Devonshire Park Primary School e-safety policy

The acceptable use of the internet and related technologies

Contents

Appendices

Our e-safety policy

The e-Safety Policy relates to other policies including those for Computing, email use, anti-bullying and for safeguarding and child protection.

The school's e-Safety Coordinator is the Headteacher, Mrs J Billinge along with the Deputy Headteacher, Miss Sullivan and Computing subject leader, Mr S Dutton.

Our e-Safety Policy has been written by the Computing subject leader, Mr S Dutton building on the Kent e-Safety Policy whilst reviewing guidance from BECTA (no longer a government agency), e-safety support policy documents and the Department for Education.

Introduction to e-Safety

1.1   e-Safety in a Changing World

The term e-Safety covers the issues relating to young people and staff and their safe use of the Internet, mobile phones and other electronic communication technologies. This policy assesses the protocols for ensuring that these initiatives are carefully developed in our school, so that we progress responsibly and appropriately in the interests of our children. It also looks at how we educate our children to be safe in a world where technology is so readily available.

At Devonshire Park Primary we celebrate the value and importance of technology in our children's learning; desktop computers, wireless laptops, iPads, learnpads, digital voice recorders, camcorders and digital cameras can all be part of children's every day learning. The Internet has become a vital source of learning and communication for all members of our school community; the exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger. Our school seeks to provide the right balance between controlling access, setting rules and educating students for responsible use.

1.2   Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:
   • Education for responsible computing use by staff and pupils;
   • A comprehensive, agreed and implemented e-Safety Policy;
   • A well thought out curriculum to develop e-Safety guidance within the school (see also Computing policy and curriculum).
   • Identified opportunities to ensure that we support families with the challenges relating to e-Safety in the digital age (family workshops, web-links etc).
   • Secure, filtered broadband from Wirral Council's Network and monitored by e-Safe;
   • A school network that complies with the National Education Network standards and specifications.

1.3   E-Safety and the Legal Issues

E-safety should be applied to protect children, staff and all members of our school community. Our school's e-Safety Policy replaces the Internet Policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day. Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere (see also appropriate Safeguarding policies). Pupils must also learn that publishing personal information could compromise their security and that of others.

Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is a criminal offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to 'groom' children. In addition there are many grey areas for schools to consider regarding communication of social network sites, storage of data etc.

Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

In practice this means that this school ensures that;

- It has effective firewalls and filters on our school network – provided by Hi-Impact.

- Ensures that e-Safety responsibilities are clearly communicated to all members of our school community.

- That our Acceptable Use Policies are fully enforced for pupils, staff and visitors.

- Ensures that our procedures are consistent with the Data Protection Act (1998).

- Additional monitoring of keystrokes is in place through use of e-Safe.

Learning and Teaching in the Digital Age

The school uses desktop computers, wireless laptops, iPads and comprehensive broadband access to develop learning and teaching through digital communication. Access to instant messenger services and mobile phones is not allowed as part of this school's curriculum. However, the school will include provision to educate children how to use this technology appropriately and safely.

2.1 Why the Internet and digital communications are important

The purpose of Internet use in school is to raise educational standards, to promote learner achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Mobile Communication equipment and the Internet are an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. We also recognise that children are actively engaged with digital communication form an early age. It is part of their lifelong learning experiences and habits. This generation are sometimes referred to as 'digital natives'. We have to embrace that opportunity. However, we also have a responsibility to ensure that our children learn to use these opportunities and resources responsibly, appropriately and productively to enhance their learning.

In addition use of the Internet is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2   Encouraging responsible use of the Internet and digital communication.

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. This is arranged through local authority provision and the school's network arrangements. Only sites approved by the Headteacher will be allowed to override the filter.

- Pupils will be taught about responsible and appropriate information sharing through the internet and other forms of digital communication (see also Behaviour policy).

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

- Pupils will be taught about using an age appropriate search engine

- Pupils will be taught about responsible use of e-mails and other sources of digital communication including e-mail, messenger services and texts (see also Anti-Bullying policy).

- 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 shown how to publish and present information to a wider audience safely and responsibly.

- All staff, parents and pupils must read and agree to comply with the Acceptable Use Policy Agreement (Appendix 1).

- The Computing subject leader will keep a log of all user account names and passwords. Currently all children in KS1 have individual password protected logon accounts with group folders and class work to be stored; KS2 have

individual password protected logon accounts with individual folders for work to be stored; FS have a number of class logons with group folders produced for class work to be stored.

2.3   Pupils will be taught how to evaluate Internet and other digital communication content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law and avoids plagiarism.

- Pupils will be taught the importance of cross-checking information before accepting its accuracy, including finding any fake news.

- Pupils will be taught how to report unpleasant Internet or other digital content including messages, e-mails and texts. Whilst we cannot promote the use of social networking sites, we must also ensure that our children know how to manage the risks and dangers associated with these activities.

- Staff are trained in recognising indicators of vulnerability to radicalisation e.g. accessing violent extremist websites and are aware of reporting procedures into the Channel process. Filtering ensures that such sites cannot be accessed in school.

- The school's Internet access is provided by Exa Networks as an approved Internet Service Provider.

- If staff or Pupils do discover unsuitable sites, the URL (address), time, content must be reported to the Headteacher, Deputy Headteacher or Computing subject leader and recorded in the e-Safety log (Appendix 11).

Managing Digital Access, Communication and Content

All Internet access is managed by the school. Individual users should only access the Internet through their username and password. The school recognises that password protection is a vital element of promoting e-Safety. The school will ensure that permission for access and use of any content including photographs and video is fully explained and sought on admission to the school (with additional permission if necessary, see appendices 3, 4 and 5).

3.1   Information system security

- School ICT systems security will be reviewed regularly. This will be part of the liaison between the Headteacher and Hi-Impact.

- Virus protection will be updated regularly as part of the school's Service Level Agreement with Hi-Impact.

- Security strategies will be discussed with Hi-Impact.

- e-Safe systems tool is active and reports will be used to monitor e-Safety, cyberbullying and inappropriate computing use on the school network.

- Incorrect use of any computing devices will be monitored by Hi Impact and class teachers. The Headteacher will then follow the Safeguarding policies, Pathways to Help (see Anti-Bullying policy), Concerns & Complaints policy or take action as necessary (see Appendix 2 Responding to Incidents) depending on the nature of any incidents (see sections 4.5 and 4.5 for handling e-Safety complaints and reporting e-Safety incidents).

3.2   Managing filtering
- The school will work with Hi-Impact and other National Bodies to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Computing subject leader, Mr S Dutton who will alert the Headteacher, Mrs J Billinge or directly to the Headteacher.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.3 E-mail

- Pupils may only use school approved e-mail accounts on the school system (Pupils do not have access to individual accounts but school does have a communal gmail account used primarily for transferring work from the iPads via Dropbox and Google maps). All use of other e-mail accounts are prohibited.

- Staff should only use school approved e-mail accounts at work. Clear guidance for what constitutes professional use of e-mail is included in the Acceptable Use agreements. However, we are absolutely clear that staff cannot use e-mail to communicate personal opinions that may be defamatory or abusive to individuals or organizations associated with the school.

- Pupils must immediately tell a teacher if they receive offensive e-mail and the Pathways of Help will then be followed by the member of staff (see Anti-Bullying, Behaviour and Safeguarding policies for further guidance).

- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission (as covered in Computing curriculum).

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- E-mail sent to external organisations by pupils or staff should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

- The forwarding of chain letters is not permitted.

3.4 Published content and the school website

- Staff or pupil personal contact information will not be published. The contact details given online are the school office (all staff use the same footnote on their emails as recommended by Hi-Impact).

- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.5 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully. The school will always risk assess/review photographs for possible abuse.

- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.

- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website. A list of children who should not be used on the website, along with their photographs is available to all staff and updated regularly.

- Pupil image file names will not refer to the pupil by name.

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. It will only be published with permission of the pupil (and parent where appropriate).

3.6 Social networking and personal publishing (see Social Networking policy and appendix 6a and 6b for further guidance)

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. The school will use BBC, CEOP and fotobabble secure websites to teach children about social interaction and communication on the Internet. This will be carefully managed and always have an educational purpose.

- Newsgroups will be blocked unless a specific use is approved.

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

- Parents sign the AUP to state they will not publish pictures on social media unless it is solely their child in the image. They also agree to use the proper Concerns & Complaints procedure, refraining from posting any grievances or concerns on social media sites, as this could be potentially damaging to the school and pupils.

- Pupils are taught about appropriate use of social networking, including how to deal with cases of cyberbullying and how to report any problems; Anti-Bullying Ambassadors will be involved as part of the curriculum.

- Pupils are encouraged to ensure they meet the minimum age for websites before signing up for them.

- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

- Pupils will be encouraged to invite known friends only and deny access to others.

- All staff are aware that they could face charges of gross misconduct if they use social networking platforms to communicate personal opinions that may be defamatory or abusive to individuals or organizations associated with the school.

- Staff know they must not show the school badge (particularly on jackets or lanyards) on their personal social media sites or accounts. They must also ensure that they are not identifying themselves as employees of the school on their personal webspace/profiles.

- Staff are also aware that they are responsible for the security protocols regarding any social networking accounts. This is a professional responsibility.

- Staff are fully informed of their responsibilities regarding the use of social networking sites such as Facebook. At Devonshire Park we have agreed that it is good practice to separate professional and personal commitments. Therefore the following groups should not be allowed as contacts and friends on social networking sites;

  - **Ex pupils or current pupils** - the context of teacher to pupil relationship is not suitable for social networking.
  - **Parents** - We believe that it is unfair on parents and staff to complicate the professional relationship that exists within school through the use of social networking sites. It is both inappropriate and open to abuse.

- Additional information for staff from NUT, NASUWT and ATL can be found in appendix 6b.

This guidance is applied through the Local Authority's policy on the agreed use of social networking sites, the school's acceptable use and e-Safety code of conduct. All staff and visitors including students have to sign these when they join our staff team (see appendices 1 and 6a).

3.7 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security. Video conferencing for pupils can only take place under the direct supervision of a member of staff. School would always seek consent from parents for any video-conferencing (See appendix 4).

- At Devonshire Park we will only use webcams for specific projects and full consent will be sought before children participate in these. Examples may be conferencing with a school in another country.

- All software for webcam use will be password protected (Skype etc).

3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the Health & Safety/ Child Protection and safeguarding officer and agreed by the governing body before use in school is allowed.

- Staff are allowed to have mobile devices in school but these must not be used during working hours except for school or emergency based communication. In these circumstances staff **should not** be using mobile devices **in the lesson or in sight of pupils** (see mobile phone policy).

- The senior leadership team should note that technologies such as mobile devices with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden – if there are any incidents the Pathways of Help (Behaviour and AntiBullying policies) or Responding to incidents (appendix 2) will be followed as appropriate.

- Pupils will be taught in the Upper Key Stage 2 curriculum about 'sexting' and the consequences this type of behaviour may have.

- Pupils are not to bring in personal mobile phones, own devices or Smart watches – if they do they must be handed into the Office for secure handling and can be collected at 3:15pm. The use by pupils of cameras in mobile devices is not allowed (see Mobile Phone policy for additional guidance).

- Handheld gaming consoles are not to be brought into school by pupils.

- Staff will be issued with a school mobile phone where contact with pupils is required or school camera/iPad to capture photographs of pupils. Staff **MUST NOT** take photographs on their personal phones under any circumstances (see Mobile Phone and Safeguarding policies for additional guidance).

3.9   Protecting and storing sensitive data including images

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. This information will be clearly communicated to all staff, including office staff on an annual basis.

Staff are aware that they have a professional responsibility to ensure the following;
- All laptops must be password protected with a complex password. Work laptops cannot be used for the storage of any inappropriate material.
- Photographs in Dropbox should only be accessed in school with a complex password. They should be moved into the school media storage folder and deleted from the device also.
- All data and images of children must be stored in the staff shared area on the curriculum network or the school's secure administration network.
- Photographs cannot be stored on personal laptops.
- Photographs must be deleted when no longer required.
- No data or images can be transported out of the school without the device being encrypted or password protected with a complex password.
- No photographs will be taken, even for the Twitter feed, on personal devices.

3.10 Use of Photographs and images (additional guidance can be found in appendix 3)

The Data Protection Act 1998 affects our use of photography. This is because an image of a child is personal data for the purpose of the Act and it is a requirement that consent is obtained from the parent of a child or young person under the age of 18 years (or the child him or herself if deemed competent from 12 years old as suggested by the Information Commissioner) for any photographs or video recordings for purposes beyond the school's core educational function (e.g. school web sites, school productions). At Devonshire Park we seek permission for all photography and video use.

There will also be times where the school will be carrying out off-site activities e.g. activity holidays or educational visits. Our guidelines are created to make sure that all images are taken appropriately by both adults in the school and children taking part in visits. Again personal devices will not be used to take these images.

For both school and other events which are photographed for publicity purposes additional consent should be sought from the child's parent/guardian and kept on file covering all cases where images of children are to be published beyond the parameters of school use.

Where children are 'Looked After' school must check consent on the corporate parent's behalf with the social worker and there may be other situations, (in adoption placements or following a resettlement from domestic violence for example), where a child's security is known by the class teacher to be at stake, indicating the need for extra care (see Safeguarding policies).

Consent is sought for the whole time that children are at Devonshire Park. Parents retain the right to withdraw consent at any stage, but they need to do so in writing.

Consent gained for photographs or videos does not extend to webcam use, so it is important to, when introducing such technology, to ask for additional consent for pupils.

Developing Our Policies on e-Safety

4.1 Authorising Internet access

- All staff must read and sign the 'Acceptable User Policy' (see appendix 1) before using any school ICT resource.

- All staff and pupils are granted access to school ICT systems unless there has been a concern over appropriate use when they might have their privileges removed.

- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

- All Parents/Carers will be asked to sign and return a consent form.

- Any person not directly employed by the school will be asked to sign an 'Acceptable User Policy' (see appendix 1) before being allowed to access the internet from the school site. This includes governors, visitors, student teachers etc.

4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor LA can accept liability for any material accessed, or any consequences of Internet access.

- 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 and effective every 12 months. If issues are highlighted then the policy will be updated as necessary.

4.3   Cyber Abuse/Bullying Abuse/Bullying using Cybertechnology

Cyber abuse/bullying may consist of threats, harassment, embarrassment, humiliation, defamation or impersonation. It may take the form of general insults, or prejudice based abuse e.g. homophobic, sexist, racist or other forms of discrimination. It may involve e-mail, virtual learning environments, chatrooms, websites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

Abuse using technology can occur at any time and incidents can intrude into the victim's private life. The audience for such messages can be very large and can be reached rapidly. The content of electronically forwarded messages is hard to control and the worry of content resurfacing can make it difficult for the victim to move on.

Staff in schools can become targets of cyber abuse/bullying and, like other forms of bullying, it can have significant impact on their health, well-being and self-confidence. Protecting staff from abuse is best done within a prevention framework, including whole school policies and appropriate practices. We at Devonshire Park operate a zero tolerance policy towards direct or indirect harassment or assault against any member of staff, volunteers and governors. This includes the use of social media and other forms of electronic communications to facilitate the act.

Cyberbullying and the Law
While there is not a specific criminal offence called cyberbullying, activities can be criminal offences under a range of different laws, including:

- The Protection from Harassment Act 1997
- The Malicious Communications Act 1988
- Section 127 of the Communications Act 2003
- Public Order Act 1986
- The Defamation Acts 1952 and 1996

It is the duty of every employer to ensure, so far as reasonably practicable, the health, safety and welfare at work of all employees. Incidents that are related to

employment, even those taking place outside the hours or place of work may fall under the responsibility of the employer.

4.4   Handling e-Safety complaints (see also appendix 2 Responding to Incidents and the Anti-Bullying policy)

- Complaints of Internet misuse will be dealt with by a senior member of staff, the safeguarding officer or Headteacher.

- Any complaint about staff misuse must be referred to the Headteacher.

- Complaints of Cyberbullying will be dealt with by the Headteacher following the Pathways for Help (Anti-Bullying policy).

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures by the Headteacher or Deputy Head.

- Pupils and parents will be informed of the complaints procedure (see Concerns & Complaints policy) and will be informed of consequences for pupils misusing the Internet.

- Discussions will be held with the Police Youth Crime Officer to establish procedures for handling potentially illegal issues.

4.5   Reporting e-Safety incidents

- Pupils are made aware that they can report any e-safety concerns relating to illegal content of a child, e.g. an indecent image of a child, directly to the Child Exploitation and Online Protection Centre (CEOP) via the report button.

- Pupils are made aware of the procedures that would follow an incident report so they know what to expect.

- An open-door policy is encouraged throughout the school so that pupils know there will always be someone there to listen to their concerns.

How to respond to an incident:

Incidents should be reported to the school's e-safety coordinator, or equivalent member of staff, who can assess the severity of the report in order to determine what course of action needs to be taken.

If it is considered that the pupil involved faces an immediate risk due to the incident, schools are advised to:
- Collect all of the relevant and available evidence.
- Inform child protection services.
- Allow any external agencies, e.g. child protection services or the police, to complete their investigation and take any necessary steps once it has concluded.

If the incident is illegal but does not pose an immediate risk to the child involved, schools should collect all of the available evidence and either encourage the pupil to report the incident using the CEOP form, or help the pupil to use the CEOP form. If a report is made, schools should await a response and act accordingly once this has been received.

If a reported e-safety incident is not illegal, e.g. cyber bullying, procedures should still be followed to ensure that the pupil is assured that their report is being taken seriously. It may be appropriate to follow school's Pathways of Help or other Safeguarding procedures. Depending on the nature and severity of the incident, it might be appropriate to take some of the following actions:
- Block reported webpages
- Notify the parents of the pupil who has reported an incident or, in cases where a pupil is making a report against another pupil, inform the parents of the alleged perpetrator ⬛ Provide any necessary disciplinary action

No matter the severity of the incident that has been reported, schools should continue to monitor the situation even after it has reached a conclusion – this is especially important in cases of cyber bullying where inappropriate behaviour may continue.

Following an e-Safety incident

Following an e-safety incident, it is important to record all of the procedures that were followed to ensure they comply with the school's E-safety Policy, and to see if any additional and effective steps were taken to deal with the incident that could be added to the e-Safety Policy during the next policy review. Information about e-safety incidents and how they were reported and dealt with may also be used in supporting staff training.

4.6   Community use of the network and Internet

- Through extended schools use and partnership with other organisations there will be wider community use of the school's network. The school will liaise with local organisations to establish a common approach to e-Safety.

- All consent forms must be used for these groups.

Communicating our e-Safety Policy

5.1   Introducing the e-Safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

- A programme of training in e-Safety for pupils has been developed, based on the materials from Arial Trust, CEOP, and Childline.

- E-Safety training is embedded within the Computing scheme of work and the Personal Social and Health Education (PSHE) curriculum. Staff training is given annually and termly updates also sent out via email.

- Pupils will be informed that Internet use will be monitored by e-Safe systems and weekly reports will be sent to the Headteacher.

5.2 Staff and the e-Safety policy

- All staff will be given the school e-Safety Policy and its importance explained.

- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

- Staff will always use a child friendly safe search engine when accessing the web with pupils. They will not search for images or documents on the web through any apps on the iPads.

- Hi-Impact will manage filtering systems and e-Safe systems will monitor Computing use for all staff which will be reported to the Headteacher on a weekly basis.

5.3 Enlisting parents' and carers' support

- Parents and carers' attention will be drawn to the school e-Safety Policy in newsletters and on the school Website. Important updates are sent out as additional letters to highlight the importance to parents.

- The school will maintain a list of e-Safety resources for parents/carers which can be accessed on the school Website.

- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

5.4   Visitors

- Visitors to school will be informed about the e-Safety policy in classrooms and as appropriate by a member of staff.

- All visitors must work within the e-Safety Policy - available in the School Office.

Appendix 1:

Devonshire Park Primary School – Acceptable use policy

For all staff, governors and external contractors accessing the school network on site or remotely.

Devonshire Park Primary School promotes the positive use of technology in school and assists in developing pupils' knowledge and understanding of digital devices and the Internet. We ensure that our school IT network is robust and resilient and staff have a duty of care to safeguard pupils when using technology in school. Any misuse of technology by a pupil or member of staff must be reported to the Designated Safeguarding Officer, so an investigation can take place.

This is the Acceptable User Policy (AUP) for our school. It highlights appropriate and inappropriate use of all technology in school and shows how we want staff to behaviour when using IT. The AUP covers the following legislation:

- Malicious Communications Act
- 1988 Data Protection Act 1998
- Computer Misuse Act 1990
- Communications Act 2003
- Sexual Offences Act 2003

Please read carefully and sign at the bottom to show you agree to these terms.

Using Technology in School

- I will only use school IT systems, external logins and email for school related purposes. Other use will be with the permission of a SLT teacher.
- I will monitor the use of all IT in school and report any inappropriate use by pupils or staff to the Designated Safeguarding Officer (DSO).
- I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, extremist, defamatory or copyright infringing.

Security, Passwords & Copyright

- I will not divulge any school related passwords and I will comply with school IT security procedures.
- I will use school email systems for school related communications. I will not use personal accounts for school business.
- I will ensure that personal data is stored securely and in line with the Data Protection Act. I will follow school policy with regard to external logins, encrypted data and not storing school material on personal IT equipment unless stated otherwise.
- I will not install software onto the network or mobile devices unless supervised by the Network Manager or IT support staff.

Social Media

- I must maintain my professionalism at all times when using personal social media and not bring the school or my profession into disrepute by posting unsuitable comments or media when using these sites.
- I must not use social media tools to communicate with current or former pupils, particularly those under the age of 18.
- I will only use authorised school social media accounts to post information to pupils or parents.
- I will ensure there is no means of identifying my employer on my social media profile (place of work or school badges visible).

Mobile Technologies

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode when I have directed time with pupils. I will only make or receive calls in specific places e.g. staffroom, office.
- I will not contact any parents or pupils on my personally-owned device.
- I will NOT use a personally-owned mobile device to take images, video or sound recordings for ANY purpose.
- I will ensure that all school data on devices is password protected and that I have agreed for the IT support staff to erase and wipe data off my device, if it is lost and/or as part of my exit strategy.

Online Professionalism

- I am aware that all network and Internet activity is logged and monitored and that the logs are available to SLT in the event of allegations of misconduct.
- I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of pupils, parents or staff on social media or websites in any way which might bring the school into disrepute.
- I will make sure that my Internet presence does not bring the teaching profession into disrepute and that I behave online in line with the Teacher Standards (2012) and other guidelines from the D of E.
- I will champion the school's e-safety policy and be a role model for positive and responsible behaviour on the school network and the Internet.
- I will not give my home address, phone number, mobile number, personal social networking details or email address to pupils. All communication with parents should be done by authorised school contact channels.
- Photographs of staff, pupils and any other members of the school community will not be used outside of the internal school IT network unless written permission has been granted by the subject of the photograph or their parent/carer. I will ask the permission of the Head Teacher (on site) or the proprietor of the building (off site) prior to taking any photographs.

Signed:_____

Name: _____

Date: _____

Devonshire Park Primary School
Acceptable User Policy

Pupils and Parents/Carers

Devonshire Park Primary School promotes the use of technology as all pupils will need these skills and knowledge in whatever field of work they enter when they become an adult. We ensure that our school IT network is robust and resilient and we do our upmost to ensure the safety of children when using it. It is important that pupils abide by the school rules when using technology in school and inform a member of staff immediately, if they become aware of any misuse.

This is the Acceptable User Policy (AUP) for our school. It highlights appropriate and inappropriate behaviour when using all technology in school and shows how we want pupils to behave when using IT. Any misuse will result in pupils being temporarily banned from using the school network.

Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form your child will not be able to have full access to the IT systems in school.

For Pupils:

Using Technology in School

- I will only use the school Internet and network for my school work or when a teacher has given permission.
- I will not try and bypass the schools Internet settings.
- I will only use a given email address when using email in school. I will always log off my email account when finished
- I will not look at, change or delete other people's work or files.
- I will be careful with all IT equipment such as keyboards, mice, headphones and when turning a computer on or off.
- I will be sensible when using mobile technologies and follow the rules about moving about the school when using them.

- I will follow the rules about bringing my own personal device into school e.g. smartphone, smartwatch.

Security, Passwords & Copyright

- I will not share my username or passwords. My password will use both letters and numbers.
- I will be careful when opening emails from people I don't know and I will ask an adult if I'm unsure whether to open it.
- I won't upload or download any pictures, writing or movies which might upset people or make other people think the school is a bad place.
- I will use non-copyrighted images and music from the Internet when creating documents, presentations or other media.
- I won't try to install software onto the school network because it might have a virus on and cause a lot of damage. Instead I will ask a teacher for advice.

Online Behaviour & Safety

- I won't give out my personal details, such as my name, age, address, school name or phone number on the Internet or when registering for a software app.
- I won't meet people I've met on the Internet unless I have told my parents and they come with me.
- I will make sure all my contact with other people at school is responsible. I will not cyber bully pupils, teachers or other members of staff.
- I won't look for or look at unpleasant or inappropriate web sites or software apps. I will check with a teacher if I think it might be unsuitable.
- I know that everything I do on the computers at school is recorded and that the school can talk to my parents if a teacher is worried about my online safety.
- I will try to follow these rules all the time because I know they are designed to keep me safe.

Signed - Pupil: _____

Pupil name: _____

Class: _____

For Parents/Carers:

- I agree to support and uphold the principles of this policy in relation to my child and their use of technology and the Internet, at home and at school.
- I agree to uphold the principles of this policy in relation to my own use of the Internet, when that use is related to the school, employees of the school and other students at the school.
- I will not use social media to make complaints or derogatory comments about the school. If I have a complaint I will follow the correct complaints procedure (see Concerns & Complaints Policy).
- Images of pupils will only be taken, stored and used for personal memories or school purposes in line with school policy. Images will only be used on the Internet, in the press, or in media, with specific written permission from the parent/carer of every pupil on the photograph.

Signed - Parent / carer: _____

Parent/carer name: _____

Date: _____

Appendix 2 – **Responding to Complaints**

If you are aware of an issue of any kind of technological device or site you must inform the Headteacher at the earliest opportunity, in order for it to be appropriately dealt with in a reasonable timescale.

When an issue is flagged to the Headteacher (against a pupil, parent or member of staff) then the Headteacher will respond in the most suitable way. This may be following the Pathways of Help if the incident is of a bullying issue toward a pupil (see Anti-Bullying policy). However, if it is of a more serious nature the following points need to be considered and appropriate actions taken.

- Where the perpetrator is known (a current pupil, parent or co-worker) this should be dealt with through the schools own behaviour management/disciplinary procedures.

- Keep any records of abuse – texts, emails, voicemails or instant messages. Take screen prints of messages or webpages. Record the time, date and address of the site.

- Staff should never retaliate i.e. personally engage with cyberbullying incidents.

- Monitoring and confiscation must be appropriate and proportionate – parents, employees and pupils should be made aware in advance of any monitoring to be implemented or the circumstances under which confiscation might take place.

- A designated member of the leadership team should contact the police where it appears that a law has been broken – for example where death threats, assaults or racially motivated criminal offences are involved. Where a potential criminal offence has been identified, the school should ensure that any internal investigation does not interfere with police enquiries. School staff are of course able to report incidents directly to the police.

- If a potential criminal offence has been committed and the school is not able to identify the perpetrator, the police may issue a Regulation of Investigatory Powers Act 2000 (RIPA) request to a service provider, enabling them to disclose the data about a message or the person sending it.

Getting Offensive Content Taken Down

Where online content is upsetting/inappropriate and the person(s) responsible for posting is known, the quickest way to get material taken down is likely to be to ensure that the person who posted it understands why the material is unacceptable and to request that they remove it. In this instance the appropriate policy and procedure will be taken but would always begin with a formal meeting with the headteacher.

If the person responsible has not been identified, or will not take the material down, the school will need to contact the host (i.e. the social networking site) to make a request to get the content taken down. The material posted may breach the service provider's terms and conditions of use and can then be removed.

It is important to be clear about where the content is – for example by taking a screenshot of the material that includes the URL or web address. If you are requesting they take down material that is not illegal, be clear about how it contravenes the site's terms and conditions.

In cases of actual/suspected illegal contact, the school should contact the police.

Appendix 3

Further Guidance on Photographing Children

3a Planning photographs of children

Images and details of pupils published together allow for the remote possibility that people outside the school could identify and then attempt to contact pupils directly. The measures described below should help to minimise the risk of such unsolicited attention.

• Where possible, use general shots of classrooms or group activities rather than close up pictures of individual children.

• Use images of children in suitable dress, and take care photographing PE events to maintain modesty, using team tracksuits if appropriate for example. Photographs should not be taken of swimming pool based events.

• Remember to include images of children from different ethnic backgrounds in your communications wherever possible, and positive images of children with disabilities to promote your school as an inclusive community, and to comply with the Disability Discrimination Act.

• Decide whether parents and visitors will be permitted to take photographs of the event. This must be authorised.

3b Identifying pupils

If the pupil is named, avoid using their photograph. If the photograph is used, avoid naming the pupil.

It is our policy that;

• You use the minimum information. Ask yourself whether it is really necessary to accompany a picture with the pupils' names, the year group, or the school.

- When *fully* naming pupils in any published text, whether in the school's brochure, website, or in the local press, avoid using their photograph, unless you have parental consent to do so.

3c Using photographs of children supplied by a third party

When using third parties, it is our school's responsibility to check that the adults are aware of the school protocols. In addition we would expect that the adult taking the images has a full CRB or is supervised when taking images by a member of the school's staff.

Children should never be left alone with a photographer.

Copyright does not apply to images for private family use. However, copyright does exist in commercial photographs and it rests with the photographer. Copyright is a right that the photographer automatically enjoys as the creator of the work to prevent other people exploiting his or her work and to control how other people use it. If you commission photographs for use at school/setting or work include in your contract that the school will own the copyright for items taken on your behalf.

3d Use of Images of children by the Press

(Please refer to the recommendations in section 3b above; 'Identifying Pupils')
There may be occasions where the press take photographs at school of pupils. If this occurs we will ensure that specific permission is sought from the parent about whether to agree to their children being featured in the press and whether their full name should accompany the photograph.

3e Videos

School will ensure that parental consent is in place before any child can appear in a video, Parents can make video recordings of nativity plays and other such events for their own personal and family use, as they are not covered by the Data Protection Act. (Please refer to section 3.10h).

3f Websites

Web use can be of particular concern to parents and staff because of the potential misuse of images by paedophiles. With digital photography there is the remote

possibility that images of children could be produced, manipulated and circulated without the parents or children's knowledge. The dual concern which follows such a risk is that children might be exploited and a school or setting might be criticised or face legal action. Images on website can be made more difficult to copy by several measures - copy-protection, overlaying with a watermark, or published in low definition.

It is important to take care with identification and to respect parental views on the use of any photography of children on a website.

Increasingly adults and children are generating content for websites e.g. children and adults placing pictures on **Instagram, Twitter, Snapchat** or **Facebook** websites. It is therefore important that schools/organisations ensure that children, staff and parents understand the risks involved and are encouraged to adopt safe practice when generating content for school related websites (www.Devonshireparkprimary.co.uk and Twitter feed). **This is included on our permission forms**. Parents and staff are not allowed to share school images on any Internet sites.

3g Webcams
The regulations for using webcams are similar to those for CCTV (closed-circuit television). This means that the area in which you are using the webcam must be well signposted and people must know that the webcam is there before they enter the area, in order to consent to being viewed in this way. Children should be consulted and adults would need to consent as well as the parents of all the affected children.

In gaining consent, the school must tell the person why the webcam is there, what you will use the images for, who might want to look at the pictures and what security measures are in place to protect access.

3h Parental right to take photographs and videos
We want parents to have the opportunity to record school events safely and responsibly.

We will allow recording, unless we feel that the images created may be inappropriate (for example a swimming gala, gymnastics display etc). We also have to ensure that consent is gained for **all** children taking part.

Parents are not covered by the Data Protection Act 1998 if they are taking photographs or making a video recording for **their own private use**. The Act does not, therefore, stop parents from taking photographs or making video recordings at school events, such as nativity plays or other such performances.

Parents are not permitted, however, to take photographs or to make a video recording for anything other than their own personal use (e.g. with a view to selling videos of a school event). Recording and/or photographing other than for private use would require the consent of the other parents whose children may be captured on film. Without this consent the Data Protection Act 1998 would be breached. **The consent form attached reminds parents of this fact**.

3i Images taken by young people
Children do have permission to take photographs on days out and residential trips etc. We will ensure that children understand that photographs must be responsible and not taken in private places. For example in bedrooms or toilets.

3j Use of Mobile Phones
Children are not allowed to use mobile phones in school. We allow children to bring mobile phones to school but these must be given to the Assistant Headteacher, Ms L White for secure handling and can be collected at 3:15pm.

Staff are **NOT** allowed to video or take photographs of children using personal mobile phones for ANY purpose. If they do then they may breach our obligations under the Data Protection Act.

Visitors are also informed of this as part of our safeguarding statement.

Parents can use them for recording only based on the guidelines above.

Appendix 4 – Suggested form for seeking additional consent for children to be photographed or filmed.

Dear parents/carers,

As part of our curriculum project on _____, the children will need additional content for photography because _____
_____. This is an exciting opportunity for your children.   We also aim to teach children how to use photographs safely.

For your child to take part in this project we need additional permission.

Additional permission for my child to be filmed or photographed in school		
Why is permission being sought?	**What are the school's responsibilities?**	
• We use photography and video throughout the curriculum. Children may use it to film their play performance or take photographs for art ideas etc. • We also use photographs to celebrate achievements in school. • So we can share our photographs with _____. • So that parents and children can film <u>authorised</u> events (nativity plays, school trips etc).	• To ensure that all photographs/videos are appropriate and related to educational purposes. • To ensure that all photographs and videos are stored securely on password protected computers or encrypted memory pens. • To only pass any photographs or video on to named 3rd parties with this parental permission. • To ensure that children's names are not printed next to photographs. • To ensure that all parents and carers are fully aware that photographs and videos they take at <u>authorised events</u> cannot be published on Internet sites including Facebook and other social networking sites.	
I give permission for my child to be photographed or recorded as part of school activities.		
	Signature	**Name**
I request permission to take photographs and video recordings of my child at authorised school events (performances, sports day etc) and confirm these are for my personal use only and will not be shared on any Internet sites.		

Appendix 5a: POLICY ON THE USE OF SOCIAL NETWORKING WEBSITES

The purpose of the policy is to provide clarity to all school staff on the use of any social networking website, e.g. Facebook, Twitter and its implications in relation to future employment status i.e. disciplinary action and potential dismissal. The policy relates to any young person under 19 years of age, any 'looked after child' under the age of 21 years of age, and any young person with special educational needs under the age of 24 years of age.

Any member of staff can have an account on a social networking web site. However, it is the responsibility of the individual to ensure that anything placed on the social networking site is appropriate and meets the standards expected of professional teachers and school support staff.   *NB School employees who have their own social networking site may have contact with relatives or family friends. However all the requirements below would still apply to the use of Social Networking Websites.*

All school staff **must:**

- Demonstrate honesty and integrity, and uphold public trust and confidence in respect of anything placed on social networking web sites.

- Ensure that any content shared on any social networking web site, at any time, would be deemed as appropriate, i.e. staff are personally responsible for ensuring that any privacy settings meet this requirement.

- Ensure appropriate language is used, at all times, for any comments placed on social networking sites.

- Ensure that any comments and/or images, at any time, could not be deemed as defamatory or in breach of any relevant legislation.

- Ensure they have no means of identifying their employer on their social media profiles (place of work or school badges on photographs).

All school staff **must not:**

- Have contact with current/ex pupils, or other children or young people where there is a relationship developed as part of their 'professional' role, e.g. music tutor, on any social networking website.

- Use social networking sites as a forum to make derogatory comments which could bring the school into disrepute, including making comments about pupils, parents, other staff members, the senior leadership team, governors, local authority or the wider community.

Any breaches of this policy could result in disciplinary action and may result in your dismissal.

I understand and agree to adhere to the Policy on the Use of Social Networking Websites.

Signed	Date

This document has been developed and consulted on with Wirral Professional Teachers' Associations and Trade Unions

Appendix 5b Union Guidance of Social Networking sites

NUT Cyber-Safe guidance states all staff should;

- not post information and photos about themselves, or school-related matters, publicly that they wouldn't want employers, colleagues, pupils or parents to see;

- keep passwords secret and protect access to accounts;

- not befriend pupils or other members of the school community on social networking sites. (Staff should consider carefully the implications of befriending parents or ex-pupils and let school management know if they decide to do this.)

NASUWT guidance states;

- To ensure that your Facebook account does not compromise your professional position, please ensure that your privacy settings are set correctly.

- Do not under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at your school.

As a minimum, NASUWT recommends the following:

Privacy Setting	Recommended security level
Send you messages	Friends only
See your friend list	Friends only
See your education and work	Friends only
See your current city and hometown	Friends only
See your likes, activities and other connections	Friends only
Your status, photos, and posts	Friends only
Bio and favourite quotations	Friends only
Family and relationships	Friends only
Photos and videos you're tagged in	Friends only
Religious and political views	Friends only
Birthday	Friends only
Permission to comment on your posts	Friends only
Places you check in to	Friends only
Contact information	Friends only

- Always make sure that you log out of Facebook after using it, particularly when using a machine that is shared with other colleagues/students. Your account can be hijacked by others if you remain logged in – even if you quit your browser and/or switch the machine off. Similarly, Facebook's instant chat facility caches conversations that can be viewed later on. Make sure you clear your chat history on Facebook (click "Clear Chat history" in the chat window).

- Employers may scour websites looking for information before a job interview. Take care to remove any content you would not want them to see.

Conduct on social networking sites

- Do not make disparaging remarks about your employer/colleagues. Doing this in the presence of others may be deemed as bullying and/or harassment.

- Act in accordance with your employer's information technology (IT) policy and any specific guidance on the use of social networking sites. If your school/college encourages the positive use of social networking sites as part of the educational process, they should provide clear guidance on what is considered to be appropriate contact with students. Having a thorough policy in place will help staff and students to keep within reasonable boundaries

- Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed. If you face disciplinary action as a result of being tagged, contact your union immediately.

- Parents and students may access your profile and could, if they find the information and/or images it contains offensive, complain to your employer.

- If you have any concerns about information on your social networking site or if you are the victim of cyberbullying, you should contact your union immediately.

- Do not publish your date of birth and home address on Facebook. Identity theft is a crime on the rise with criminals using such information to access to your bank or credit card account.

- Be aware of what monitoring, if any, may be carried out by the school/college. Full details of this should be detailed in the IT policy.

- Stop the network provider from passing on your details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click "Privacy Settings". Under "Applications and websites" click "edit your settings". Scroll down to "instant personalisation" and make sure the checkbox for "enable instant personalisation on partner websites" is unchecked.

- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation

ATL guidance states;

The following advice shows best practice for both yourself and the school/college.

- Act in accordance with the school/college information technology (IT) policy, which should contain a section on the use of social networking sites. If your school/ college encourages the positive use of social networking sites as part of the educational process, they should provide clear guidance on what is considered to be appropriate contact with students. Having a thorough policy in place will help staff and students to keep within reasonable boundaries

- Ensure that any contact with students is kept strictly within an educational context.

- Set your privacy settings. Most social networking sites allow you to control who can see your information. For example, at the bottom of every page on Facebook, there is a link that reads 'privacy'. The linked page is 'a guide to privacy on Facebook', containing the latest privacy functions and policies. Set your privacy settings to "only friends". Settings such as "friends of friends" and "networks and friends" open your content to a wider audience. Your privacy and that of your family, friends, colleagues and students could be compromised.

- Bear in mind that somebody else could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed. If you face disciplinary action as a result of being tagged, ATL can provide advice and assistance.

- Remember humour is relative. For example, posting images and/or text about a recent stag or hen night may be deemed inappropriate. Likewise, a few 'light-hearted' comments and/or images about colleagues or students may not be perceived as such by either the subject(s) of the humour or your employer. The guiding rule is if in doubt, don't post it.

- Make sure you regularly check and refresh your site page to ensure it is free of any inappropriate comments and/or images.

- Remember that parents and students may access your profile and could, if they find the information and/ or images it contains offensive, complain to your employer.

- Consider that colleagues, including management, might access your profile. Depending on the comments and/or images it contains, you may face disciplinary action. Any member that does face disciplinary action should contact ATL as soon as possible.

- Remember that there is a growing trend for schools/ colleges to access social networking sites before interviewing job applicants. Depending on the comments and/or images contained on your site you may not be selected for interview.

- Be clear who you should contact if you have any concerns about information on your social networking site or if you are the victim of cyberbullying.

- Keep your date of birth and home address to yourself. Identity theft is a growing crime and this kind of information could be used to gain access to your bank or credit card account.

- Mind your language. Abrupt, inappropriate and unthinking use of language may lead to complaints from colleagues, pupils, parents and/or management.

- Be aware of what monitoring, if any, may be carried out by the school/college. Full details of this should be detailed in the IT policy.

- Stop the network provider from passing on your details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click 'account', then 'privacy settings', then 'search'. Beside 'instant personalisation pilot programme', click 'edit setting'. Make sure the box at the bottom of the screen has not been ticked. To ensure that you do not appear in any adverts, click 'accounts', then 'account settings', then 'Facebook adverts'. Select 'No one' on the 'allow ads on platform pages to show my information to' and 'show my social actions in Facebook ads to'.

- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.

- Be aware that an employee's personal messages can be monitored by the employer. ATL urges employers to amend their IT policies in light of the judgement and in doing so provide clear, unambiguous guidance to their staff. ATL advises its members to ensure that all communications sent during work hours from company devices are entirely professional.

There are many professional and personal benefits to be obtained through social networking sites. Building these simple procedures into your routine should help you get the most from the sites while maintaining a confident and positive digital profile.

Think Then Click
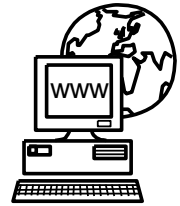
Use these rules to stay safe when using a computer:

Our eSafety Top Tips!

1 People you don't know are strangers.

They're not always who they say they are.

2 Be nice to people like you would on the playground.

3 Keep your personal information private.

4 If you ever get that 'uh oh' feeling, tell a grown-up you trust.

Think Then Click

At Devonshire Park Primary we use these rules to stay safe when using a computer or any electronic device that can access the Internet:

S — Stay Safe
Don't give out your personal information to people / places you don't know.

M — Don't Meet Up
Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.

A — Accepting Files
Accepting emails, files, pictures or texts from people you don't know can cause problems.

R — Reliable?
Check information before you believe it. Is the person or website telling the truth?

T — Tell Someone
Tell an adult if someone or something makes you feel worried or uncomfortable.

Follow these SMART tips to keep yourself safe online!

Appendix 8 - *Flowchart for responding to e-Safety incidents*

```
                           ┌──────────────┐
                           │   e-Safety   │
                           │   Incident   │
                           └──────┬───────┘
              ┌───────────────────┴──────────────────┐
       ┌─────────────┐                        ┌──────────────┐
       │  Unsuitable │                        │ Inappropriate│
       │  materials  │                        │   Activity   │
       └──────┬──────┘                        └──────┬───────┘
       ┌─────────────┐                        ┌──────────────┐
       │  Report to  │                        │   Contact    │
       │ Headteacher │                        │ Headteacher  │
       └──────┬──────┘                        └──────┬───────┘
     ┌────────┴────────┐                   ┌─────────┴─────────┐
```
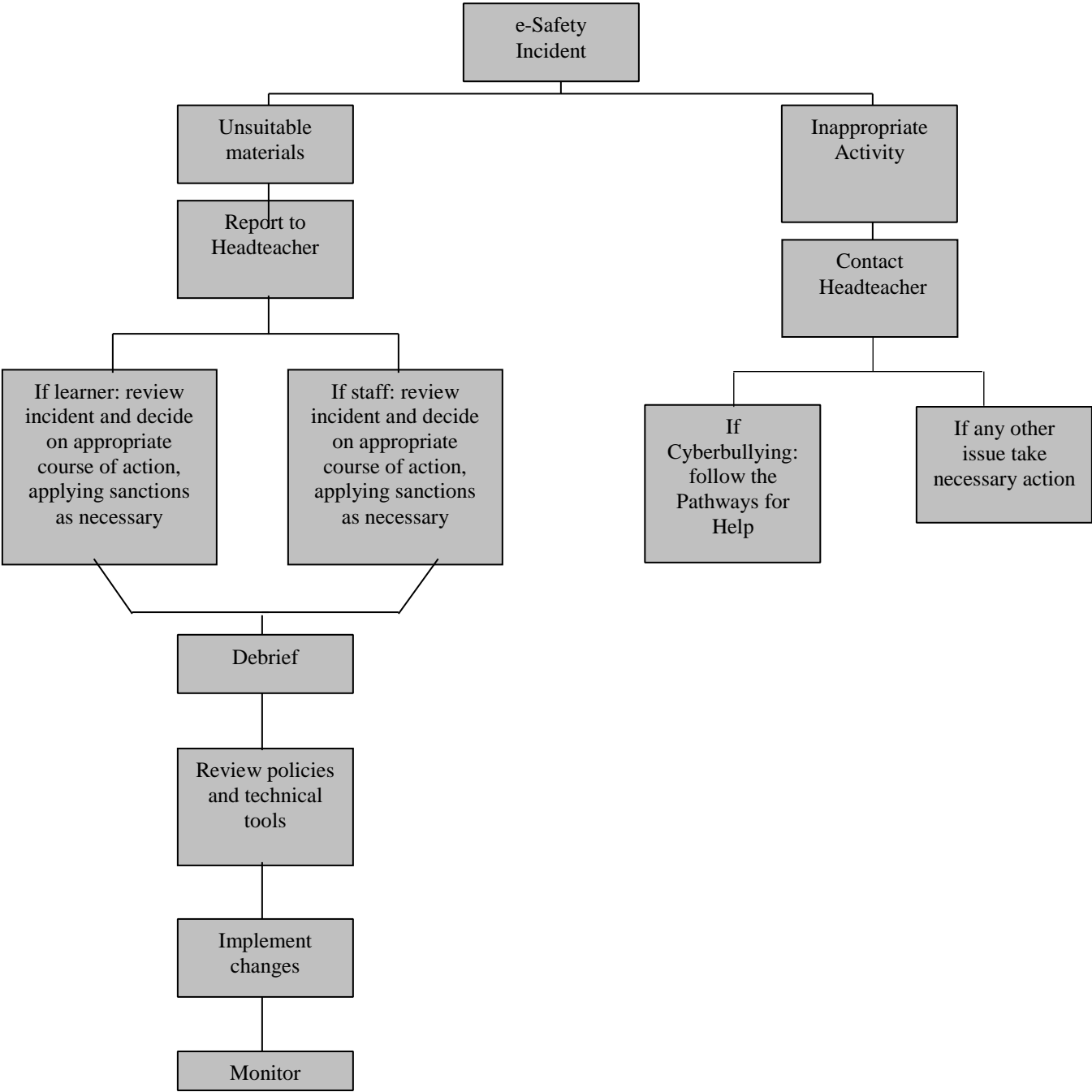
| If learner: review incident and decide on appropriate course of action, applying sanctions as necessary | If staff: review incident and decide on appropriate course of action, applying sanctions as necessary | If Cyberbullying: follow the Pathways for Help | If any other issue take necessary action |

```
              ┌──────────┐
              │ Debrief  │
              └────┬─────┘
       ┌──────────────────────┐
       │    Review policies    │
       │   and technical       │
       │      tools            │
       └──────────┬───────────┘
       ┌──────────────────────┐
       │     Implement         │
       │      changes          │
       └──────────┬───────────┘
              ┌──────────┐
              │ Monitor  │
              └──────────┘
```

Appendix 9 - **e-Safety Audit**

This quick self-audit will help the senior management team (SMT) assess whether the e-Safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	Y/N
Date of latest update: October 2017	
The Policy was agreed by governors on:	
The Policy is available for staff at: T:/Policies & Procedures/	
And for parents at: www.Devonshireparkprimary.co.uk	
The designated Child Protection Teacher/Officer is: Mrs R Tootell	
The e-Safety Coordinator is: Mr S Dutton/Mrs J Billinge	
Has e-Safety training been provided for both Pupils and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign a COMPUTING Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Have school e-Safety Rules been set for Pupils?	Y/N
Are the e-Safety Rules displayed in all rooms with computers?	Y/N
Is Internet access provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access?	Y/N
Has the school filtering policy been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT?	Y/N

Appendix 10 - **Are you an e-Safe school?**

Do all your staff...	Does your school...
☐ Understand e-Safety issues and risks? ☐ Receive regular training and updates? ☐ Know how to escalate an issue of concern? ☐ Know how to keep data safe and secure? ☐ Know how to protect themselves online? ☐ Know how to conduct themselves professionally online? ☐ Know about the updated e-Safety guidance for QTS standard Q21: Health and well-being?	☐ Have a nominated e-Safety co-ordinator? ☐ Audit its e-Safety measures? ☐ Have a robust AUP? ☐ Use a Becta accredited supplier for internet services? ☐ Include e-Safety measures in your SEF? ☐ Keep an incident log and monitor your measures? ☐ Handle cyberbullying issues well? ☐ Raise awareness of the issues, e.g. through holding an assembly?
Do your Pupils...	Do your parents and governors...
☐ Understand what safe and responsible online behaviour means? ☐ Receive e-Safety education at appropriate places across the curriculum? ☐ Get the opportunity to improve their digital literacy skills? ☐ Know the SMART rules? ☐ Know how to report any concerns they may have?	☐ Understand e-Safety issues and risks? ☐ Understand their roles and responsibilities? ☐ Receive regular training and updates? ☐ Understand how to protect their children in the home?

Appendix 11 - *e-Safety Incident Log*

Date	Staff	Incident (including URL)	Action