

- I will not use school equipment for on-line purchasing, selling or gaming unless I have permission to do so.

General Equipment Use

- Any ICT equipment issued to you remains the property of the school.
- On termination of employment/volunteering or for extended absences the school will require equipment to be returned.
- The school reserves the right to demand equipment to be returned at any time within 7 calendar days.
- I will not download or install any unapproved software, system utilities or resources that might compromise the network or are not adequately licensed.
- I will not try to alter computer settings without the appropriate permission.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.

Problems

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Online Safety Coordinator or Head teacher.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

For all staff & volunteers: I understand if I do not follow these rules that this may result in loss of access to these resources.

For school employed staff only: I understand this forms part of the terms and conditions set out in my contract of employment and any breaches may result in possible disciplinary action.

✂ --

Staff/Volunteer Acceptable Use Agreement

I agree to use the school network and associated resources in a responsible way and observe all the restrictions as explained in the staff ICT Acceptable Use Agreement (as set out above). I agree to use ICT by these rules when:

- ✓ I use school ICT systems at school or at home when I have permission to do so
- ✓ I use my own ICT (where permitted) in school
- ✓ I use my own ICT out of school to access school sites or for activities relating to my employment or position within school.

Staff/Volunteer Name			
Job Title (where applicable)			
Signed		**Date:**	

This page is intentionally blank for printing purposes

Appendix H

SOCIAL NETWORKING SITES - FACEBOOK

GUIDANCE FOR PARENTS

There are many children of School age who have Facebook Profiles whilst under the allowed age, despite the permitted minimum age to use the site being 13, according to the site terms and conditions.

Our school is committed to promoting the safe and responsible use of the Internet and as such we feel it is our responsibility to raise this particular issue as a concern. Whilst children cannot access Facebook or other social networking sites at school, they could have access to it on any other computer or mobile technology. Websites such as Facebook offer amazing communication and social connections, however they are created with their audience in mind and this is specifically 13 years and older. Possible risks for children under 13 using the site and similar sites of a Social Networking nature may include:

- Facebook use 'age targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated they were when they registered;
- Children may accept 'friend requests' from people they don't know in real life which could increase the risk of inappropriate contact or behaviour;
- Facebook is one of the social networking sites used by those attempting to radicalise young people;
- Language, games, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal or unsuitable for children;
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own;
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and other options;
- Facebook could be exploited by bullies and for other inappropriate contact;
- Facebook cannot and does not verify its members therefore it important to remember that if your child can lie about who they are online, so can anyone else!

We feel that it is important to point out to parents the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from school and sometimes by a child, their friends, siblings or even parents. We will take action (such as reporting aged profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our children.

Should you decide to allow your children to have a Facebook profile we strongly advise you to:

- Check their profile is set to private and that only 'friends' can see information that is posted;
- Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting offensive messages or photos;
- Ask them to install the CEOP (Child Exploitation and Online Protection Centre) application from www.facebook.com/clickceop on their profile. This places a bookmark on their profile to CEOP and the 'Report Abuse' button which has been known to deter offenders;
- Have a look at the advice for parents from Facebook www.facebook.com/help/?safety=parents;
- Set up your own profile so you understand how the site works and ask them to add you as a friend on their profile so you can keep track of what they are posting online;
- Make sure your child understands the following rules:

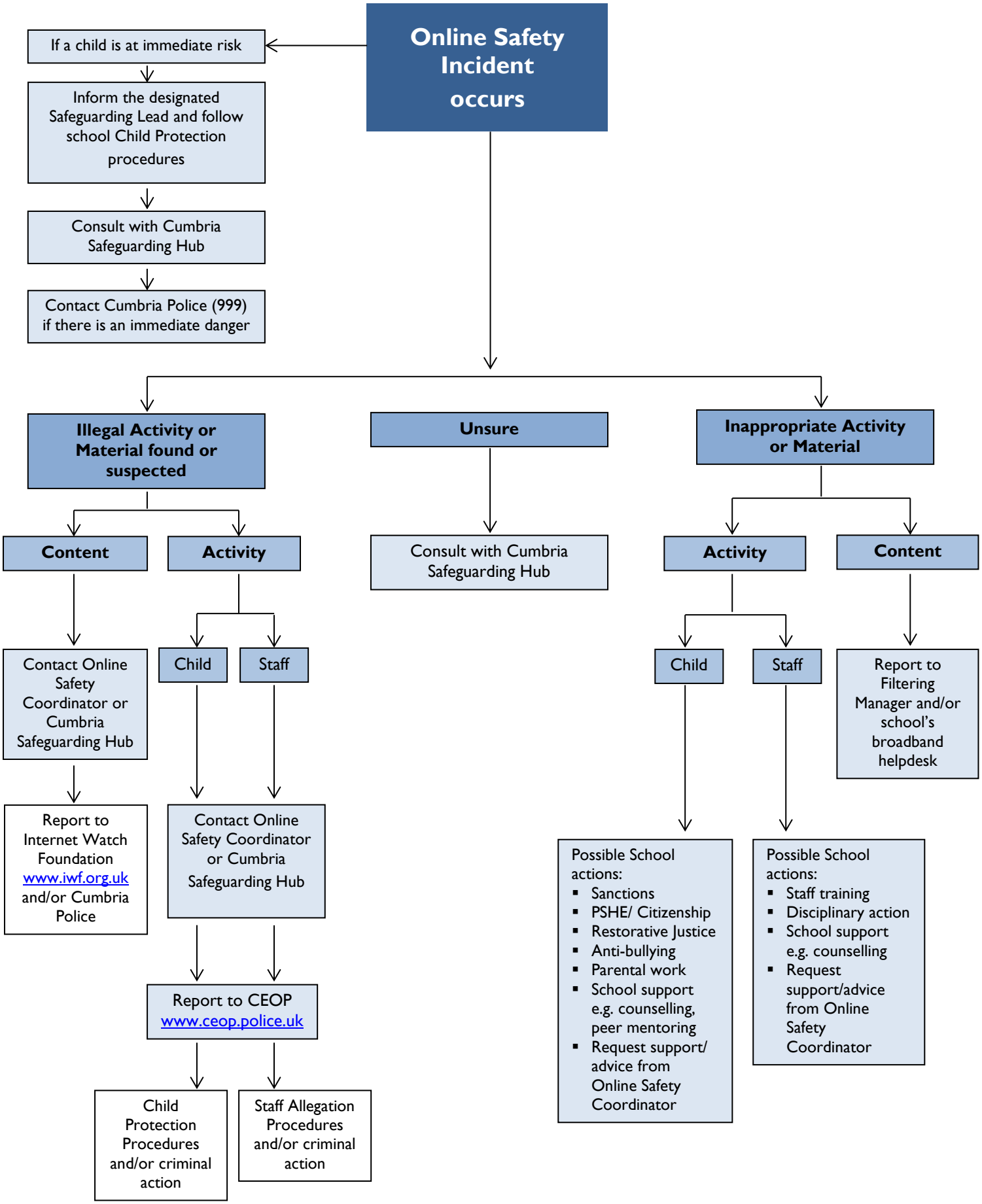
  - Always keep your profile private;
  - Never accept friends you don't know in real life;
  - Never post anything which could reveal your identity;
  - Never post anything you wouldn't want your parents to see;
  - Never agree to meet someone you only know online without telling a trusted adult;
  - Always tell someone if you feel threatened or someone upsets you.

We recommend that all parents visit the CEOP ThinkUKnow website for more information on keeping your child safe online Click here to access.

This page is intentionally blank for printing purposes

Appendix I

RESPONSE TO AN INCIDENT OF CONCERN



Review school Online Safety Policy and procedures; record actions in Online Safety incident log and implement any changes in the future.

Appendix J

CUMBRIA FUTURES FEDERATION - ONLINE SAFETY INCIDENT LOG

SEE ALSO DAILY INCIDENT / PASTORAL LOG AS APPROPRIATE.

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

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

Appendix K

ONLINE SAFETY LINKS

The following links may help those who are developing or reviewing a school Online Safety Policy and procedures.

- **CEOP (Child Exploitation and Online Protection Centre)**: Click here to access
- **Childline**: Click here to access
- **Childnet**: Click here to access
- **Internet Watch Foundation (IWF)**: Click here to access
- **Cumbria Local Safeguarding Children Board (Cumbria LSCB)**: Click here to access
- **Kidsmart**: Click here to access
- **Think U Know website**: Click here to access
- **Virtual Global Taskforce — Report Abuse**: Click here to access
- **EE Safety Education**: Click here to access
- **O2 Safety Education**: Click here to access
- **Information Commissioner's Office (ICO)** Click here to access
- **INSAFE** Click here to access
- **Anti-Bullying Network** - Click here to access
- **Cyberbullying.org** - Click here to access
- **Learning Curve Education:** Click here to access
- **UK Safer Internet Centre:** Click here to access
- **UK Council for Child Internet Safety (UKCCIS):** Click here to access
- **Wise Kids:** Click here to access
- **Teem:** Click here to access
- **Know the Net:** Click here to access
- **Family Online Safety Institute:** Click here to access
- **e-safe Education**: Click here to access
- **Facebook Advice to Parents:** Click here to access
- **Test your online safety skills:** Click here to access

The above internet site links were correct at the time of publishing. School staff are advised to check the content of each site prior to allowing access to students.

Department for Education/Home Office guidance for schools

PREVENT Duty statutory guidance for Public Bodies: England and Wales – March 2015
The PREVENT Duty – non-statutory Departmental advice for Schools and Childcare Providers – DfE – June 2015
How Social Media is used to encourage travel to Syria and Iraq – Home Office advice to schools – June 2015

LEGAL FRAMEWORK

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should have a copy of The Home Office "Children & Families: Safer from Sexual Crime" document as part of their child protection packs. Click here to access.

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure

- Not transferred to other countries without adequate protection

The Computer Misuse Act 1990 (sections 1 - 3)
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Public Order Act 1986 (sections 17 — 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;

- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Criminal Justice and Immigration Act 2008
Section 63 offence to possess "extreme pornographic image"
63 (6) must be "grossly offensive, disgusting or otherwise obscene"
63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006
Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyber-bullying/ Bullying:

- Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of students off site.
- School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/antibullying procedures.

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial.
- The right to respect for private and family life, home and correspondence.
- Freedom of thought, conscience and religion.
- Freedom of expression.
- Freedom of assembly.
- Prohibition of discrimination.
- The right to education.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Appendix M

GLOSSARY OF TERMS

Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology) – *NOTE: Becta Closed in 2011*
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CLEO	The Regional Broadband Consortium of Cumbria and Lancashire – is the provider of broadband and other services for schools and other organisations in Cumbria and Lancashire
CPD	Continuous Professional Development
DfE	Department for Education
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by Naace Click here to access
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network.
KS1	Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups e.g. KS3 = years 7 to 9 (age 11 to 14)
LA	Local Authority
LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
MLE	Managed Learning Environment
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. CLEO in Cumbria) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
RBC	Regional Broadband Consortia (e.g. CLEO) have been established to procure broadband connectivity for schools in England. There are 13 RBCs covering most local authorities in England, Wales and Northern Ireland.

SEF	Self Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection
TUK	Think U Know – educational E-Safety programmes for schools, young people and parents.
URL	Uniform Resource Locator (URL) it is the global address of documents and other resources on the World Wide Web.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol