



## Policy status

title:	Online safety policy 2015		
status:	Approved		
owner:	Head Teacher		
nominated governor:	Joyce White		
release date:	January 2015 ( reviewed Sep 15)	Valid until:	September 2016
Head teacher (signature if required):		Date:	
Chair of governing body (signature if required):		Date:	

---

## Preshute CE Primary School Online Safety Policy 2015-16

### 1. Leadership and Management

#### 1.1 Developing a policy

Our online policy has been written by the school, building on the Wiltshire online template policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

#### 1.2 Authorised Access

- The school receives Internet Service Provision (ISP) from South West Grid for Learning (SWGfL) and has a service which proactively monitors Internet usage for attempts to access illegal (child abuse and incitement for racial hatred) content and will notify the local police and Wiltshire Council in these instances.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance if a pupil's access is withdrawn.
- Upon starting the school parents and children are asked to sign the Responsible Use Policy and guidance for sound, image and video for publication online.
- In Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials wherever possible.
- Parents will be informed that pupils will be provided with supervised Internet access.

#### 1.3 Filtering and Monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to staff.

- As a result there is no member of the school community who is allowed unfiltered access to the internet.
- A designated member of staff (ICT coordinator) will review the popular permitted and banned sites accessed by the school.
- The school will work in partnership with parents, Wiltshire Council, DFE and its ISP to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider via the online safety lead (ICT co-ordinator or head teacher).
- Website logs will be regularly sampled and monitored by a nominee of the school and reported to the head teacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal, extremist or may place an individual at risk must be referred to the appropriate authorities i.e. Head teacher, LADO, Police, Internet Watch Foundation.

## 1.4 Risk Assessment

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- 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 Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

## 2. Teaching and Learning

### 2.1 The Curriculum

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, ensure wellbeing, to support the professional work of staff and to enhance the school's management information and business administration systems.

- Whilst Internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.
- The Internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

## 2.2 Enhancing Teaching and Learning

Benefits of using the Internet in education include:

- Access to a variety of worldwide educational resources.
- Inclusion in the National Education Network which connects all UK schools.
- Educational and cultural exchanges between pupils worldwide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments.
- Educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Access to learning wherever and whenever convenient.

## 2.3 Evaluating Content

- Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- If staff or pupils discover unsuitable site or content they consider to be inappropriate or extremist , the URL (address) and content should be reported to their ISP/SWGfL
- The school will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

# 3. Communication and Content

## 3.1 Website Content

- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- Written permission from individuals, parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will be selected carefully and will not enable individuals to be clearly identified.

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- The nature of all items uploaded will not include content that allows the pupils to be identified, either individually or through aggregated pieces of information.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

### **3.2 Managing e-mail**

- Pupils will only use emails through a class email account, when appropriate, and will not have personal email accounts.
- Where class email accounts are used for a project, school staff will monitor and moderate messages sent and received.
- Pupils should use email in an acceptable way. Sending images without consent, explicit images, messages that cause distress and harassment to others are considered significant breaches of school RUP and will be dealt with accordingly.
- E-mail sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.

### **3.3 On-line communications and Social Media.**

On-line communications, social networking and social media services may be filtered in school by their ISP but are likely to be accessible from home.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Schools have a key role to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private.

- Pupils will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be taught about the dangers of revealing personal details of themselves or others in online communication, including the tagging of photos or video, or to arrange to meet anyone.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and only operate with approval from the SLT.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

- No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.
- Parents wishing to photograph or video at an event should be made aware of the schools expectations and be required to comply with the schools RUP as a condition of permission to photograph or record.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Responsible Use Policy.
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.

### 3.4 Mobile Devices (Including Bring You Own Device-BYOD)

**Mobile devices** refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras.

The use of mobile devices is permitted in school, and is subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- Users have access to resources to support learning and teaching
- Users should be given clear boundaries on responsible and professional use
- Mobile devices that are brought in to school remain the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.
- School staff authorised by the Head teacher may search pupils or their possessions, and confiscate any mobile device they believe is being used to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.
- Sending abusive or inappropriate messages or content is forbidden by any user within the school community.
- Mobile devices may be used during lessons or formal school time as part of approved and directed curriculum based activity.
- Mobile devices are not permitted to be used in certain areas or situations within the school site e.g. changing rooms or toilets, situations of emotional distress etc.
- Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. admin e-mail account or school phone) In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP.
- Staff should be provided with school equipment for the taking photos or videos of pupils linked to an educational intention. In exceptional circumstances staff may need to use personal devices for such a purpose and when doing so, should ensure they comply with the school's Responsible Use Agreement.
- The school will take steps to monitor responsible use in accordance with the Responsible Use Policy

### 3.5 Video Conferencing

- Video conferencing may include FaceTime, Skype, Lync as well as other sites.

- Staff must refer to any Responsible Use agreements prior to children taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Pupils will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised.

### 3.6 Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

### 3.7 Cyber Bullying

**Cyber bullying** can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone” DCSF 2007.

Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school’s behaviour, anti-bullying and child protection policies, which should include:

- Clear procedures set out to investigate incidents or allegations of cyber bullying.
- Clear procedures in place to support anyone in the school community affected by cyber bullying.
- All incidents of cyber bullying reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school’s e-Safety ethos.

### 3.8 Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Schools will already have information about their obligations under the Act; this section is a reminder that all data from which people can be identified is protected. For advice and guidance relating to a contravention of the Act, contact [www.wiltshire.gov.uk](http://www.wiltshire.gov.uk)

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

## 4 Implementation

### 4.1 Policy in Practice - Pupils

- All users will be informed that network and Internet use will be monitored.
- Online Safety teaching should be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst pupils.
- Online Safety teaching will be included in PSHE, Citizenship and/or ICT and cover safe use at school and home.
- Online Safety rules and/or copies of the Responsible Use Policy will be on display in all rooms with Internet access.

- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

#### **4.2 Policy in Practice - Staff**

- The Online Safety Policy will be provided to and discussed with all members of staff and Responsible User protocols detailed and signed for compliance in the Code of Conduct.
- Staff should be aware that Internet traffic is monitored (and automatically reported by the SWGfL) and can be traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

#### **4.3 Policy in Practice - Parents**

- Parents' attention will be drawn to the Online Safety Policy and Responsible User Policy RUP in newsletters, school prospectus and Website.
- A partnership approach with parents will be encouraged. This could include offering parent evenings, demonstrations, practical sessions and suggestions for resources and safer Internet use at home.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

#### **4.4 Handling of complaints**

- Responsibility for handling incidents will be delegated to the ICT coordinator.
- Any complaint about staff misuse must be referred to the head teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.