MARYPORT
CHURCH OF ENGLAND
JUNIOR SCHOOL

e-SAFETY POLICY

Head teacher: Mrs J Ormond

Chair of Governors: Ms C O'Brien

Guidance:

Why does a School or Setting need an e-Safety Policy?

This School e-Safety Policy is intended to help school leaders produce a suitable E-Safety policy document which will consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Safeguarding Statement, Child Protection, Data Protection and Whole School Behaviour policies for example.

It is essential for schools to take a leading role in e-Safety. Schools should support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, all schools have should have acceptable use policies, and ensure that parents are aware of the procedures for e-Safety within the school. Recognising the growing trend for home-school links and extended school activities, schools should take an active role in providing information and guidance for parents on promoting e-Safety messages in home use of ICT, too.

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> *"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-Safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their e-Safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

Schools are expected to evaluate their level of e-Safety in the Ofsted Self Evaluation Form (SEF) and will be subject to an increased level of scrutiny by Ofsted Inspectors during school inspections. Many schools are opting to gain recognition for the quality of their ICT provision through ICTMark accreditation. The ICTMark Self Review Framework (SRF) contains a number of aspects regarding the school's e-Safety policies and provision.

An effective School e-Safety Policy must be tailored to the needs of each school and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole school community.

It is suggested that consultation in the production of this policy should involve:

- *Governors*
- *Teaching Staff and Support Staff*
- *Students/pupils*
- *Parents/Carers*
- *Community users and any other relevant groups.*

Due to the ever changing nature of Information and Communication Technologies, it is best practice that the school reviews the e-Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place.

e-Safety Policy

Given the range of optional statements offered and the guidance notes provided, this template document is much longer than the resulting school policy is likely to be. It is intended that, while covering a complicated and ever changing aspect of the work of the school, the resulting policy should be concise and easily understood, if it is to be effective and adopted by all.

Groups or individuals responsible for producing the e-Safety policy may wish to carry out further reading/ research by using the e-Safety Links found in Appendix J to this document.

Contents

e-Safety Policy

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/pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

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

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student/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 sharing/distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication/contact with others, including strangers;
- Cyberbullying;
- 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 e-Safety policy is used in conjunction with other school policies including the overarching Safeguarding Statement, Child Protection, Data Protection and Whole School Behaviour Policies for example – see Point 1 below.

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

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

1. Associated School Policies

This Policy should be read in conjunction with the following school policies/procedures:

- Overarching Safeguarding Statement
- Child Protection Policy
- Data Protection Policy
- Health and Safety Policy
- Procedures for Using Pupils Images

- Whole School Behaviour Policy
- Cumbria County Council Information Technology Acceptable Use Guidance for School Based Staff Click here to access

2. Development/Monitoring/Review of this Policy

This e-Safety policy has been developed by a working group made up of:

- School e-Safety Coordinator
- Head teacher/Senior Leaders
- Teachers
- Support Staff
- Governors

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School/Student/Pupil Council
- Governors meeting/sub-committee meeting
- Parents evening
- School website/newsletters

2.1 Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the *Governing Body/Governors Sub-Committee on:*	*June 2016*
The implementation of this e-Safety policy will be monitored by the:	*ICT co-ordinator* *Senior Leadership team*
Monitoring will take place at regular intervals:	*Spring term each year*
The *Governing Body/Governors Sub-Committee* will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	*Spring term annually*
The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place. The next anticipated review date will be:	*March each year*
Should serious e-Safety incidents take place, the following external persons/agencies should be informed:	*LA ICT Manager, LADO, Police Commissioner's Office*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - students/pupils (e.g. Ofsted "Tell-us" survey)
    - parents/carers
    - staff

3. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students/pupils 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 cyberbullying, or other e-Safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and the Whole School Behaviour Policy which includes anti-bullying and will, where known, inform parents/carers of incidents of inappropriate e-Safety behaviour that take place out of school.

4. Roles and Responsibilities

The following section outlines the roles and responsibilities for e-Safety of individuals and groups within the school:

4.1 Governors

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors/Governors Sub-Committee receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *e-Safety Governor* **(currently Ms C O'Brien).** The role of the e-Safety Governor will include:

- regular meetings with the e-Safety Co-ordinator
- regular monitoring of e-Safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors committee/meeting

4.2 Head teacher and Senior Leaders

- The Head teacher is responsible for ensuring the safety (including e-Safety) of members of the school community, though the day to day responsibility for e-Safety will be delegated to the e-Safety Co-ordinator.
- The Head teacher/Senior Leaders are responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
- The Head teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles, this will be provided through CPD as appropriate.
- The Senior Leadership Team/Senior Management Team will receive regular monitoring reports from the e-Safety Coordinator.
- The Head teacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff (see flow chart on dealing with e-Safety incidents – Appendix H, and relevant Local Authority HR/school disciplinary procedures). The procedures for dealing with allegations against staff can be found within the school Child Protection Policy.

4.3 e-Safety Coordinator

School's e-Safety co-ordinator is Miss S Dover.

- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies/documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place;
- provides training and advice for staff;
- liaises with the Local Authority (where appropriate);
- liaises with school ICT technical staff;
- receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments;
- meets regularly with e-Safety Governor to discuss current issues, review incident logs and filtering/change control logs;
- attends relevant meeting/committee of Governors;
- reports regularly to Senior Leadership Team.

Incidents will be dealt with initially by the e-Safety co-ordinator and passed to senior staff as appropriate.

4.4 Network Manager/Technical staff

The Network Manager/Systems Manager/ICT Technician/ICT Co-ordinator is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets the e-Safety technical requirements outlined in the School Acceptable Use Policy and any relevant Local Authority e-Safety Policy and guidance;
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed;
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- that he/she keeps up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant;
- that the use of the network/Virtual Learning Environment (VLE)/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-Safety Co-ordinator/Head teacher/Senior Leader/Head of ICT/ICT Co-ordinator/Class teacher/Head of Year (as in the section above) for investigation/action/sanction;
- that monitoring software/systems are implemented and updated as agreed in school policies.

4.5 Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices;
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP) – see Appendix F;
- they report any suspected misuse or problem to the e-Safety Co-ordinator/Head teacher/ Senior Leader/Head of ICT/ICT Co-ordinator/Class teacher/Head of Year (as in the section above) for investigation/action/sanction;
- digital communications with students/pupils (email/Virtual Learning Environment (VLE)/ voice) should be on a professional level *and only carried out using official school systems;*
- e-Safety issues are embedded in all aspects of the curriculum and other school activities;
- students/pupils understand and follow the school e-Safety and acceptable use policy – see Appendix D or E depending on the age of pupils in school;

- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extra-curricular and extended school activities;
- they are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices;
- in lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.6 Designated Person for Child Protection (DPCP)

Should be trained in e-Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- cyberbullying.

4.7 e-Safety Committee

Ms C O'Brien (ICT link governor) will assist the *e-Safety Coordinator* with:

- the production/review/monitoring of the school e-Safety policy/documents;

4.8 Students/Pupils

Taking into account the age and level of understanding, students/pupils:

- are responsible for using the school ICT systems in accordance with the Student/Pupil Acceptable Use Policy (AUP) – see Appendix D or E, which they and/or their parents/carers 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;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyberbullying;
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school.

4.9 Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. 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 e-Safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy (AUP) – see Appendix D or E;
- accessing the school website/VLE/on-line student/pupil records in accordance with the relevant school Acceptable Use Policy.

- ensuring that they themselves do not use the internet/social network sites/other forms of technical communication in an inappropriate or defamatory way.

4.10 Community Users

Community Users who access school ICT systems/website/VLE as part of the Extended School provision will be expected to sign a AUP before being provided with access to school systems – see Appendix F.

5. Teaching and Learning

5.1 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.
- Pupils 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.

5.2 How Internet Use Benefits Education

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network (NEN) which connects all UK schools Click here to access NEN;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils 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.

5.3 How Internet Use Enhances Learning

- The school's Internet access will be designed to enhance and extend education.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

5.4 How Pupils will Learn How to Evaluate Internet Content

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

5.5 Pupils with Additional Needs

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

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

- A fundamental part of teaching e-Safety is to check pupil's understanding and knowledge of general personal safety issues. Some pupils 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 pupils and it is important to achieve consistency of how rules can be applied.
- This is a difficult area for some pupils 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 pupils, there is a need to establish e-Safety rules for school that are similar to those for home. 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 pupils 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 pupils.

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

- Visual support is usually important to help most pupils' 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 pupils 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 pupils 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 pupils 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 pupils 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 pupils 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 pupils in this group may choose recreational internet activities that are perhaps simpler or aimed at pupils 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 pupils 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, pupils with additional needs may find it difficult to explain or describe events when using the internet.
- Some pupils 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 pupils 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 pupils may not be able to ask for help. Staff will need to know specific pupils well so that this can be addressed.
- Pupils may need a system or a help sound set up on computers which will help them to get adult attention. If pupils don't recognise that they need help, then adult supervision is the safe way to improve their recognition of this.

6. Managing Information Systems

6.1 Maintaining Information Systems Security

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 Policy 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.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- 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 http://www.cleo.net.uk/ and Cumbria Software Systems (ICT support at time of writing policy).

6.2 Password Security

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 policies);
- access to personal data is securely controlled in line with the school's personal data policy;
- 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 **(Mrs M Penn, School Administrator)**

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 **(Mrs M Penn, School Administrator)** Any changes carried out must be notified to the member of staff responsible for issuing and co-ordinating password security (above).

Users will change their passwords every **90 days (once per term)**

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 e-Safety policy;
- through the Acceptable Use Agreement;

Pupils/students will be made aware of the school's password security procedures:

- in ICT and/or e-Safety lessons (reminders at the beginning of each academic year and as appropriate thereafter).
- through the Acceptable Use Agreement

Policy Statements:

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the e-Safety Committee (or other group).

All users will be provided with a username and password by (Gemini) who will keep an up to date record of users and their usernames. Staff users will be required to change their password every (90 days)

The following rules apply to the use of passwords:

- passwords must be changed every 90 days
- the last four passwords cannot be re-used;
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special character;
- the account should be "locked out" following six successive incorrect log-on attempts;
- 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

The "master/administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Head teacher or other nominated senior leader and kept in a secure place.

Audit/Monitoring/Reporting/Review:

The responsible person **(Mrs M Penn, School Administrator)** will ensure that full records are kept of:

- User IDs and requests for password changes;
- User log-ons;
- Security incidents related to this policy.

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 (e-Safety Coordinator/e-Safety Committee/e-Safety Governor) at regular intervals (as requested but at least annually).

6.3 Managing Email

Guidance:

Email is an essential means of communication for both staff and pupils. 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 pupils need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries.

A central question is the degree of responsibility that can be delegated to individual pupils 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 pupils 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/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

The use of email identities such as john.smith@school.co.uk generally needs to be avoided for younger pupils, as revealing this information could potentially expose a child to identification by unsuitable people. Email accounts should not be provided which can be used to identify both a student's full name and their school. 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.

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils 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 pupils and parents/carers, as approved by the Senior Leadership Team.
- The official school email service may be regarded as safe and secure and is monitored. Staff and students/pupils 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, 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/pupils or parents/carers (email, chat, VLE etc.) must be professional in tone and content.
- Whole class or group email addresses will be provided with individual school email addresses for educational use. Pupils will 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 (Cleo) ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.

6.4 Emailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible;
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted;
- Where your conclusion is that e-mail must be used to transmit such data:

  - Obtain express consent from your manager to provide the information by e-mail;
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Verify the details, including accurate e-mail address, of any intended recipient of the information;
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information;
    - Do not copy or forward the e-mail 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 e-mail;
  - 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 e-mail;
  - Request confirmation of safe receipt.

6.5 Zombie Accounts

Zombie accounts refers 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.

6.6 Managing Published Content

Guidance:

Many schools have created excellent websites and communication channels, which inspire pupils to publish work of a high standard. Websites can celebrate pupils' 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 pupils 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 should be the school address, email and telephone number. Staff or pupils' personal information must not be 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 policies and copyright.

6.7 Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, students/pupils and parents/carers 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 policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies 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/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the pupil/student school career. A model Consent Form can be found in Kym Allan Health and Safety Consultants Ltd. (KAHSC) General Safety Series G21 Click here to access.
-

6.8 Managing Social Networking, Social Media and Personal Publishing Sites

Guidance:

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. Pupils 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. Further guidance can be found on the Cumbria LSCB website 'Online Communication Code of Conduct for Staff Working with Children' Click here to access and in the 'Safe Use of Facebook and Other Social Networking Sites' on the KAHSC website Click here to access.

- The school will control access to social media and social networking sites.
- Pupils 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.
- Pupils 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 students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' 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 Policy – see Appendix F.
- Further guidance can be found on the Cumbria LSCB website 'Online Communication Code of Conduct for Staff Working with Children' Click here to access and in the 'Safe Use of Facebook and Other Social Networking Sites' on the KAHSC website Click here to access.
- A sample advice leaflet for parents on Social Networking Sites, in particular, Facebook, can be found at Appendix G.

6.9 Managing Filtering

Guidance:

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. 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 pupils' 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 policies 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 Policies 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 e-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 pupils. 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 pupils.
- The school will work with the Schools Broadband team **(Cleo)** to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-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 policy 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 pupils, with advice from network managers.

6.10 Managing Videoconferencing

Guidance:

Videoconferencing 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.

At the time of reviewing this policy, school does not have this facility.

- All videoconferencing 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.*
- *Videoconferencing 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 videoconferencing equipment will not be taken off school premises without permission.*
- *Responsibility for the use of the videoconferencing 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:

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers 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.*

6.11 Webcams and CCTV

At the time of reviewing this policy, school does not have this facility.

- *The school uses CCTV for security and safety. The only people with access to this are.*
- *Notification of CCTV use is displayed at the front of the school. Please refer to the Information Commissioners Office (ICO) for further guidance Click here to access and the school CCTV Policy.*
- *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.*
- *Webcams can be found. Notification is given in this/these area(s) filmed by webcams by signage.*
- *Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.*

6.12 Managing Emerging Technologies

Guidance:

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 pupils 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 pupils 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. Pupils may need reminding that such use is inappropriate and conflicts with school policy. 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.
- *Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.*

6.13 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.

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 policy (below) once it has been transferred or its use is complete.

6.14 Disposal of Redundant ICT Equipment

- No ICT equipment can be disposed of through the school's general waste collection process.
- Any computers, or storage media, that may have held personal or confidential data must have their hard drives 'scrubbed' either before or as part of the disposal process. This is to ensure you do not contravene the Data Protection Act.

Guidance:

WEEE purchased on or after 13th August 2005:
Any WEEE (waste computers, etc.) purchased on or after 13th August 2005, that you wish to dispose of, are the responsibility of the manufacturer. That is, the manufacturer of this WEEE is obliged to dispose of the waste equipment Free of Charge (e.g. RM or DELL). However, whilst the disposal of the WEEE is free there may be a cost for transportation to the 'nominated' collection centre.

Many manufacturers require the request be submitted within a maximum of 30 days following dispatch of new equipment.)

WEEE purchased before 13th August 2005:
If you are purchasing new EEE (computers, etc.) to replace existing equipment that was purchased before 13th August 2005 it is the responsibility of the manufacturer (of the new equipment) to dispose of any items (on a one to

one basis, e.g. one new computer for one old computer) Free of Charge. Again you may bear a cost for transportation to the 'nominated' collection centre.

If you are disposing of WEEE – purchased before 13th August 2005 - that is not being replaced by any new purchase you will need to arrange for its lawful disposal. There will be a charge for this.

What do you need to do?
*EEE manufacturers that are compliant with the WEEE Directive will have a form that needs to be completed and returned to them as soon as possible and generally **within 30 days** of the new equipment having been dispatched by them.*

Are all manufacturers WEEE Compliant?
They should be but if they are not then it will be the responsibility of the school to arrange correct disposal of WEEE. WEEE compliant companies have a registration number.

Before making purchasing decisions you should establish whether the provider (of the new equipment) is WEEE complaint. If they are not there will be a charge for the disposal of any WEEE so you should include this in any cost comparisons you make when considering new EEE purchases.

- 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 Click here to access
  - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007 Click here to access
  - Environment Agency Guidance (WEEE) Click here to access
  - ICO Guidance - Data Protection Act 1998 Click here to access
  - Electricity at Work Regulations 1989 Click here to access

- 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.

7. Policy Decisions

7.1 Authorising Internet Access

Guidance:

The school should allocate Internet access to staff and pupils on the basis of educational need. It should be clear who has Internet access and who has not. In a primary school, where pupil usage should be fully supervised, all pupils in a class could be authorised as a group. Normally most pupils 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 pupils join or as part of the Home-School agreement. 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 pupils who are granted access to the school's electronic communications.
- All staff will read and sign the Staff Acceptable Use Policy (Appendix F) before using any school ICT resources.
- Parents will be asked to read and sign the School Acceptable Use Policy for pupil access (Appendix D or E) and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy (Appendix F).
- Parents will be informed that pupils 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).

- All pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

7.2 Assessing Risks

Guidance:

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 pupils 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. Guidance and considerations for schools around this topic can be found on the Cumbria LSCB website on Online Communication Code of Conduct for Staff Working with Children Click here to access.

- 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 e–Safety policy is adequate and that the implementation of the e–safety policy is appropriate – see Appendix A for a sample e-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.
-

7.3 Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyberbullying would be banned 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 that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

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

7.4 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

7.5 Responding to Incidents of Concern

Guidance:

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 e-Safety Policy 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. e-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 pupils 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 Person for Child Protection.

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 i.e.

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

school should refer to the Flow Chart found at Appendix H.

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Person for Child Protection will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Child Protection Policy for dealing with concerns.
- The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers 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 Children's Services and escalate the concern to the Police.
- Any racist incidents will be reported to Children's Services. Racist Incident Monitoring forms should be completed electronically through the **School Portal** Click here to access the Portal. This allows for individual incidents to be reported as and when they happen and will also generate a termly report for schools to agree to and return. Click here for the Children's Services Guidance to Racist Incidents.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Local Authority Designated Officer (LADO) – see Child Protection Policy.

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:

Students/Pupils **Actions / Sanctions**

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

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).		✓	✓	✓		✓		✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email							✓	✓
Unauthorised downloading or uploading of files		✓	✓					
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		✓			✓			
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓	✓			✓		
Deliberate actions to breach data protection or network security rules							✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓				
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		✓				✓		
Actions which could compromise the staff member's professional standing		✓	✓			✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school							✓	✓
Using proxy sites or other means to subvert the school's filtering system								✓
Accidentally accessing offensive or pornographic material and failing to report the incident					✓			
Deliberately accessing or trying to access offensive or pornographic material								✓
Breaching copyright or licensing regulations								✓
Continued infringements of the above, following previous warnings or sanctions							✓	✓

7.6 Handling e–safety Complaints

Guidance:

Parents, teachers and pupils 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. e-Safety incidents may have an impact on pupils, 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 disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Person for Child Protection. Advice on dealing with illegal use can, when deemed necessary, be discussed with Cumbria Police or Children's Services.

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e–safety complaints and incidents will be recorded by the school, including any actions taken (see Appendix I).
- Pupils and parents will be informed of the complaints procedure via the school website.
- Parents and pupils 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.
- Discussions will be held with the local Police and/or Children's Services to establish 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.

7.7 How the Internet is used across the Community

Guidance:

Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, supermarket or cyber café. Ideally, young people would encounter a consistent internet use policy wherever they are.

Regarding internet access in the community, there is a fine balance between ensuring open access to information whilst providing adequate protection for children and others who may be offended by inappropriate material. Organisations are developing access appropriate to their own client groups and pupils may find variations in the rules and even unrestricted Internet access. Although policies and practice may differ, community partners adhere to the same laws as schools. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with pupils on the reasons for the differences could be worthwhile.

Sensitive handling of cultural aspects is important. For instance filtering software should work across community languages and school Internet policies may need to reflect the pupils' cultural backgrounds.

- The school will liaise with local organisations to establish a common approach to e–safety.
- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

7.8 Managing Cyberbullying

Guidance:

Cyberbullying 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 cyberbullying 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/carers understand how cyberbullying 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 pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents/carers;*
- *gives head teachers the ability to ensure that pupils 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.

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 cyberbullying: Click here to access.

- Cyberbullying (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 cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers 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.

- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos, this is included as part of the Kidsafe programme..
- Sanctions for those involved in cyberbullying 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 pupils and staff may also be used in accordance with the Whole School Behaviour Policy, Acceptable Use Policy and Disciplinary Procedures.
  - Parent/carers of pupils will be informed.
  - The Police will be contacted if a criminal offence is suspected.

7.9 Managing Learning Environment/Platforms

Guidance:

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It can enable pupils 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 pupils 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 regarding the use of the VLE, and all users must be informed of any changes made.

- SLT and staff will regularly monitor the usage of the VLE by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the VLE.
- Only members of the current pupil, parent/carers 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, pupils 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:
  a) The user will be asked to remove any material deemed to be inappropriate or offensive.
  b) The material will be removed by the site administrator if the user does not comply.
  c) Access to the VLE for the user may be suspended.
  d) The user will need to discuss the issues with a member of SLT before reinstatement.
- A pupil's parent/carer 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.
- Pupils 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.
-

7.10 Managing Mobile Phones and Personal Devices

Guidance:

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.

However, 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 pupils or staff subject to cyberbullying;*
- *Internet access on phones and personal devices can allow pupils 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 pupils or staff.*

Staff should be given clear boundaries on professional use.

The use of mobile phones and personal devices is a school decision, however the following points have been provided to support schools in creating effective policies.

- The use of mobile phones by pupils in school is not allowed.
- 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.
- School staff may confiscate a phone or device if brought to school (this should be sent to the school office for safe keeping until the end of the school day.
- 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.
- Staff mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- Mobile phones 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.
- 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.

Pupils use of personal devices:

- If a pupil breaches the school policy 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/carers in accordance with the school policy..
- If a pupil needs to contact his/her parents/carers 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.

Staff use of personal devices:

- When out on trips/visits, staff are permitted to use their own personal phones for contacting parents within in a professional capacity in the event of an emergency and only if the school office is unavailable to make this contact in the first instance.

- Mobile phones and devices will be switched off or switched to 'silent' mode; Bluetooth communication should be "hidden" or switched off and mobile phones or 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.
- Personal devices such as mobile phones or cameras may be used to take photos or videos of pupils by staff although work-provided equipment is recommended for this purpose. Any photos/videos taken must adhere to all sections of this policy and must be uploaded to the server and deleted off the personal device as soon as is possible.
- If a member of staff breaches the school policy then disciplinary action may be taken.

	Staff & other adults				**Students/Pupils**			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photos on mobile phones or other camera devices		✓					✓	
Use of hand held devices e.g. PDAs, PSPs		✓					✓	
Use of personal email addresses in school, or on school network			✓					✓
Use of school email for personal emails				✓				✓
Use of chat rooms/facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites		✓						✓
Use of blogs		✓				✓		

8. Communication Policy

8.1 Introducing the Policy to Pupils?

Guidance:

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

Posters covering e–safety rules should be displayed in every room with a computer to remind pupils of the e–safety rules at the point of use – See Appendix B and C for age appropriate examples.

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

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

Useful e–safety programmes include:

- *Think U Know: www.thinkuknow.co.uk*
- *Childnet: www.childnet.com*
- *Kidsmart: www.kidsmart.org.uk*
- *Orange Education: www.orange.co.uk/education*
- *Safe: www.safesocialnetworking.org*

- All users will be informed that network and Internet use will be monitored.
- An e–safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An e–safety module will be included in the PSHE, Citizenship, Kidsafe and/or ICT programmes covering both safe school and home use.
- e–safety training will be part of the transition programme across the Key Stage and when moving between establishments.
- e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access – see Appendix B and C for age appropriate examples.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

8.2 Discussing the Policy with Staff

Guidance:

It is important that all staff feel confident to use new technologies in teaching and the School e–safety Policy 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 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 e–safety Policy.

- The e–safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- 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 pupils.
- 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.

8.3 Enlisting Parents’ Support

Guidance:

Internet use in pupils’ homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils 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.

One strategy is to help parents to understand more about ICT , perhaps by running courses and parent awareness sessions (although the resource implications will need to be considered). KAHSC offers e-Safety Training for pupils, staff and parents through Jeff Haslam, e-Safety Consultant. Contact Penny Gosling on Tel: 01228 210152 or email: penny.gosling@kymallanhsc.co.uk for further details.

- Parents’ attention will be drawn to the school e–safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read and sign the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on e–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 “e–safety Links” at Appendix J.

9. 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.

Appendix A

MARYPORT CHURCH OF ENGLAND JUNIOR SCHOOL
SCHOOL E-SAFETY AUDIT

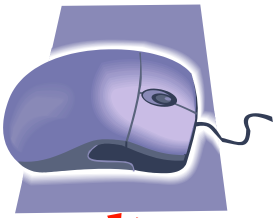
This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-Safety policy. Staff that could contribute to the audit include: Designated Person for Child Protection, SENCO, e-Safety Coordinator, Network Manager and Head teacher.

Does the school have an e-Safety Policy	**YES**
Date of latest update:	June 2016
Date of future review:	March 2017
The school e-Safety policy was agreed by governors on:	June 2016
The policy is available for staff to access at:	Staff shared area on school server
The policy is available for parents/carers to access at:	School website
The responsible member of the Senior Leadership Team is:	Mrs J Ormond
The governor responsible for e-Safety is:	Ms C O'Brien
The Designated Person for Child Protection is:	Mrs J Ormond
The e-Safety Coordinator is:	Miss S Dover
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school e-Safety Policy?	**NO**
Has up-to-date e-Safety training been provided for all members of staff? (not just teaching staff)	**YES**
Do all members of staff sign an Acceptable Use Policy 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, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	**YES**
Have e-Safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	**YES**
Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	**YES**
Are e-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**YES**
Do parents/carers or pupils sign an Acceptable Use Policy?	**YES**
Are staff, pupils, parents/carers 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 e-Safety incidents, including any action taken?	**YES**
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	**YES**

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 e-mails 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 student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail 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 D

Maryport Church of England Junior School

PUPIL ACCEPTABLE USE POLICY

These rules will help us to be fair to others and keep everyone safe.

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.

✂- -

Maryport Church of England Junior School

Pupil Acceptable Use – Pupil <u>and</u> Parent/Carer Agreement

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs H Beggs

Parent/Carer signature

We have discussed this and ………………………………………… (child's name) agrees to follow the e-Safety rules and to support the safe use of ICT at **Maryport Church of England Junior School**

Parent/Carers Name		**Pupil Class**	
Signed *(Parent/Carer)*		**Date**	
Signed *(Pupil)*		**Date**	

STUDENT/PUPIL ACCEPTABLE USE POLICY

SECONDARY SCHOOLS

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/Learning Platform with my own user name and 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 e-mail address.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- 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 not give out any personal information 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.
- Images of pupils and/or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of **NAME OF PERSON**.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- 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
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- 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/carer may be contacted.

✂- -

[School logo and details]

Pupil Acceptable Use – Pupil and Parent/Carer Agreement

Dear Parent/ Carer

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-Safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or **NAME OF PERSON**.

Pupil and Parent/ carer signature

We have discussed this document and …………………………………………………. (pupil name) of Class/Form ……… agrees to follow the e-Safety rules and to support the safe and responsible use of ICT at **XXXX** School.

Parent/Carers Signature		**Date**	
Pupil Signature		**Date**	

Maryport Church of England Junior School
STAFF / GOVERNOR/ VISITOR
ACCEPTABLE USE POLICY AGREEMENT

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional 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 employment by the school. All staff/Governors/visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with **Miss S Dover** (e-Safety coordinator) or **Mrs J Ormond** (Head teacher).

- I will only use the school's email/Internet/Intranet/Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head teacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head teacher or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of **Mrs J Ormond**
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes using school equipment in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head teacher.
- 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 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.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety, Data Protection and Behaviour policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

Staff / Governor / Visitor - Acceptable Use Agreement

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines. I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Name			
Job Title			
Signed		**Date:**	

Maryport Church of England Junior School
SOCIAL NETWORKING SITES - FACEBOOK
GUIDANCE FOR PARENTS/CARERS

There are many children of Primary School age or Years 7 and 8 in Secondary Schools who have Facebook Profiles 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 old. Possible risks for children under 13 using the site 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;
- 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/carers 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.

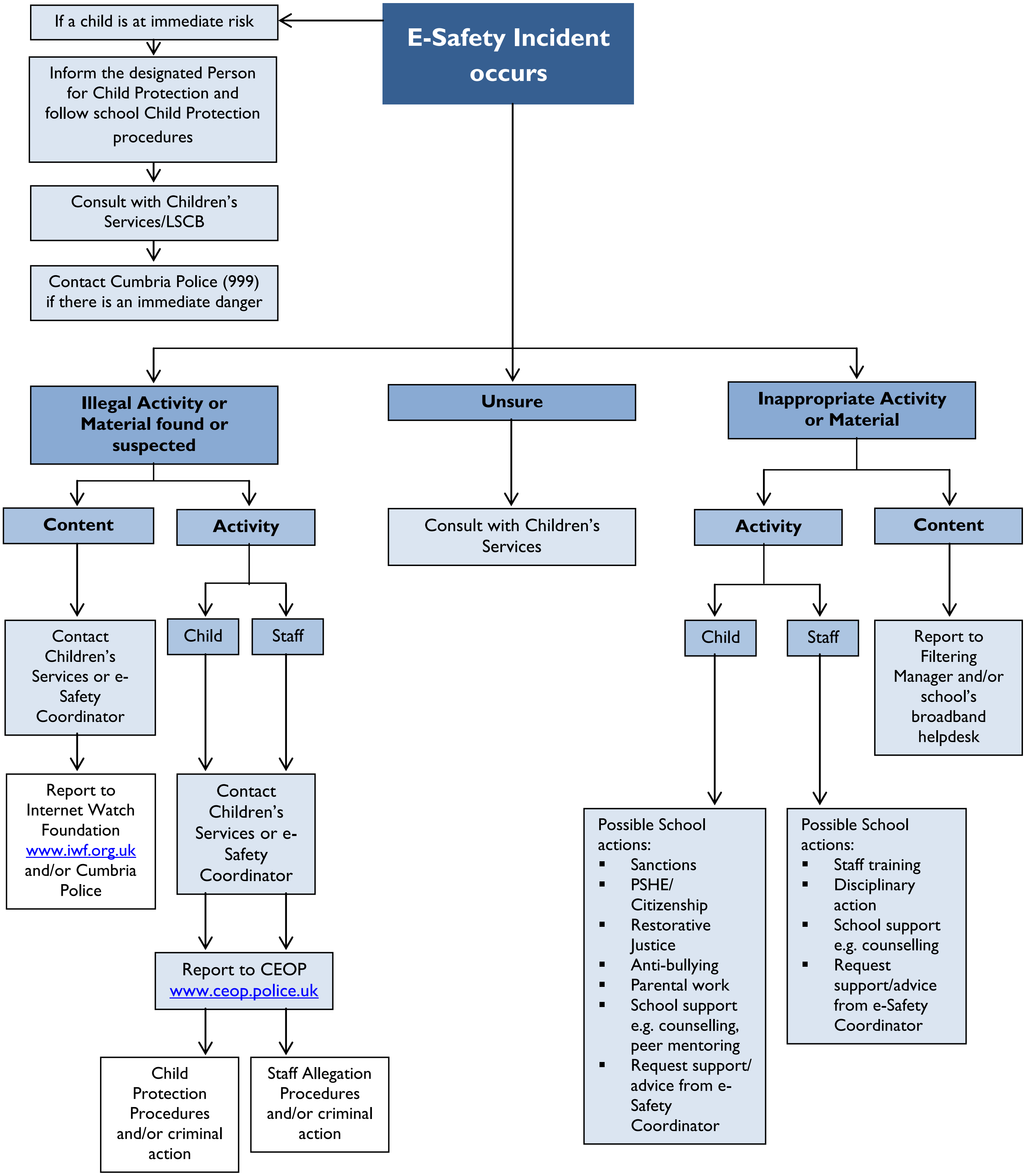
Should you decide to allow your children to have a Facebook profile we strongly advise you to:

- 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/carers 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/carers visit the CEOP ThinkUKnow website for more information on keeping your child safe online Click here to access.

RESPONSE TO AN INCIDENT OF CONCERN



E-Safety Incident occurs

If a child is at immediate risk

Inform the designated Person for Child Protection and follow school Child Protection procedures

Consult with Children's Services/LSCB

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

Illegal Activity or Material found or suspected

Content

Contact Children's Services or e-Safety Coordinator

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

Activity

Child

Staff

Contact Children's Services or e-Safety Coordinator

Report to CEOP www.ceop.police.uk

Child Protection Procedures and/or criminal action

Staff Allegation Procedures and/or criminal action

Unsure

Consult with Children's Services

Inappropriate Activity or Material

Activity

Child

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

Staff

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

Content

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

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

Appendix I

MARYPORT CHURCH OF ENGLAND JUNIOR SCHOOL
E-SAFETY INCIDENT LOG

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

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

E-SAFETY LINKS

The following links may help those who are developing or reviewing a school e-Safety policy.

- **CEOP (Child Exploitation and Online Protection Centre)**: Click here to access
- **Childline**: Click here to access
- **Childnet**: Click here to access
- **Click Clever Click Safe Campaign**: Click here to access
- **Cybermentors**: Click here to access
- **Digizen**: 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
- **Teach Today**: Click here to access
- **Think U Know website**: Click here to access
- **Virtual Global Taskforce — Report Abuse**: Click here to access
- **Orange Education**: Click here to access
- **Safe**: Click here to access
- **Information Commissioner's Office (ICO)** Click here to access
- **INSAFE** Click here to access
- **National Education Network (NEN)** E-Safety Audit Tool: Click here to access
- **Anti-Bullying Network** - Click here to access
- **Cyberbullying.org** - Click here to access
- **Ofcom Report:** 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
- **Teacher Tube:** Click here to access
- **Teach Today:** Click here to access
- **Beat Bullying:** Click here to access
- **BBC Teachers:** Click here to access
- **Grid Club**: Click here to access
- **Teem:** Click here to access
- **Sites for Teachers:** Click here to access
- **DfE:** 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
- **Record Management Society:** Click here to access
- **Test your online safety skills:** Click here to access
- **Cumbria County Council Information Technology Acceptable Use Guidance for School Based Staff:** Click here to access

BECTA publications ***(saved from the National Archives since BECTA's closure in 2011)***
Some of BECTA's guidance documents include:

- E-Safety - Click here to access
- Safeguarding Children Guide - - Click here to access
- Safeguarding Children Checklist - Click here to access
- LSCB Strategy - Click here to access
- Online Behaviours - Click here to access
- Safeguarding Learners - Click here to access

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 Cyberbullying/ Bullying:

- Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils 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 policy.

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.

GLOSSARY OF TERMS

AUP	Acceptable Use Policy – see templates earlier in this document
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
ECM	Every Child Matters
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

SRF Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark

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