St. Paul's
C.E. Primary School
Learning Together

On Line Safety Policy

Background

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorized access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

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

The E Safety Committee

Liane Moore, Cath Palmer-Named Person
Jennifer Charles – ICT co-ordinator/E-safety lead
Grace Briggs- PHSCE Coordinator
Danny Newton - School Technician. The committee will consult him over technical issues related to safeguarding and security of data.
Sandra Philips – Safeguarding Governor

This policy should be read in conjunction with our other safeguarding policies including:
Anti bullying policy
Child Protection Policy
Allegations against staff Policy
Whistle blowing policy
Data protection policy
Staff Acceptable Use of ICT Policy
Pupil Acceptable Use of ICT Policy

Development and Review of this policy.

This e-safeguarding policy was approved by the	Full Governing Body
The implementation of this e-safety policy will be monitored by the:	The E-Safety Committee
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Allana Khan Safeguarding Officer Bradford Council
The Board of Directors / Governing Body / Governors Sub Committee will receive an annual report regarding the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2020

Monitoring the impact of the policy

The school will monitor the impact of the policy using

- Logs of reported incidents in the e safeguarding incident log
- Internal monitoring data for network activity (See Danny Newton – school technician)
- Surveys/questionnaires of pupils , parents/carers and staff

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Resources Committee receiving regular information about e-safety incidents and monitoring reports.

The Governor responsible for Safeguarding (Sandra Phillips) will take on the responsibility for e- safety.

The role of this governor will include meeting with the E-safety Committee where :

- e- safety issues will be discussed
- e-safety incident logs will be monitored
- filtering logs will be monitored

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, although the day to day responsibility for e-safety will be delegated to Jennifer Charles the E-safety lead
- The Head teacher is responsible for ensuring that relevant staff receives suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head teacher is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. This is detailed in the Allegations against staff policy.

E-Safety Co-ordinator

- takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policy.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- attends Full Governing Body meetings (when e safeguarding issues are to be discussed).

Network Manager / Technical staff:

Danny Newton the school technician ensures:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that he keeps up to date with e-safety technical information and updates the E Safety Coordinator as relevant.
- that monitoring software and anti- virus software is implemented and updated

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety leader
- digital communications with pupils should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities . E Safety lessons are taught through the Common Sense and South West Grid for Learning Digital Literacy scheme.
- pupils understand and follow the school e-safety and acceptable use policy
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

Named person for child protection

Cath Palmer and Liane Moore are the named people for child protection.

They are trained in e-safety issues and to be aware of the potential for serious child protection issues to arise from:

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

Children

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
    - Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their action out of school, if related to their membership of school
    - Should know and understand the school policies on the taking/use of images and on cyber-bullying

Parents / Carers

The school will take every opportunity to help carers / parents to understand issues related to e-safety. We will assist parents to understand key issues in the following ways:

A parents e-safety presentation takes place annually.

Our school web site http://stpaulsceprimary.com/ has links to e-safety guidance

Parents are asked to discuss the pupil Acceptable use policy with their children.

Community Users

No person can log on to the internet without a user account or the Internet password. A community user account with minimal privileges will be given after discussion of the sites wished to be accessed.

Education – Pupils

The education of pupils in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-Safety education will be provided in the following ways:

- In accordance with the 2014 National Curriculum requirements a planned e-safety programme is delivered as part of Computing/PHSE in the form of the Common Sense/ SWGFL Digital Literacy Scheme.
- The Bradford Computing Scheme of work also highlights e Safeguarding issues that arise in the context of Computing lessons.
- Key e-safety messages are reinforced as part of a planned programme of assemblies. They take place once a term and are mentioned in the school diary.
- Pupils are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information. Validation of information is covered in the research strand of the Bradford Computing scheme of work.
- Rules for use of ICT systems will be posted in all classrooms
- For directed searches in school staff should direct children to Primary Safe Search or other search tools recommended in the research section of the Bradford Computing Scheme of work.

  http://innovationcentres.org.uk/index.php?option=com_content&view=article&id=1733&Itemid=240
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. Evaluation and cross referencing of sources are covered in the research strand of the Bradford ICT scheme of work which the school follows.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Copyright free audio and image sources are detailed in the Multimedia and Sound strands of the Bradford Computing scheme of work which the school follows.

Education - Staff Training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A Staff meeting covering e-safety will take place annually. This will be delivered by a member of Bradford Council Children's Services Curriculum ICT Team, the police cyber team or a member of the E Safeguarding Committee.
- An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.

Education - Governor Training

Governors should take part in e-safety training / awareness sessions. E-Safety training is planned annually; governors are encouraged to attend the parents' e- safety training session.

Internet Provision

The school Internet is provided by the Bradford Learning Network, a DFE accredited educational internet service provider. All sites are filtered using the Smoothwall filtering system which also generates reports on user activity. School also subscribes to E-safe which also monitors and provides report of inappropriate user activity.

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images online. It is vital both staff and pupils are aware of and take responsibility for their digital footprint. Images may remain available on the internet forever and may cause harm or embarrassment to individuals in the sort or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Photographs of children published on the website or blog must not contain names.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.

Personal Data Protection

Staff must ensure that they:

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

Passwords

- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- Passwords for new users, and replacement passwords for existing users can be allocated by Danny Newton

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

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

- in ICT and / or e-safety lessons
- through the Acceptable Use Agreement

All users (at KS2 and above) will be provided with a username and password by Danny Newton who will keep an up to date record of users and their usernames.

Acceptable Use Policy

Use of the Internet is now an integral part of people's lives. In spite of this, it is important schools continue to be aware of issues and problems and to continue to educate our children accordingly. It is important staff, pupils and parents understand the moral and ethical issues surrounding access to the Internet before allowing access.

There are a number of options available that restrict access to the Internet, but it must be understood that no system, other than a ban on using the Internet, can ensure users do not access material that is deemed inappropriate. Pornographic material is usually the main focus of filtering methods, but users need to be aware that removing racist, sexist and political material is beyond many filtering programs. There is also the difficulty with any filtering software that content which is deemed offensive to one group of people is regarded differently by others. Furthermore, we are now faced with more recent issues such as grooming, cyber-bullying and identity theft which cannot be controlled by filtering systems. For these reasons, treating the use of the Internet as an issue that involves pupils, staff and parents has to be the most sensible approach.

In response to this, the most appropriate course of action is to develop a school policy on use of the Internet together with rules for safe internet use and acceptable use policies for children and staff.(See appendix 1, 2 and 3)

Today millions of people use the Internet and e-mail on a daily basis. In recent years, use of the Internet has continued to increase, particularly with the introduction of mobile devices. This is not only for business and personal use, but also for educational purposes. A wealth of educational resources is now available on the Internet and via mobile devices; and this continues to grow. At St Paul's CE Primary School, we believe that our pupils should have opportunity to use these emerging and changing technologies to support their learning and to equip themselves with the skills that will be required for lifelong learning

Resources found on the Internet, are unlike those found in more traditional media. Historically, resources such as books, videos and other resources could be carefully selected for the learning process. The Internet, by its open and dynamic nature, may lead pupils to material over which the teacher has had no previous viewing and has therefore been unable to judge its suitability for classroom use. Although the school will endeavour to point pupils to relevant curriculum sites or to previously researched sites that have been identified as being relevant to the area of study, we also accept our responsibility in educating our pupils about responsible, respectful and safe use of the Internet.

Research using electronic methods is now fundamental to preparing pupils for citizenship and future employment possibilities. The school will ensure that opportunities for both integrating the use of the Internet into the curriculum and teaching pupils about e-safety will be planned and that staff will guide pupils in line with Government guidelines.

The school recognises that training the staff in preparation for using the Internet and indeed any mobile technology in a safe manner is vital. The school will use a variety of agencies to train the staff in integrating new technologies into the curriculum. Staff will be given regular opportunities to discuss issues surrounding the use of the Internet and e safety and develop appropriate teaching strategies. In addition, relevant governmental guidelines will be made available to all staff as a point of reference.

The school uses an Internet Service Provider (ISP) that has filtering software in place to minimise the risk of accessing inappropriate Internet material or receiving inappropriate e-mail. Should any pupils access material they have concerns about, they should notify a member of staff, who will then inform the ESafety Co-ordinator. The Co-ordinator will then ask the ICT Technician to inform the ISP of the address of the offending web site. Where possible, appropriate action will then be taken to block further access. On occasions where a total block is not possible, staff will then use this to remind pupils of their own responsibilities in becoming safe users, in line with the Computing curriculum. The school will take appropriate action against users that use the school facilities to knowingly access, or attempt to access inappropriate materials. Therefore, the school reserves the right to access the work area of any user to view files held in that area.

All pupils across the school have access to the Internet and are able to use the technology available. It is anticipated that access to younger pupils will be more directed, with autonomous use being available to older pupils. Where pupils are given freedom to search the Internet for information, they should be given clear learning objectives by their teacher. In the event of inappropriate use or the accessing of inappropriate materials, action will be taken by the teacher, E safety co-ordinator or the Head. Any incidents will be reported and logged by the E safety co-ordinator.

Pupils will be taught to use e-mail, the Internet, the school blog and mobile technology responsibly to reduce the risk to themselves and others. After being agreed by staff and pupils at the beginning of each year, rules for Internet access and the use of all technologies within school will be posted in each classroom and around the school. E safety will form an integral part of Computing lessons but will also be covered in regular assemblies and as part of our PSHE programme of study.

The school believes that access to the Internet and mobile devices will enable pupils to explore resources available from libraries, other schools, LAs and commercial content providers in a way that will enhance the learning process in ways impossible by other means. E-mail will allow communication to be made with other individuals and organisations, regardless of time and distance.

The school believes that access to this technology brings benefits to the learning processes that outweigh the possible risks that might be encountered.

Older children will be encouraged to accept some responsibility for their use of the Internet and will be asked to sign a pupil e-safety declaration.

The final responsibility for use of the Internet and E safety lies with the parents/carers of our pupils. Parents will therefore also be provided with support and guidance to maintain their children’s safety away from school, through regular events in school and through documentation provided on our website. Such information will also be available in hard copies from the school, should this be required.

Appendix 1

Pupil Acceptable Use Policy

This document has been developed to help you understand the rules of using computers in school. You should always follow the rules set out in this policy because these rules will help keep you and your classmates safe.

School's ICT equipment

- I will make sure I take care of any school-owned ICT equipment that I use in school or at home.
- I will not eat or drink while using school-owned ICT equipment.
- I will only go on the internet using my own username and password
- I will not try and get to any websites that the school has blocked access to.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I see anything like this I will tell my teacher immediately.
- I will only use memory sticks with permission from my teacher.
- I will not install any software on school computers.
- I will return any school-owned ICT equipment when I have finished using it.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my safety.

Social Media

- I know that some websites and social networks have age restrictions and I should not use them unless I am old enough.
- I will not say nasty or hurtful things about any member of staff or pupil online.
- I will not give away any of my personal details (full name, age, date of birth, sex, address etc.) or the personal details of other users in school, over the internet. This includes photographs or video images of me, other pupils or members of staff.
- I will never arrange to meet anyone I have only met online unless a trusted adult is with me.
- If I see any hurtful comments about the school, staff or pupils. I will take screenshots for evidence and report to the e-Safety coordinator.

Managing Digital Content

- I will only use school-owned equipment to create pictures, video and sound. Pictures, video and sound will not be taken without asking permission first.
- I will not publish anything online, e.g. images or pictures, without asking my teacher.

Email

- I will only use my school email address to contact people I know or those agreed by my teacher.
- I will take care in opening any attachments sent by email. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.

- When sending emails I will make sure that they are polite and sensible. I will not use my school email account to forward chain emails.

Mobile phones and devices

- If I bring will my mobile phone or other devices to school I will hand it in at the office on my arrival and collect it at home time.

- I will not take pictures in school on my mobile phone or mobile device.

Agreement

I agree to follow the rules set out in this acceptable use policy. I know that if I break any of these rules my parent/carer may be told.

Pupil name

Signed

Date

Appendix 2

Staff Acceptable Use of ICT Policy

(including mobile phones)

This document has been developed to ensure staff within school are aware of their professional responsibilities when using ICT equipment and systems. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when carrying out any activity which involves using ICT equipment and information systems, either within school or at other locations, such as home. ICT equipment and associated technologies include all facilities and resources used to access the school ICT network and internet as well as standalone devices with digital storage.

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements

- I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the e-safety coordinator.

- All passwords I create will be in accordance with the school e-safety policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems and that I will use a unique password for each system.

- I will not share my passwords with any colleagues or pupils within school.

- I will seek consent from the e-safety coordinator/ICT coordinator prior to the use of any new technologies (hardware, software, cloud-based services) within school.

- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-safety coordinator/ ICT coordinator

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the e-safety coordinator/ ICT coordinator

- I will ensure that all devices taken off site, (laptops, tablets, cameras, removable media or phones) will be secured in accordance with the school's Data Protection Registration and any information-handling procedures both on and off site.

- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.

- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.

- I will secure any equipment taken off site for school trips.

- I will only put school information on school-owned or provided portable storage (USB sticks, portable hard drives etc).

- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.

- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the ICT coordinator

- I will return any school-owned ICT equipment or software to the relevant individual within school once it is no longer required.

- I understand that 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 the appropriate authorities.

- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.

- I understand that if I do not follow all statements in this AUP and in other school policies relating to the use of ICT equipment I may be subject to disciplinary action in line with the schools established disciplinary procedures.

Social Media

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.

- I must not use social media tools to communicate with current or former pupils under the age of 18.

- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.

- Staff must not access social networking sites for personal use during school hours.

- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the e-safety coordinator.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.

- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the eSafeguarding Policy

- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from the designated member of staff. (eSafeguarding coordinator or Head Teacher).

- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright law.

- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.

- I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and immediately deleted from the memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Learning and teaching

- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

Email

- I will use a school email address for all correspondence with pupils, parents or other agencies and I understand that any use of the school email system will be monitored and checked
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of the school.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- Emails sent to external organisations will be written carefully and authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the headteacher, line manager or another suitable member of staff into the email.
- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

Mobile phones and devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to ‘silent’ mode during school hours.
- Mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- I will not contact any parents or pupils on my personally-owned device.
- I will not use any personally-owned mobile device to take images, video or sound recordings.

Agreement

I have read and understand all of the above listed points relating to my use of technology (including mobile phones) within school. I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Staff name

Signed

Date

Appendix 3

St. Paul's
C.E. Primary School
Learning Together

RULES FOR RESPONSIBLE INTERNET USE

The school has computers, laptops and iPads with internet access to help our learning.

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

- I will ask permission from a member of staff before using the internet on any device,
- I will use only my own log in details and not share these with others,
- I will not access other people's files,
- I will use the computers only for school work and homework,
- I will not bring USB memory sticks into school unless I have permission,
- I will only e-mail people I know, or people my teacher has approved,
- The messages I send will be polite and sensible,
- I will not give out my home address, telephone number or any other personal details online, or arrange to meet someone, unless my parent, carer or teacher has given permission,
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or if I receive a message I do not like,
- I understand that the school may check my computer files and monitor the internet sites I visit.