Primrose Hill C of E Primary Academy

E Safety Policy

This Review	Next Review
January 2018	January 2019

Our E-Safety Policy has been written by the school E-Safety Lead and ICT Lead building on a variety of exemplar policies. It will be reviewed in light of the SWGfL model policy for E-Safety

Introduction

Roles and Responsibilities

E-Safety in the Curriculum

Password Security

Managing the Internet safely

Managing other Web 2 technologies

Mobile Technologies

Managing email

Safe Use of Images

Misuse and Infringements

Equal Opportunities

Parental Involvement

Writing and Reviewing this Policy

Acceptable Use Agreement: Staff, Governors and Visitors Acceptable Use Agreement: Pupils

Smile and Stay Safe Poster

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web- based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Primrose Hill C of E Primary Academy, we understand the responsibility to educate our pupils on E- Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones and portable media players, etc).

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety Lead in our school is the Head Teacher, Mrs Victoria Henson. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety Lead, in collaboration with the Computing subject leader, to keep abreast of current issues and guidance through organisations such as the Local Authority, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the ICT lead and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: safeguarding, health and safety, home–school agreements, social media policy and behaviour (including the anti-bullying) policy and PSHE.

E-Safety skills development for staff

Our staff receive regular information and training on E-Safety issues in the form of training from visiting experts and through attendance at relevant CPD.

New staff receive information on the school's Acceptable Use Policy as part of their induction.

All staff have been made aware of 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.

All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

Managing the school E-Safety messages

We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used. The e-safety policy is introduced to the pupils at the start of each school year. E-safety posters will be prominently displayed.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- The school has a framework for teaching internet skills in ICT lessons
- The school provides opportunities within a range of curriculum areas to teach about E-
Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
- Pupils are made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are informed about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- • All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-safety Policy.
- • Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- • If you think your password may have been compromised or someone else has become aware of your password report this to the E-Safety Lead.
- • Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended in a logged-on state.

In our school, all ICT password policies are the responsibility of the ICT lead and all staff and pupils are expected to comply with the policies at all times.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the South West Grid for Learning (SWGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously
been checked by the teacher. It is advised that parents recheck these sites and supervise
this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school
software or illegal software from other sources.

Infrastructure

School internet access is controlled through the LA's web filtering service.

- Primrose Hill C of E Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the nearest member of staff and to the E-Safety Lead as soon as possible.

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the class teacher or E-Safety Lead for a safety check first.

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the e safety lead.

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of cyber-bullying to the school.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. In special circumstances the school does allow a member of staff to contact a pupil or parent/ carer using their personal device.
- Pupils are not allowed to bring personal mobile devices/phones to school. In certain circumstances pupils may be given permission to have a mobile device in school and in such cases permission may be given by the class teacher on receipt of a written or verbal request from parent(s). If permission is given then the device is to be kept in a safe place by the class teacher.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community
is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- E-mails sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. All children use a class or group email address.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission. Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the E-Safety Lead if they receive an offensive e-mail.
- Pupils are introduced to email as part of the Computing Scheme of Work.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Publishing pupils' images and work

All parents/guardians will be asked to give permission to use their child's photographs in the following ways:

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc. Parents/carers may withdraw permission, in writing, at any time.

Pupils' surnames will not be published by the school alongside their image. Local press may insist on publishing photographs with full details of children. Permission for the press to publish these photographs must come from parents at all times. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Web Manager and Curriculum Lead have authority to upload to the site.

Webcams and CCTV

The school uses CCTV for security and safety. The only people with access to this are the head teacher and nominated office staff. Notification of CCTV use is displayed at the front of the school. We do not use publicly accessible webcams in school. Webcams in school are only ever used for specific learning purposes, i.e. monitoring birds' eggs and may sometimes include images of children or adults in school. Misuse of a webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).

Misuse and Infringements

Complaints

Complaints relating to E-Safety should be made to the E-Safety Lead or Senior Management Team. Incidents should be logged and follow-up action taken by the E-Safety Lead.

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Safety Lead.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety Lead, depending on the seriousness of the offence; investigation by the E-Safety Lead/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's E-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting E-Safety both in and outside of school. We aim to regularly consult and discuss E-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks. Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school E- Safety policy by informing the E-Safety Lead. Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child. Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website).

The school disseminates information to parents relating to E-Safety where appropriate in the form

of:

- Information and celebration evenings • Posters
- Website
- Newsletter items

Writing and Reviewing this Policy

Review Procedure

There will be an on-going opportunity for staff to discuss with the E-Safety Lead any issue of E- Safety that concerns them. This policy will be reviewed in light of the SWGfL model policy for E- Safety by the schools E-Safety Working Party. Consideration will be given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government changes the orders or guidance in any way.

Acceptable Use Agreement: Staff, Governors and Visitors Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school E-Safety Lead.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body
- I will not install any hardware or software without permission of the E-Safety Lead
- I will not browse, download, upload or distribute any material that could be considered
offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will ensure that my online activity, both in school and outside school, will not bring my
professional role into disrepute
- I will support and promote the school's E-Safety policy and help pupils to be safe and
responsible in their use of ICT and related technologies

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ..... Date .....

Full Name .....(printed)

Job Title……

KS1 Acceptable Use Agreement

These rules have been written to make sure that you stay safe when using the computers and other IT equipment. By using IT in school, you have agreed to follow these rules. Your teacher will talk to you about these rules before you take them home to talk through with your parents.

Name: _____ Class: _____

I agree that:

- ✓ I will be careful when using or carrying equipment.
- ✓ I will only use the equipment I have been given for the task the teacher has set.
- ✓ I will follow instructions for using the equipment carefully.
- ✓ I will remember to log off properly before shutting down computers.
- ✓ I will only use the internet when a teacher or other trusted adult is with me.
- ✓ I will be sensible when going on the internet by only looking at pages that the teacher has asked me to use.
- ✓ I will tell a trusted adult straight away if I see something I don't like
- ✓ I will keep my passwords secret, but I can tell my family. I will only log on using my own username.

Please read through these rules with your child and sign below to show that they understand and agree to abide by them:

Signed:_____(parent/guardian)

KS2 Acceptable Use Agreement

These rules have been written to make sure that you stay safe when using the computers and other IT equipment. By using IT in school, you have agreed to follow these rules. Your teacher will talk to you about these rules before you take them home to talk through with your parents.

Name: _____ Class: _____

I agree that:

- ✓ I will always keep my passwords a secret and will tell my teacher if I think someone else knows them.
- ✓ I will only use the internet and email when I have permission to do so.
- ✓ I will not tell anyone about myself online (this is my surname, home address, phone number, school address, school name, family information etc).
- ✓ I will not upload pictures or digital images of myself or others without my teacher's permission.
- ✓ I will minimise the screen and tell my teacher or another trusted adult if anything online or in a message makes me feel scared or uncomfortable.
- ✓ I will only create and share content that is legal.
- ✓ I will never meet an online friend without taking a responsible adult that I know with me.
- ✓ I will only access my own work and will never knowingly damage anyone else's digital work.
- ✓ I understand that the school may check my computer files and may monitor the Internet sites I visit.

Please read through these rules with your child and sign below to show that they understand and agree to abide by them:

Signed:_____(parent/guardian)