PIMLICO PRIMARY
LIBERTAS PER CULTUM

Online Safety Policy 2020-21

Introduction

Computing 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 computing within our society as a whole. Currently the Internet technologies children and young people are using include:

- Websites
  Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
  Podcasting (Audio Sharing) Video Sharing
  Music Sharing / Downloading Gaming
- Mobile / Smart phones with functionality including: text, video, web, audio, music, global positioning (GPS)
  Other mobile devices with similar functionality (tablets, laptops, gaming devices)

Whilst exciting and beneficial both in and out of the context of education, much computing, 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. Ensuring children and young people are aware of the risks associated with the use of technologies, and can adopt safer behaviours, is vital in safeguarding them against cyber- bullying and grooming.

At Pimlico Primary whilst we do not teach Computing as a subject, we understand the responsibility to educate our pupils on Online 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.

This policy relates to both fixed and mobile Internet technologies provided by the school, and technologies owned by pupils, parents and staff, but brought onto school premises.

Roles and Responsibilities

As is an important aspect of strategic leadership within the school, the Principal and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety co-ordinator in our school is Shahid Sahil and Sheena Clark who has been designated this role. They report to Miss Blain who is the Designated Safeguarding Lead. It is the role of the co-ordinator to keep abreast of current issues and guidance through organisations such as Westminster LA, CEOP (Child Exploitation and Online Protection), UKCCIS, and Childnet.

Senior Management and Governors are updated by the Principal / co-ordinator 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, and visitors (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, and behaviour/pupil discipline (including the anti- bullying) policy and particularly to the curricular for PHSE and RSE.

Skills development for staff

- our staff receive regular information and training on Online Safety issues in the form of updated Acceptable Use policy
- new staff receive information on the school's Acceptable Use policy as part of their induction
- all staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of and know what to do in the event of misuse of technology by any member of the school community
- all staff are expected to incorporate activities and awareness within the PSHE and RSE curriculum areas.

Managing the school Online Safety messages

- we endeavour to embed messages across the curriculum whenever the Internet and/or related technologies are used. This is particularly reinforced in PSHE and RSE lessons in relation to cyber-bullying and to grooming.

Computing in the Curriculum

Computing is not taught at Pimlico Primary, currently.

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.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Policy.
- Users are provided with an individual network username.
  Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left logged / are locked.
- In our school, all staff are expected to comply with the policies at all times.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the Principal.
- Any data taken off the school premises must be encrypted.

The school network is back up internally by our Trust IT department.

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

- Raw image searches (e.g.: Google image search) are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested. These will have 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.
- All users must observe copyright of materials from electronic resources.

Pimlico primary 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) 7 Regulations 2000, Regulation of Investigatory Powers Act 2000,

Human Rights Act 1998.

Staff are aware that school based email and Internet activity can be monitored. The school uses management control tools for controlling and monitoring workstations. If staff discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the IT department.

Pupils and staff are not permitted to download programs or files on school equipment, these are controlled by the Trust IT department

If there are any issues related to viruses or anti-virus software, Trust IT department should be informed through the office administrator.

Managing other Communication & Networking technologies

The Internet includes a wide range of communication and networking tools & sites. Children need to be educated about appropriate ways of communicating and about the risks of making personal information too easily available. If used responsibly both outside and within 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.

- At present, the school does not teach computing, we do have lessons on online safety in Safer Internet Week (usually early in Spring term)
- 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.
- Pupils are asked to report any incidents of bullying to the school.

Staff understand that it is highly inappropriate to use social networking sites and other personal communication tools with pupils and / or parents (e.g.: Facebook, Instagram, Twitter, email etc.).

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, Smart phones, Tablets etc.) are familiar to children outside of school. Allowing such personal devices to access the school network can provide immense benefits in collaboration, but also create risks associated with misuse, inappropriate communications, etc. Emerging technologies will be examined for educational benefit and the risk assessed before such use of personal devices is facilitated in school. 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)

- Only under extreme circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device but they should always dial 141 to block their number first.
- Pupils in year 6 are allowed to bring personal mobile devices/phones to school but must hand them in at the office every morning. At all times, the device must be switched to silent mode.
- Technology may be used, for educational purposes, as mutually agreed with the Principal. The device user, in this instance, must always ask the prior permission of the bill payer.
- 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; video or sound recordings are made on these devices of any member of the school community.
- Capturing images & video is not allowed by students / staff unless on school equipment and for educational purposes.
- 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; video or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies (e.g.: phones, laptops, etc.) for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop, tablet for staff, only this device may be used to conduct school business outside of school.

Sexting

In January 2017, the UK Council for Child Internet Safety (UKCCIS) published the comprehensive 50-page guidance document Sexting In Schools This document, created by many expert agencies and with the backing of the Department for Education, has everything that designated safeguarding leads, principals and other senior school leaders need to deal appropriately with incidents of sexting, from legal advice and prevention to education tools, flowcharts for responding to incidents, research and analysis tool and aids for staff training.

Managing email

The use of email within most schools is an essential means of communication for staff. 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 be aware of what constitutes good 'netiquette'. In order to achieve computing level 4 or above, pupils must have experienced sending and receiving emails.

- The School gives all staff an individual outlook account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and that 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. Staff mail should be used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school. The responsibility for adding this disclaimer lies with the account holder.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations or parents are advised to send via the designated office account.
- All email 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 email communication, or arrange to meet anyone without specific permission.
- Staff must inform IT department if they receive an offensive email.

Safe Use of Images / Video

Taking of Images and Video

Digital images / video are easy to capture, reproduce and publish and, therefore, easily 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 / video by staff and pupils with school equipment.
- Staff are not permitted to use personal devices, (e.g.: mobile phones, tablets and cameras), to record images of pupils, this includes when on field trips. However with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the schools network and deleted from the staff device.

Consent of adults who work at the school

- Permission to use images / video of all staff who work at the school is sought on a regular basis and a copy is located in the personnel file
- Parents must seek permission to take photos / video school events, and must agree to NOT post images / video on the Internet.
- Parents are requested NOT to video school performances. Video are captured ONLY by school staff and are stored on the school system

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos/ video in the following ways:

- on the school website
- 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, i.e. exhibition promoting the school
- general media appearances, e.g. 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, e.g.: divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. Email 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 has authority to upload to the public website

Storage of Images / Video

- images/ video of children are stored on the school's network
- staff are not permitted to use personal portable media (e.g.: USB storage devices) for storage of images without the express permission of the Principal
- Rights of access to this material are restricted to the teaching staff within the confines of the school network
- Images / video of pupils are deleted when pupils leave the school.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the Principal, DSL and the office Manager. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school other than for special projects such as nature cams which are streamed to the web.
- Webcams in school are only ever used for specific learning purposes, (e.g.: monitoring hens' eggs) Images of children / adults ever never broadcast.
- 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)
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

The school's Relationships & Sex Education curriculum (RSE) provides a set of preventative tools which help safeguard pupils against cyber-bullying and grooming. The school has a comprehensive RSE policy in place which includes the appropriate teaching & learning of:

- Private and personal space
- Appropriate / safe and inappropriate / harmful relationships

- Consent

Misuse and Infringements

Complaints

Complaints relating to Online Safety should be made to the Principal and the IT department. Incidents should be logged and process should be followed.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the IT department.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the IT department and depending on the seriousness of the offence may lead to:
    - Reporting to the Child Protection / Safeguarding Manager
    - Investigation by the Principal / LA
    - Immediate suspension
    - Dismissal Involvement of police

Equal Opportunities

Pupils with additional needs

The school endeavours work in partnership with parents to convey a consistent message to all pupils. This in turn should aid the establishment and future development of the schools' rules. Staff are aware that some pupils will require additional reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting both in and outside of school while appreciating the benefits provided by technologies generally. We regularly consult and discuss with parents/ carers and seek to promote a wide understanding about the link between and safeguarding.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school policy through questionnaires
- 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 where appropriate in the form of:
    - Information and celebration evenings
    - Website posting
    - Newsletter items

Reviewing this Policy

Review Procedure

This policy will be reviewed regularly and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change orders or guidance in any way. An appendix will be added for Staff acceptable use.