Furness Vale Primary School
e–Safety Policy 2017

Derbyshire County Council believes that the use of information and communication technologies in schools brings great benefits. Recognising the e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications. This Policy template will help schools and settings to review their e-Safety Policy.

Schools and Settings e–Safety Policy Template 2012 Disclaimer

Derbyshire County Council (DCC) makes every effort to ensure that the information in this document is accurate and up to date. If errors are brought to our attention, we will correct them as soon as practicable.

Nevertheless, DCC and its employees cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication Schools and Settings e–Safety Policy Template 2012

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

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Schools and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Schools must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have.

Schools must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and the Governing body.

The e-Safety policy is essential in setting out how the school plans to develop and establish its e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

Teachers and officers working with child protection officers, multi-agency children's workforce professionals and Police have produced this template to help schools write their own e-Safety policies. The policy template provides a range of statements to make policy review easier and more comprehensive. It should be used to develop the schools e-Safety ethos and whole school approach. This policy template is suitable for all schools and other educational settings (such as Pupil Referral Units, 14-19 settings etc) and we encourage all establishments to ensure that their e-Safety policy is fit for purpose and individualised for the context of each setting. For simplicity we have used the terms 'school', 'pupils' and 'students' in the document, but wider educational settings are equally relevant.

How to use this document

It is recommended that schools see e-Safety as a whole school issue. As such, they should develop a holistic approach to writing and updating the school's e-Safety Policy as well as embedding safe practice.

DCC strongly recommends that guidance highlighted by the red **D** in the e-Safety Policy template is included and is rigorously implemented.

This policy template provides a structure for policy writing and material to stimulate this essential debate. It is strongly recommended that all stakeholders (staff, parents/carers, pupils etc.) should be actively involved in writing the e-Safety policy to collaboratively create a policy that is appropriate for their establishment.

When writing your policy, educational, management and technical issues will need to be considered and members of staff should be involved from a variety of roles and experience. The policy is presented in this template document as a series of questions with discussion content and a range of suggested statements. The writing team should consider each question and discussion content and select statements appropriate to the school context. They may choose to modify or replace any statements.

1.1 Who will write and review the policy?

Discussion:
The e-Safety Policy is part of many different schools policies including the ICT Policy, Child Protection or Safeguarding Policy, Anti-Bullying and School Development Plan and should relate to other policies including those for behaviour, for personal, social and health education (PSHE) and for citizenship. Policy construction provides a method to review practice - in this case the use of technology and its benefits and risks. The more that staff, parents, governors and pupils are involved in deciding and creating the policy, the more effective it will be.

It is recommended as best practice that all schools appoint an e-Safety Coordinator to lead on e-Safety. The person who is appointed does not need to have vast technical knowledge; however it would be helpful if they had some basic understanding of ICT.

The school's Designated Child Protection Coordinator (DCPC) will need to be aware of e-Safety training and resources and be available should any child wish to disclose information regarding an online incident. Therefore it may be an idea to elect them as e-Safety representative. However another member of staff may be selected. The DCPC must be made aware of any disclosures, incidents or Child Protection concerns. The Senior Leadership Team and Governing Body must be involved and should review the e-Safety policy annually and monitor its impact. They will also need to ensure that they take responsibility for revising the e-Safety policy and practice where necessary (such as after an incident or change in national legislation).

The Headteacher and Governing body have a legal responsibility to safeguard children and staff and this includes online activity.

Possible statements:

D The school has appointed an e–Safety Coordinator.
D The e–Safety Policy and its implementation will be reviewed annually.
- Our e–Safety Policy has been written by the school, building on the DCC e–Safety Policy and government guidance.
- Our School Policy has been agreed by the Senior Leadership Team and approved by governors and other stakeholders such as the PTA.
- The School has appointed a member of the Governing Body to take lead responsibility for e-Safety

The School e-Safety Coordinator is Carol Taylor

Policy approved by Head Teacher: Carol Taylor Date: June 2017

Policy approved by Governing Body: Stephen Wright.. (Chair of Governors)

Date: June 2017

The date for the next policy review is June 2020

1.2 Teaching and learning

1.2.1 Why is Internet use important?

Discussion:

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

Possible statements:

D Internet use is part of the statutory curriculum and is a necessary tool for learning.

D The Internet is a part of everyday life for education, business and social interaction.

D The school has a duty to provide students with quality Internet access as part of their learning experience.

D 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.

1.2.2 How does Internet use benefit education?

Discussion:

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Possible statements:

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- 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 KCC and DfE;
- access to learning wherever and whenever convenient.

1.2.3 How can Internet use enhance learning?

Discussion:

Increased computer numbers and improved Internet access may be provided but its impact on pupils learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be developed.

Possible statements:

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

D Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

D 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.

1.2.4 How will pupils learn how to evaluate Internet content?

Discussion:

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for pupils to develop skills in evaluating Internet content. For example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

Possible statements:

The following statements require adaptation according to the pupils' age:

D Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

D 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.

1.3 Managing Information Systems

1.3.1 How will information systems security be maintained?

Discussion:

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

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

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For DCC staff, flouting electronic use policy is 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:

- Central KPSN Schools Broadband firewalls and local CPEs are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between schools and KCC/EiS.

The Schools Broadband network is protected by a cluster of high performance firewalls. These industry leading appliances are monitored and maintained by a specialist security command centre.

Possible statements:

D The security of the school information systems and users will be reviewed regularly.

D Virus protection will be updated regularly.

- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not 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.
- The use of user logins and passwords to access the school network will be enforced.

1.3.2 How will email be managed?

Discussion:

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

Spam, phishing and virus attachments can make email dangerous.

Possible statements:

- **D** Pupils may only use approved email accounts for school purposes.
- **D** Pupils must immediately tell a designated member of staff if they receive offensive email.
- **D** Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- **D** Whole -class or group email addresses will be used in primary schools for communication outside of the school.
- **D** Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Schools will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

- Staff should not use personal email accounts during school hours or for professional purposes.

1.3.3 How will published content be managed?

Discussion:

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.

Possible statements:

D 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.

1.3.4 Can pupils' images or work be published?

Discussion:

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.

Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport style" photographs but still convey the educational activity. Personal photographs can be replaced with self portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed.

Images of a pupil should not be published without the parent's or carer's written permission. Some schools ask permission to publish images of work or appropriate personal photographs on entry, some once a year, others at the time of use.

Pupils also need to be taught the reasons for caution in publishing personal information and images online (see section 2.3.6).

.

Possible statements:

- **D** Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- **D** Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- **D** Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils work can only be published with their permission or the parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.

1.3.5 How will social networking, social media and personal publishing be managed?

Discussion:

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. 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.

Schools may wish to consider creating a separate social media policy to outline actions taken to reduce risk and to highlight the benefits of using social media.

Possible statements:

- **D** The school will control access to social media and social networking sites.
- **D** 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.
- **D** 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 safe and professional behaviour will be outlined in the school Acceptable Use Policy.

1.3.6 How will filtering be managed?

Discussion:

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

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

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit 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 DCC where appropriate.

Any material that the school believes is illegal must be reported to appropriate agencies such as Derbyshire Police or CEOP.

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.

Possible statements:

- **D** The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- **D** The school will work with DCC to ensure that filtering policy is continually reviewed.
- **D** 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.
- **D** 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.
- **D** The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- 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 Derbyshire Police or CEOP
- 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.

1.3.7 How will videoconferencing be managed?

Discussion:

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 ten regional schools' networks across England with the Welsh, Scottish and the Northern Ireland networks.

Schools with full broadband are connected through the KPSN and 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 which do not require KPSN systems. If Flashmeeting is used, conferences should always be booked as private and not made public. The conference URL should only be given to those who you wish to take part. Check who has signed into your conference; as a guest without a camera would not be visible.

Possible statements:

D 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.

Users

D Pupils will ask permission from a teacher before making or answering a videoconference call.

D Videoconferencing will be supervised appropriately for the pupils' age and ability.

D Parents and carers consent should be obtained prior to children taking part in videoconferences.

- 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.

1.3.8 How are emerging technologies managed?

Discussion:

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

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

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible.

Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

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

Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many 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.

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 school’s behaviour and/or anti-bullying policies.

Possible statements:

D 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.

1.3.9 How should personal data be protected?

Discussion:

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 (“the Act”) gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual’s rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

Possible statements:

D Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

1.4 Policy Decisions

1.4.1 How will Internet access be authorised?

Discussion:

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. Authorisation is generally on an individual basis in a secondary school. 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 annually when pupils' home details are checked and 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 school behaviour policy.

Possible statements:

- **D** The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- **D** All staff will read and sign the 'Staff Information Systems Code of Conduct' or School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitor 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.
- 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).

According to Setting Type

- **D** At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- **D** At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

1.4.2 How will risks be assessed?

Discussion:

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. It is wise to include a disclaimer, an example of which is given below.

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

Possible statements:

D 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 DCC can accept liability for the material accessed, or any consequences resulting from Internet use.

D 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.

- 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 Derbyshire Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

1.4.3 How will the school respond to any incidents of concern?

Discussion:

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However it is also important to consider the risks associated with the way these technologies can be used. An e-Safety Policy should recognise and seek 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 Child Protection Coordinator.

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 the Children Safeguard Team or e-Safety officer, if the offence is deemed to be out of the remit of the school to deal with.

Possible statements:

- 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 Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- 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, indentify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other schools in Derbyshire.

1.4.4 How will e–Safety complaints be handled?

Discussion:

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 Child Protection Coordinator or e–Safety Coordinator. Advice on dealing with illegal use can, when deemed necessary, be discussed with the Children's Safeguard Team.

Possible statements:

- **D** Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- **D** Any complaint about staff misuse will be referred to the head teacher.
- **D** All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.

- 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 Children's Safeguard Team 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.

1.4.5 How is the Internet used across the community?

Discussion:

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. Assistance from the community in drawing up the policy could be helpful.

Possible statements:

- 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.

1.4.6 How will Cyberbullying be managed?

Discussion:

Cyberbullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 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 mobiles 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 and 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
- gives headteachers 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”
http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tackling-bullying

DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

Possible Statements:

D 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 school’s policy on anti-bullying and behaviour.

D There are clear procedures in place to support anyone in the school community affected by cyberbullying.
D All incidents of cyberbullying reported to the school will be recorded.
D 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.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or 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 to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

1

1.4.8 How will mobile phones and personal devices be managed?

Discussion

Mobile phones and other personal devices such as Games Consoles, Tablets, PDAs and 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 accesses 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.

A policy which prohibits pupils from taking mobile phones to school could be considered to be unreasonable and unrealistic for schools to achieve. Many parents/carers would also be concerned for health and safety reasons if their child

were not allowed to carry a phone and many staff also use mobile phones to stay in touch with family.

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

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

Possible Statements

D The use of mobile phones and other personal devices by students in school is not allowed. Pupils can if given permission by the school be able to bring them to school- but must be kept in the school office during the school day.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone 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 device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

1.5 Communication Policy

1.5.1 How will the policy be introduced to pupils?

Discussion:

Many pupils are very familiar with 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.

e–Safety rules should be on display in every room with a computer to remind pupils of the e–Safety rules at the point of use.

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

Possible statements:

D All users will be informed that network and Internet use will be monitored.

D 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 and/or ICT programmes covering both safe school and home use.
- e–Safety training will be part of the transition programme across the Key Stages 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.
- 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.

1.5.2 How will the policy be discussed with staff?

Discussion:

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 DCC 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.

Possible statements:

D The e–Safety Policy will be formally provided to and discussed with all members of staff.

D To protect all staff and pupils, the school will implement Acceptable Use Policies.

D Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- 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.

1.5.3 How will parents' support be enlisted?

Discussion:

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).

Possible statements:

D Parents' attention will be drawn to the school e–Safety on the school website.

- A partnership approach to e-Safety at home and at school with parents will be encouraged.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it's implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents I 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 Contacts and References section".

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com