PERRYFIELDS PRIMARY PRU

E-Safety Policy

Review Date	Reviewed Date	Reviewer	Action
September 2017	**22.09.17**	**Staff**	**Ratified by Management Committee: 17.10.2017**
September 2018			

Our Vision

Perryfields embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, we aim to provide a safe and secure environment, which not only protects all people on the premises, but also educates them on how to stay e-safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies, owned and supplied by the school, and to personal devices owned by adults and young people whilst on the school premises.

Related Documents:

- Acceptable Use Policy
- Data Protection Policy
- Behaviour Policy
- Anti-bullying Policy
- Safeguarding Policy

Publicising e-Safety

To communicate the e-Safety Policy we will:

- make this policy, and related documents, available on the school website;
- introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year when it is updated;
- post relevant e-Safety information in all areas where computers are used.
- provide e-Safety information at parents' evenings and through the school newsletter and website.

Roles and Responsibilities

The Head and Management Committee have the ultimate responsibility for establishing safe practice and managing e-Safety issues at our school. There is an e-Safety Leader (currently the ICT Leader), who is responsible for policy review, risk assessment and e-Safety in the curriculum. The e-Safety Leader is the central point of contact for all e-Safety issues and will be responsible for day to day management. The current members of the strategic group are: the Head Teacher, ICT Leader and the ICT Technician.

All adult members of the school community have certain core responsibilities within and outside the school environment. They should:

- follow the e-Safety policy;
- use technology responsibly, as stated in the Acceptable Use Policy;

- accept responsibility for their use of technology;
- model best practice when using technology;
- report any incidents to the e-Safety Leader/Head Teacher using the school procedures;
- understand that network activity and online communications are monitored, including any personal and private communications made via the school network;
- be aware that in certain circumstances, where unacceptable use is suspected, enhanced monitoring and procedures may come into action;
- Check that any computer they are using has the latest updated Anti-Virus software installed before accessing the Internet/e-mails.

Physical Environment/Security

The school endeavours to provide a safe environment for the whole community, reviewing both physical and network security regularly, monitoring who has access to the system and consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly;
- Central filtering is provided and managed by IBS. All staff and students understand that if an inappropriate site is discovered, it must be reported to the e-Safety Leader who will report it to IBS;
- Requests for changes to the filtering will be directed to the e-Safety Leader in the first instance, who will forward these on to IBS, as appropriate.
- The Head Teacher controls access to inappropriate sites;
- The school uses firewall and monitoring software on all school owned equipment to ensure compliance with the Acceptable Use Policy;
- Pupils' use is monitored by the Head Teacher, ICT Leader and the ICT Technician;
- Staff use is monitored by the Head Teacher, ICT Leader and ICT Technician;
- All staff are issued with their own username and password to access network resources, which they must not share with others. If they suspect misuse, they must change their password immediately and report to the Head Teacher, ICT Leader and/or ICT Technician;
- Pupils have their own username to access network resources.

Mobile / Emerging Technologies

All Teaching staff are allocated a laptop/I-Pad. This is for their professional role in school, educational/school administrative use and staff's own professional development. All staff must understand that the Acceptable Use Policies apply to this equipment at all times.

To ensure the security of the school systems, personal equipment (laptops, tablets, memory sticks, external hard drives, etc.), is generally not permitted to be connected to the school network, unless formal approval has been sought from the Head Teacher and the ICT Leader. To ensure the security of the school systems, personal equipment will need to be swept for viruses before it is connected to the school

network and each time is it taken forth and back. The school's Acceptable Use Policy will also apply to this equipment.

The school will allocate staff a memory stick, should they feel they need one for their professional role in school, which should to be encrypted. As per the statement above, personal devices are not permitted unless formal approval has been sought from the Head Teacher and the ICT Leader.

Staff should use their own mobile phones sensibly and in accordance with school mobile phone policy. Pupils must hand phones and gaming devices to their class teacher to be locked in the class stock room, until returned at the end of the school day. Pupils' phones must be switched off, at all times, on school premises. The Educations and Inspections Act 2006 grants the Head Teacher the legal power to confiscate mobile devices, where there is reasonable suspicion of misuse, and they will exercise this right at their discretion.

Pictures/videos of pupils and staff (in their school role capacity) must not be taken on personal devices. Visiting teachers/visiting adults/students are not allowed to take pictures/videos on personal devices, unless permission has been sought from the relevant shareholders.

New technologies are evaluated for their educational benefits and risk assessed, by the ICT Technician, ICT Leader and Head Teacher, before they are introduced to the school community.

E-Mail

The school e-mail system is provided, filtered and monitored by IBS.

All staff are issued a school e-mail address, which must be used for all professional communication. Any correspondence with third parties must be done to recipient's official work email address.

When sensitive information is involved, it should be attached as a password protected/encrypted file and not written within the body of the message. The password for this attached file(s) should not be revealed within the same message - instead revealed over the phone to the person directly or through a separate message.

Key Stage 1 pupils may be given access to class based e-mail accounts that are monitored by the class teacher. Keys Stage 2 pupils may be given (where necessary and required by the school ICT/Computing curriculum) a school e-mail address that can be used for class-based activities. Parents and carers will be informed if this is going to take place.

Where appropriate, all pupils can be given a school e-mail address that can be used for educational purposes. Parents and carers will be informed if this is going to take place.

Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication. Guidance is given to the school community around how e-mail should be structured when using school e-mail

addresses. Staff and pupils are not allowed to access personal e-mail accounts on the school system.

Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher and e-Safety Leader, as soon as possible.

Published Content

The Head Teacher takes responsibility for content published on the school web site. The teachers are responsible for the editorial control of work published by themselves and their students (when necessary and appropriate). The school will hold the copyright for any material published on the school website or will obtain permission from the copyright holder, prior to publishing, with appropriate attribution.

The school encourages the use of e-mail to contact the school. The school does not publish any contact details for the pupils or staff.

The school encourages appropriate, educational use of other Internet sites, and where possible, embeds these in the school website.

Digital Media

We respect the privacy of the school community and will obtain written permission from staff, parents/carers for pupils before any images or video are published or distributed outside the school. Photographs will be published but not identify any individual pupil. Students' full names will not be published outside the school environment.

Written permission will be obtained from parents or carers, prior to pupils taking part in any external video conferencing. Although not currently used, Students must have their teacher's permission to make or answer a video conference call if this facility becomes available. Supervision of video conferencing will be appropriate to the age of the pupils.

Social Networking and Online Communication

The school is constantly reviewing the use of social networking sites and online communication, and currently does not allow any access to Social Networking Sites. Most popular sites are currently blocked through the IBS monitored filtering system. Perryfields will provide guidance to the school community on how to use these sites safely, and appropriately, in the home environment, via the school website, leaflets and newsletters. This includes:

• not publishing personal information;

• not publishing information relating to the school community;

• how to set appropriate privacy settings;

• how to report issues or inappropriate content.

Unmoderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of

such sites at home via e-Safety lessons, through their Computing curriculum, assemblies etc. Information pertaining to the above is provided to relevant shareholders at relevant times in a child's school career.

Staff are advised of the risks of putting private information into a public domain and also 'bringing school into disrepute' through the private use of social networking sites. For the safety and the protection of all relevant parties, staff should NOT add/accept school pupils as friends on social networking sites.

Parents are advised that social networking sites should not be used as an inappropriate forum, regarding school matters. If there is an issue, please raise it with school, using the appropriate channels. If it is felt that there is inappropriate usage, then school will seek advice from Legal Services. In extreme cases, Criminal proceedings could ensue.

Educational Use

All School staff must model appropriate use of school resources, including the internet. All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material. Where appropriate, links to specific web sites will be provided instead of open searching for information. Students will be taught how to conduct safe searches of the internet, when appropriate, during ICT/Computing lessons. Where pupils are allowed to freely search the Internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the children visit.

Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Policy before any activity. Teachers will check the suitability of sites before using them on an interactive whiteboard.

Staff and students will be expected to reference all third party resources that are used; plagiarism is to be discouraged.

Pupil Responsibilities

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. e-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited - this will cover both the use of ICT and new technologies in school and outside school;
- key e-Safety messages should be reinforced as part of a planned programme of assemblies or lessons;

- Pupils should be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school;
- Pupils (KS1/2) and parents will sign an Internet/acceptable use policy;
- Pupils will be advised never to give out personal details of any kind, which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, e-mail addresses, full names of friends/family, specific interests and clubs etc.
- Pupils understand and follow the school e-safety and Acceptable Use Policy (AUP);
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Pupils will be informed that network activity use will be monitored
- Instruction in responsible and safe use should precede Internet access.
- Use of aged related website , apps and software

Staff Responsibilities

- All staff must accept the terms of the 'Worcestershire Code of Conduct'
- Staff will ensure they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP).
- Staff should be aware that network traffic (including the Internet), can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by the Head Teacher.
- All staff need have an up to date awareness of the current school e-safety policy and practices.
- Staff must report any suspected misuse or problem to the ICT Leader, DSL, Head Teacher for investigation/action/sanction.
- Digital communications with pupils should be on a professional level and only carried out using official school systems.
- Staff are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices, monitoring their use and implementing current school policies with regard to these devices.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction; safe and professional behaviour will be outlined as part of induction procedures.

E-Safety Training

- Perryfields has a programme of continuing professional development in place that includes whole school INSET, in-school support, consultancy and course attendance (where appropriate).

- There is an induction process and mentor scheme available for new members of staff.
- Educational resources are reviewed by Curriculum Leaders and disseminated through curriculum meetings/staff meetings/training sessions.
- e-Safety is embedded throughout the school curriculum and visited by each year group.
- Pupils are taught how to validate the accuracy of information found on the Internet.
- We recommend parents apply their own age appropriate controls at home.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available, in line with the Data Protection Act 1998, which states that personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- kept no longer than is necessary;
- processed in accordance with the data subject's rights;
- secure;
- only transferred to others with adequate protection.

Data is stored on the school systems and transferred in accordance with LA Guidelines. Wider Community/Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and passwords that will be recorded in the school office, and only have access to appropriate content. Students/ volunteers can only access a limited amount of content in a designated student area on the school system.

Equal Opportunities

This e-Safety policy works in conjunction with the school Disability, Equality and Accessibility policy. Perryfields will take all reasonable measures to ensure that all children have suitable access to ICT.

Responding to Incidents

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

- If any apparent or actual misuse appears to involve illegal activity, i.e. Child sexual abuse images;
- Adult material which potentially breaches the Obscene Publications Act;
- Criminally discriminatory or prejudicial material;
- Other criminal conduct, activity or materials.

Any inappropriate use of the school's resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying, Safeguarding. Any suspected illegal activity will be reported directly to the police. IBS' service desk will also be informed to ensure that the Local Authority can provide appropriate support for the school.

Breaches of this policy by staff will be investigated by the Head Teacher. Action will be taken under Worcestershire LA's Disciplinary Policy, where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files, with the ultimate sanction of dismissal reserved for the most serious of cases involving gross misconduct.

All monitoring of staff use will be carried out by at least two senior members of staff. Breaches of policy will be recorded and held in school personnel files.

Student policy breaches relating to cyber bullying, must be reported to the Headteacher and if necessary, to the Designated Senior Leader for Child Protection (DSL). Action will be taken in line with the school Behaviour/Antibullying and Safeguarding policies. There may be occasions when the police must be involved.

Serious breaches of this policy by students will be treated as any other serious breach of conduct in line with the school's Behaviour Policy. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files, with the ultimate sanction of exclusion reserved for the most serious of cases.

Minor student offences, such as being off-task, visiting games or email websites, will be handled by the teacher in situ by invoking the school behaviour policy.

Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head Teacher.

Although Cyber bullying outside of school is not the direct responsibility of the school, if incidents are reported to school, we will contact the Parents/Carers concerned and the police, if we think a crime has been committed. We are responsible for educating our pupils in how to keep themselves safe both in school and outside the school environment. This includes e-Safety. The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.