Dean Bank
Primary and Nursery School

e–Safety Policy

February 2018
February 2020
Why does a Dean Bank Primary and Nursery School 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.
Dean Bank Primary and Nursery School sees e-Safety as a whole school issue. As such, a holistic approach to writing and updating the school’s e-Safety Policy as well as embedding safe practice has been developed.

The e-Safety Policy is part of many different school’s policies including the Computing 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.

The Headteacher and Governing Body of Dean Bank Primary and Nursery School have a legal responsibility to safeguard children and staff and this includes online activity.

The Senior Leadership Team and Governing Body will review the e-Safety policy annually and monitor its impact and revise the e-Safety policy and practice where necessary (such as after an incident or change in national legislation).

The Designated Child Protection Coordinator (DCPC) will be aware of e-Safety training and resources and be available should any child wish to disclose information regarding an online incident. They must be made aware of any disclosures, incidents or Child Protection concerns.

- Governor with lead responsibility for e-Safety: Mr J Lindsay / Mr A Potts
- e-Safety Coordinators: Mrs P Northcott
- Mrs D Emmerson
- Designated Child Protection Co-ordinator: Mrs S Temple

Policy approved by Head Teacher:
Date:

Policy approved by Governing Body: (Chair of Governors)
Date:

The date for the next policy review is February 2020
Why is Internet use important?

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 computing and internet use.

- 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.
- Dean Bank Primary and Nursery 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.
How does Internet use benefit education?

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.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- 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 DCC and DfE;
- access to learning wherever and whenever convenient.
How can Internet use enhance learning?

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.

Dean Bank Primary and Nursery 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.

- Dean Bank Primary and Nursery School will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

- 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.
How will pupils learn how to evaluate Internet content?

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.

- 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.

- 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 be taught to use search engines appropriately for their age.

- 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.
Managing Information Systems

How will information systems security be maintained?

- The security of Dean Bank Primary and Nursery Schools information systems and users will be reviewed regularly.

- Virus protection will be updated regularly.

- Dean Bank Primary and Nursery School will comply with the terms of the data protection act, and is responsible for registering with the information commissioner's office.

- 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 Computing coordinator/network manager will review system capacity regularly.

- The use of user logins and passwords to access the school network will be enforced.
How will email be managed?

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.

However, the implications of email use for Dean Bank Primary and Nursery School and its pupils needs appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries.

- 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.
- 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 if necessary 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.
- 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.
How will published content be managed?

Dean Bank Primary and Nursery Schools has created excellent website and communication channels, which inspire pupils to publish work of a high standard. Our website celebrates pupils’ work, promotes our school and publishes resources for projects.

Publication of any information online is always to be considered from a personal and school security viewpoint:

- Contact details on the website are the school address, email and telephone number.

- Staff or pupils’ personal information must not be published.

- The head teacher has overall editorial responsibility for online content published by 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.

Can pupils’ images or work be published?

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.

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.

- Pupils’ full names will not be used anywhere on the website, particularly in association with photographs.

- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.

- Written consent will be kept by the school where pupils’ images are used for publicity purposes, until the image is no longer in use.
How will social networking, social media and personal publishing be managed?

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 are aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They have been 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.

- Dean Bank Primary and Nursery 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 will 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.
How will filtering be managed?

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.

Dean Bank Primary and Nursery School 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 and followed.

Internet Safety Rules are displayed, and both children and adults should be educated about the risks online. There is an Incident Log to report breaches of filtering or inappropriate content being accessed. Procedures will be established to report such incidents to parents and DCC.

Websites which Dean Bank Primary and Nursery School believe should be blocked centrally will be reported to the ICT 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.

- Dean Bank Primary and Nursery School’s broadband access will include filtering.
- A system is in place to make changes to the filter, including deciding who is responsible for authorising changes.
- Dean Bank Primary and Nursery School works with DCC to review filtering.
- A clear procedure for reporting breaches of filtering is in place. All members of the school community (all staff and all pupils) are 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 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.

• 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, Durham Police or CEOP
How will videoconferencing be managed?

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. Systems include complex standalone equipment and software based systems such as Skype.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- 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.
- 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
  1. Pupils will ask permission from a teacher before making or answering a videoconference call.
  2. Videoconferencing will be supervised appropriately for the pupils’ age and ability.
  3. Parents and carers consent should be obtained prior to children taking part in videoconferences.
  4. Only key administrators should be given access to videoconferencing administration areas or remote control pages.
  5. Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

- Content
  a. 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.
  b. Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
  c. If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
  d. 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.
How are emerging technologies managed?

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.

- 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.
How should personal data be protected?

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.

At Dean Bank Primary and Nursery School personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
Policy Decisions

How will Internet access be authorised?

- All staff will read and sign the 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 visitors to school site who require access to the school’s 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) Dean Bank Primary and Nursery School will make decisions based on the specific needs and understanding of the pupil(s).

How will risks be assessed?

Dean Bank Primary and Nursery 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.

- 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 Durham Police.

- Use methods to identify, assess and minimise risks and these will be reviewed regularly.
How will Dean Bank Primary and Nursery School respond to any incidents of concern?

- 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, identify lessons learnt and implement any changes required.

- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the 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 Durham.
How will e-Safety complaints be handled?

- 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, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with 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 Safer Schools Partnership Coordinators and/or Children’s Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to 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.
How is the Internet used across the community?

Dean Bank Primary and Nursery School will:

- Liaise with local organisations to establish a common approach to e-Safety.
- Will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- Will provide an AUP for any guest who needs to access the school computer system or internet on site.

How will Cyberbullying be managed?

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.

- 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 policy on anti-bullying and behaviour.
• 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.

• Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

• Steps will be taken 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.
How will Learning Platforms be managed?

- SLT and staff will regularly monitor the usage of the LP 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 LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- 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 LP 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 LP for the user may be suspended.

d. The user will need to discuss the issues with a member of SLT before reinstatement.

e. A pupil’s parent/carer may be informed.

- A visitor may be invited onto the LP 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.
How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by students and staff in school will be decided and covered in the school Acceptable Use or Mobile Phone Policies.

- 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 they believe it is being used to contravene the behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

- Mobile phones and personal devices will not be used during lessons or formal school time. 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. Dean Bank Primary and Nursery School accepts no responsibility for the loss, theft or damage of such items. Nor will Dean Bank Primary and Nursery School accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.
Use of Personal Devices

- If a pupil is found to have a mobile phone in school it will be removed and placed in the school office for collection at home time.

- 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.

- 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.
Communication Policy

How will the policy be introduced to pupils?

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

- An e-Safety training programme will be established across Dean Bank Primary and Nursery 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 Computing programmes covering both safe school and home use.

- e-Safety training will be part of the transition programme across the Key Stages.

- 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.

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
How will the policy be discussed with staff?

- 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.

- 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.
How will parents’ support be enlisted?

- Parents’ attention will be drawn to Dean Bank Primary and Nursery Schools 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 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 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
Durham EDS – E-safety, Teaching and learning advice Tel: 0191 3834370
Durham Safeguarding Children Board (DLSCB): www.durham-lscb.gov.uk
ICT Service Desk – Changes to filtering Tel: 03000 261100
ICTSS Service Desk – All other ICT issues Tel: 01388 424999
Internet Watch Foundation (IWF): www.iwf.org.uk
Kidsmart: www.kidsmart.org.uk
Schools e–Safety Blog: www.kentrustweb.org.uk?esafetyblog
Teach Today: http://en.teachtoday.eu
Think U Know website: www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com
The role of the e-Safety Lead/Coordinator in Education Settings

Dean Bank Primary and Nursery has appointed an e-Safety lead, who is responsible for co-ordinating the whole school/setting e-Safety approaches, supporting and raising awareness with the wider community, promoting a safe and responsible e-Safety culture and acting as the lead for dealing with e-Safety issues that arise.

Key Tasks of the e-Safety Lead/Coordinator:

- Developing an e-Safe culture throughout the setting as part of safeguarding, which is in line with national best practice recommendations (e.g. Ofsted, DfE)

- Ensuring that e-Safety is clearly identified and established as part of the roles and responsibility of the management/senior leadership team and governing body etc.

- Acting as a named point of contact on all e-Safety issues and liaising with other members of staff as appropriate.

- Auditing and evaluating current practice to identify strengths and areas for improvement (Kent Self evaluation tool and 360 safe)

- Keeping up-to-date with current research, legislation and trends. This may include accessing appropriate training and using a range of approaches to enable them to understand the role of new technology as part of modern British society and the wider safeguarding agenda.

- Leading an e-Safety team with input from all stakeholder groups when necessary

- Embedding e-Safety in staff training and CPD by ensuring that all members of staff receive up-to-date and appropriate e-Safety training (at least annually and as part of induction) which sets out clear boundaries for safe and professional online conduct.
• Ensuring that there is an age and ability appropriate e-Safety curriculum that is embedded, progressive, flexible and relevant which engages children’s interest and promotes their ability to use technology responsibly and to keep themselves and others safe online.

• Ensuring that the setting participates in local and national events to promote positive online behaviour, e.g. Safer Internet Day.

• Ensuring that e-Safety is promoted to parents and carers and the wider community through a variety of channels and approaches.

• Ensuring there are robust reporting channels for the community to access regarding e-Safety concerns, including internal, local and national support.

• To ensure that age-appropriate filtering is in place, which is actively monitored.

• Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

• Work with the lead for data protection and data security to ensure that practice is in line with legislation.

• Maintaining an e-Safety incident/action log to record incidents and actions taken.

• Liaising with the local authority and other local and national bodies as appropriate.

• Reviewing and updating e-Safety policies, Acceptable Use Policies and other procedures on a regular basis (at least annually) with stakeholder input and ensuring that e-Safety is integrated with other appropriate school policies and procedures.

• Monitoring and reporting on e-Safety issues to the school management team, Governing Body and other agencies as appropriate.
## E-Safety Incident Record

<table>
<thead>
<tr>
<th>E-safety incident</th>
<th>Outline :</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of member of staff (Discovering the incident)</td>
<td>Date</td>
</tr>
<tr>
<td>Child(ren) involved. (or other adults if no children involved)</td>
<td>Time</td>
</tr>
<tr>
<td>Device(s), Websites, Usernames..</td>
<td>Note:- If there is a possibility of legal action the device should be disconnected and powered down. Do not investigate device as this will damage / remove any evidence. Obtain Police advice.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nature of incident</th>
<th>Accidental access to inappropriate material</th>
<th>Intentional access to inappropriate material</th>
<th>Creating / Distributing inappropriate Images</th>
<th>Cyber Bullying</th>
<th>Grooming</th>
<th>Other</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Details</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>The event occurred</th>
<th>During a lesson</th>
<th>In unsupervised time</th>
<th>Outside school hours</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Does the even warrant direct Police involvement (Yes if...)</th>
<th>Grooming</th>
<th>Violent image(s)</th>
<th>Pornographic image(s)</th>
<th>Illegal Images</th>
<th>Blackmail</th>
<th>Other criminal activity</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Police Involvement</th>
<th>Yes/No</th>
<th>Date &amp; Time</th>
<th>Contact</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>LADO Involvement</th>
<th>Yes/No</th>
<th>Date &amp; Time</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head Teacher/Deputy Head / Safeguarding Contact</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>(Staff)</strong></td>
<td>Contact made with SGSS / Personnel</td>
<td>Recommended action</td>
<td>Action applied</td>
</tr>
<tr>
<td>Other Children</td>
<td>Contacted Parents (names)</td>
<td>Date</td>
<td>Time</td>
</tr>
<tr>
<td>Interviewed Parents/Carers</td>
<td>Other Interviews</td>
<td>Append notes of interviews</td>
<td></td>
</tr>
<tr>
<td>Potential Technical Changes</td>
<td></td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Potential Teaching Changes</td>
<td></td>
<td>Completed</td>
<td></td>
</tr>
</tbody>
</table>