Online Safety Policy
Poulton-le-Sands C of E Primary School

As a sanctuary of Christian love, we forge futures in our community. We inspire a joy of learning and a delight in one another. In faith, we are refined through challenge, growing with God, together.

The light shines in the darkness and the darkness shall not overcome it.

John 1 v.5

Introduction

At Poulton-le-Sands we recognise the importance of ICT in education and the needs of pupils to access the benefits which the digital environment can offer. These technologies are powerful tools, which open up new opportunities for everyone and can improve effective learning, stimulate discussion and promote creativity. However, above all, we believe that everyone is entitled to safe internet access at all times. With this new technology there is an element of risk that cannot be eliminated. Therefore, we help the children to develop their skills, knowledge and confidence to manage these risks and to make informed sensible decisions.
This policy applies to all members of the school community (including staff, pupils, parents/carers and visitors)

Vision

Online safety is an integral part of our teaching and learning by supporting everyone to be safe when using IT equipment within the school environment and wider community. It is a key part of forging futures in our community. The Online Safety policy is linked to the computing policy, along with the PSHE policy and guidance. Online safety is a part of the computing curriculum and is taught in every year group, throughout the year.

The internet

The purpose of using the internet in school is to raise educational standards, promote achievement and to support the professional work of staff. It allows us access to worldwide educational resources, access to experts, and communication between support services and promotes staff development through the acquisition of knowledge. Internet use is planned to enrich and develop learning opportunities, it is not a “bolt on”. Filtering is through Tech-Hub. Filtering is achieved through their SurfProtect Filtering for Education system. Requests to unblock sites can be given to the subject leader. Sites can be unblocked for different users for different time periods. You tube access is currently granted to staff accounts after a professional discussion, but restricted on children logons. The safe search SWIGGLE is now the default on the computers, although google and others are still available via the search bar.

Online Safety Champion

Our Online Safety Champions are L Marshall (also backup DSL) and H Buckham (Computing Subject Leader). Any staff concerns should be brought to them regarding computing or online safety. They are responsible for maintenance and review of the online safety policy, including acceptable use policies along with ensuring policies are implemented and compliance is monitored. Any online safety issues are noted on CPOMs under online safety concern.

Data Protection

Please read the Data Protection Policy.
All data in school is kept securely and staff informed of what they can or can’t do with data through the Online Safety Policy and statements in the Acceptable Use Policy (AUP) that is signed for annually.

The Headteacher has overall responsibility for the management of data within school. Access to data is password protected with individual rights assigned, depending on job requirements. Confidential data can only be accessed with approval from the Headteacher.
The Bursar has remote access to school data. She is aware of the dangers of using unsecured wireless networks at home to access school information.
Class assessment trackers are kept on SIMS, which is password protected.
Staff have individual logons to the network and children access the network through their year group logon.
Any data loss should be reported to the Headteacher immediately. All data is backed up by Tech-Hub and sent offsite to a UK data centre.

Use of Mobile Devices

While we fully acknowledge a parent's right to allow their child to bring a mobile phone to school, Poulton-le-Sands CE Primary School discourages pupils from bringing mobile phones to school.

- If pupils bring mobile phones to school, the phones must remain switched off while pupils are in class, the school building and the school grounds. It must be handed in to the class teacher for safekeeping.
- Should parents need to contact pupils, or vice versa, this should be done following the usual school procedures: via the school office. (tel no. 01524 413273)
- Where a pupil is found by a member of staff to be using a mobile phone, the phone will be taken from the pupil, handed to a senior member of staff who will record the name of the child and attach to the phone. The mobile phone will be stored by that teacher. The pupil may collect the phone at the end of the school day.
- If a pupil is found taking photographs or video footage with a mobile phone of either other pupils or teachers, this will be regarded as a serious offence and disciplinary action will be taken according to the school's Behaviour Policy.
- If images of other pupils or teachers have been taken, the phone will not be returned to the pupil until the images have been removed by the pupil in the presence of a teacher.
- Parents are advised that Poulton-le-Sands accepts no liability for the loss or damage to mobile phones which are brought into the school or school grounds.

Staff mobile phones

Phones should be turned off during teaching sessions. Individual personal circumstances are discussed with the SLT e.g. hospitalised relative and permission may be given for that phone to remain on silent.
Personal phones may be used on school trips but personal numbers should not appear on any documents where parents or children may see it.
EYFS to take a phone on home visits.
At school events (sports days/productions) parents are asked to focus upon their child and agree to not post images/videos on any social media sites.

iPads

The school uses these for teaching and learning. iPads do not allow access to the app store, email or facetime. Content is stored on individual devices. In some lesson's children are taught to use cloud-based services such as drop box, but this is closely monitored within lessons.

Use of Digital Media

Various forms of digital media offer substantial benefits to education but equally present school with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites. In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.
As photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), we ensure we have written permission for their use from the individual and/or their parents or carers. This information is collected when a child starts school and an up-to-date list is obtainable from the office. The permission is made in terms of the intended use of the photograph. No names will be attached to photographs on the website or in the local media without the permission

of the person involved and no children's names will be attached to photographs on the school website. Photographs and videos must only be taken on school equipment and must not be taken off the school premises.
· Training has taken place to ensure that staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
· When taking photographs/video, staff must ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
· Close up shots should be avoided as these might be considered intrusive. Shots should preferably include a background context and show children in group situations.
· Publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved is an offence.

These guidelines are monitored annually by the Online Safety Champion. Only school equipment is used for taking photographs and films for use in school. Guests in school are not allowed to take photographs on their own devices. See safeguarding policy.

Storage of Photographs/Videos
These should be saved to the staff drive in the photograph folder. These are organised into the year taken and then the year group. Photos should be deleted from the memory card of the camera as soon as possible. Photos and videos are deleted when the child has left our school. Items taken from the ipad remain on the individual device and these are checked/deleted throughout the year.

Communication Technologies

Email:

In our school the following statements reflect our practice in the use of email.
· All users have access to the Lancashire Grid for Learning service as the preferred school e-mail system.
· Only official email addresses should be used to contact staff/pupils.
· Pupils may have individual email addresses.
· Class email accounts will be monitored by individual teachers at appropriate time intervals or following a period of usage.
· The SurfProtect Filtering for Education should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Tech-Hub.
· All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
· All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
· All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
· All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
· All users are aware that they should not open any attachments if they suspect they may contain illegal content as they could be inadvertently committing a criminal act.

- Our school will include a standard disclaimer at the bottom of all outgoing emails

Example of school e-mail disclaimer:

This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent Poulton-le-Sands CE Primary School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Social Networks:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter and Instagram. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments. NB: Many Social Network sites have age restrictions for membership e.g. Facebook minimum age is 13 years old. All staff need to be aware of the following points:

· They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.

· Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.

· If a Social Network site is used, details must not be shared with pupils and privacy settings should be set at maximum.

· Pupils must not be added as 'friends' on any Social Network site.

· Careful consideration is required if parents of Poulton-le-Sands pupils are 'friends' on any Social Network site.

Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Video Conferencing

- Parents will be asked for permission before pupils take part in video conferencing sessions.
- Approval by the Headteacher must be obtained in advance of the video conference taking place. All sessions will be logged including the date, time and the name of the external organisation/person(s) taking part.
- Pupils using video conferencing equipment should be supervised at all times.
- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to 'hang up' the call.
- Staff understands that copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.
- Video conferencing will be used to keep in contact with children in the event of a bubble closure, or full lockdown. Staff, children and parents will be made aware of the expectations for ensuring online video conferencing is safe and successful. Zoom and Google Meets will be used for video conferencing.

School Website

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

· Data that is specified under the School Information (England) (Amended) Regulations 2012 is available on the school website. Data is updated by designation office staff and/or the Deputy Headteacher.

· The Lancashire E-Safety advice and guidance is linked from the school website

· The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.

· Web site photographs that include pupils will be selected carefully

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

· Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

· The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

· The website should comply with the school's guidelines for publications.

· The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
· Downloadable materials must be in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the school's consent.

Online Challenges or Hoaxes

What we do when a harmful online challenge or online hoax is circulating between children and young people.

· The designated safeguarding lead (DSL) will be involved in the pre-planning and will provide any formal responses, if deemed necessary.

· We will undertake a case-by-case assessment, establishing the scale and nature of the possible risk to our children and young people, including considering (where the evidence allows) if the risk is a national one or is it localised to our area, or even just at Poulton-le-Sands C of E Primary School. Quick local action may prevent a local online hoax or local harmful online challenge going viral.

· A named DSL will check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the Professional Online Safety Helpline from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be sought.

· Forward planning, together with case-by-case research, will allow for a calm and measured response and avoid creating panic or confusion.

Acceptable Use Policy

Acceptable Use Policy (AUP) is intended to ensure that all users of technology within Poulton-le-Sands School are responsible and protected from potential risk in their use of ICT. AUPs are in place for pupils and staff; supply teachers, student teachers, parental volunteers who use the internet/computers in school and visitors/guests. AUPs are signed and all users must adhere to the AUP. AUPs are stored securely in the office. AUPs support the school's online safety policy.

Dealing with Incidents

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor LCC can accept liability for the material accessed, or any consequences of internet access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

The headteacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Always report potential illegal content to the Internet Watch Foundation. (http://www.iwf.org.uk) .They are licensed to investigate – schools are not!

Potential illegal content must always be reported to the Internet Watch Foundation

(http://www.iwf.org.uk). Examples of illegal offences are:

1. Accessing child sexual abuse images
2. Accessing non-photographic child sexual abuse images
3. Accessing criminally obscene adult content
4. Incitement to racial hatred

More details regarding these categories can be found on the IWF website;
http://www.iwf.org.uk

Incident	Response
Accidental access to inappropriate materials.	Minimise the webpage/turn the monitor off. Tell a trusted adult. Enter the details on CPOMs and report to a named DSL. The computer technician may be informed to remote in and identify the breach. Persistent 'accidental' offenders may need further disciplinary action. Use the CEOP button on school website to report a concern if necessary.
Using other people's logins and passwords maliciously.	Inform SLT or designated Online Safety Champion. Enter the details on CPOMs. Additional awareness raising of eSafety issues and the AUP with individual child/class. More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. Consider parent/carer involvement.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

- Online safety incidents will be reported to the DSL or Deputy DSL's and will be recorded on CPOMS. They will then decide on the appropriate action to be taken.

  - All staff are aware of the different types of Online safety incidents and how to respond appropriately.
  - All pupils are informed of procedures through discussions from members of staff.
  - Incidents are monitored by the Online Safety Champion and Headteacher on a regular basis.
  - The Headteacher will decide on which point that parents or carers are informed.
  - The procedures are in place to protect staff and escalate a suspected incident / allegation involving a staff member

Infrastructure and Technology Pupil Access:

Pupils will only have supervised access to the internet. Limited access is to be allowed during playtime or lunchtime.
Passwords: Children only have class access. Teachers have class and staff access. The administrator password is only known by the ICT technician and the computing subject leader.
Software/hardware: School has legal ownership of all software, including site licences where appropriate. Licenses for all software are kept in a secure place by the computing subject leader and technical staff. The computing subject leader regularly audits equipment and software. Control over what software is installed on school systems is maintained by the computing subject leader.

Managing the Network and Technical Support:

The network is managed and technical support provided by Tech-Hub.

· The server are located in the IT room and password protected.
· All wireless devices have had their security enabled.
· The technician responsible for managing the security of the curriculum school network and the BT internet services manage the security of the office network.
· Computers are regularly updated with critical software updates/patches by the technician.
· Breaches of security must be reported immediately to the SLT.
· Laptops may be used for personal use but must not be used by family members.
· Technical support providers are made aware of our schools requirements / standards regarding Online Safety.
· It is the SLT's responsibility to liaise with/manage the technical support staff.

Filtering and Virus Protection:

· Filtering may be performed by the ISP, by the LEA, at school-level or by any combination.
· The school will work in partnership with parents, the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
· Staff use Google as the default on their homepage. Pupils use Swiggle as the default, although other search engines are available to either.
· If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT subject leader.
· Staff are expected to bring their laptops into school on a regular basis to have security software updated.
· Suspected or actual computer virus infection should be reported immediately to the SLT or technician.

Education and Training

In 21st Century society, staff and pupils need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond. The three main areas of Online Safety risk that your school needs to be aware of and consider are:

Area of Risk	Examples of risk
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising e.g. SPAM Privacy of information (data protection, identity fraud, scams, phishing) Invasive software e.g. Virus', Trojans, Spyware Premium Rate services Online gambling
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	Illegal materials Inaccurate/bias materials Inappropriate materials Copyright and plagiarism User-generated content e.g. YouTube, Flickr, Cyber-tattoo, Sexting
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying Contact Inappropriate emails/instant messaging/blogging Encouraging inappropriate contact

Online Safety Across the Curriculum

· Online Safety is part of the computing Curriculum (2014)
· Teaching and learning is progressive through planning and resourcing. Online safety is taught at specific times e.g. safer Internet Day, along with PSHE lessons and computing lessons through the year, or as a result of a specific incident.
· Content is age appropriate.

· Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
· Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
· Rules for Internet access will be posted in all rooms where computers are used.
· Pupils will be informed that Internet use will be monitored.
· Instruction in responsible and safe use should precede Internet access.
- Safe internet learning is taught through Online Safety as part of the computing curriculum. In addition to this Safer internet day is promoted in February as a whole school project.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Staff Awareness

- The Online Safety Champions will provide advice / guidance to all members of staff to ensure they are regularly updated on their responsibilities as outlined in this policy.
- The Online Safety Champions will provide advice/guidance or training to individuals as and when required.
- The Online safety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Online safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's Online safety Policy and Online safety agreements.
- Regular updates on Online safety Policy, Online safety agreements, curriculum resources and general Online safety issues are discussed in staff / TA meetings.

Raising Parents/Carers Awareness

'Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.' (Byron Report, 2008).
· The school offers external information sessions by CLEOP approved trainers for parents.
· Further information for parents is available on the school website.
· Information on eSafety is included in newsletters to parents.

Raising Governors' Awareness

Our school considers how Governors, particularly those with specific responsibilities for Online safety, ICT or child protection, are kept up to date. This is through discussion at Governor Meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

The Online safety Policy will be approved by the governing body and made available on the school's website. There is a Governor responsible for Online safety who will meet with our Online Safety Champions on a regular basis.

Created 11th March 2015
Reviewed: Autumn 2023
Next Review: Autumn 2024

Signed: L.D.Marshall

Liam Marshall - Deputy Headteacher

Online Safety Governor: *Peter Bennett*