Pensilva Primary School

E-Safety Policy

Statement

At Pensilva Primary School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives. Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

The DfE created a new version of their child protection and safeguarding statutory guidance, ‘Keeping Children Safe in Education’, which was released in September 2016.

The guidance contains additional information and clarification related to E-safety, including:

- A new section dedicated to online safety; it sets out how schools should ensure that appropriate filtering and monitoring systems are in place, and that such systems should be able to identify pupils accessing or trying to access, harmful or inappropriate material.
- Rewording from “should consider” to “should ensure” with regards to how schools will teach their pupils about safeguarding, including online.
- Clarifying that whilst it is important for schools to ensure that appropriate filters and monitoring systems are in place, “over blocking” should not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.
- Stating that ‘the use of mobile technology’ should be included in schools’ child protection and safeguarding policies.

Legal framework

This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 1998
- The Regulation of Investigatory Powers Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006

This policy also has regard to the following statutory guidance:
DfE (2015, updated 2016) ‘Keeping Children Safe in Education’

Use of the internet

The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for schools to implement, which minimise harmful risks.

When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful.

These risks include the following:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

Roles and responsibilities

It is the responsibility of all staff to be alert to possible harm to pupils or staff, due to inappropriate internet access or use within school and an awareness of safe use outside of school, and to deal with incidents of such as a priority. The school has established a procedure for reporting incidents and inappropriate internet use, either by pupils or staff. A copy of these procedures and forms are available in the staffroom (safeguarding concern form). The Headteacher will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

The E-Safety Co-ordinators Mrs L Halliday and Mrs J Thomas are responsible for ensuring the day-to-day e-safety in our school and managing any issues that may arise. The E-Safety Co-ordinators will regularly monitor the provision of e-safety in the school and will provide feedback to the Headteacher and reports to the Governing Body. The safeguarding/E-Safety governor will hold termly meetings with the E-Safety Co-ordinator to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

The Headteacher is responsible for ensuring that relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff. The Headteacher will ensure there is a system in place which monitors and supports the E-Safety Lead (regular meetings with the E-Safety Coordinators and ICT4), whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements. The Headteacher, along with the E-Safety Coordinators is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

Staff are expected to use social media sites in accordance with the school's Code of Conduct. However, where no other alternative presents itself and it is sufficiently necessary to outweigh the need for privacy, social media use by staff may be monitored by the Headteacher. The member of staff who is being monitored will be consulted prior to any interception by the school.

Cyber bullying incidents will be reported in accordance with the school's Behaviour and Anti-Bullying Policy.

The Headteacher and E-Safety Co-ordinators will evaluate and review this policy on a annually, taking into account the latest developments in legislation, ICT and feedback from staff/ pupils. These amendments will be presented to the Safeguarding Governor and E-Safety Governor and its committee. The full governing body will evaluate and review this E-safety Policy on an annual basis, taking into account the latest developments in ICT and the feedback from staff/pupils. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.

All staff and pupils will ensure they understand and adhere to our Acceptable Use Policy, which they must sign and return to the Headteacher. Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

E-safety control measures

Educating pupils:

An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school. Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material.

Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism. Clear guidance on the rules of internet use will be presented in all classrooms and in the home school agreement. Pupils are instructed to report any suspicious use of the internet and digital devices.

Educating staff:

All staff/governors will undergo annual e-safety training in addition to Tier 2 Safeguarding, to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole. This could be more frequent if changes relevant to e-safety become apparent.

The staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

Staff will be educated on which sites are deemed appropriate and inappropriate and will receive emails/newsletters highlighting any key changes. They are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

Any new staff are inducted and as part of this induction process they are required to undergo e-safety training (incorporated within Tier 2 Safeguarding training), ensuring they fully understand this E-safety Policy as well as understand and adhere to our Acceptable Use Policy, which they must sign and return to the Headteacher.

Internet Access:

Internet access will be authorised once parents and pupils have returned the signed consent form as part of our Acceptable Use Policy. A record will be kept by the school office of all pupils who have been granted internet access.

All users will be provided with usernames and passwords, and are advised to keep this confidential to avoid any other pupils using their login details. Pupils' passwords and their activity is monitored by the E-Safety Co-ordinators.

Any requests by staff for websites to be added or removed from the filtering list will first be authorised by the Headteacher.

All school systems are protected by up-to-date virus software. All temporary users, e.g. volunteers are required to have read the E-Safety Policy at the point of induction and will be given instructions by the E-Safety Co-ordinators as to the access of the internet during their time at the school. The master users' passwords will be available to the Headteacher for regular monitoring of activity.

Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times, in accordance with the school's Code of Conduct.

Personal use will be monitored by the Headteacher for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy or in cases where personal use impinges on working hours. Inappropriate internet access by staff may result in the staff member having access removed and could lead to disciplinary action.

Email

Staff will be given approved email accounts and are only able to use these accounts for school purposes. Use of personal email to send and receive personal data or information is prohibited. Any sensitive personal data shall only be sent to staff internally with encryption. No data of a sensitive nature must be sent to any external email addresses. Chain letters, spam and all other emails from unknown sources should be deleted without opening.

Social Networking

Use of social media on behalf of the school will be conducted following the processes outlined in our Staff Code of Conduct. Access to social networking sites will be filtered as appropriate. Should access be needed to social networking sites for any reason, this will be monitored and controlled by the Computing Co-ordinator and must be first authorised by the Headteacher.

Pupils are regularly educated on the implications of posting personal data online, outside of the school. Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole. Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.

Staff are not permitted to publish comments about the school which may affect its reputability. Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the Headteacher prior to accessing the social media site

The School website and published content including images.

The Headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate. All contact details on the school website will be the phone, email and address of the school. No personal details of staff or pupils will be published, unless by prior consent, with only first names of pupils used.

Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted unless a parent has agreed at the start of the pupils school career. Pupils are not permitted to take or publish photos of others without permission from the individual.

Staff are able to take images, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment. Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile Devices and Handheld Computers

Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the E-Safety Co-ordinators when using these on the school premises.

The sending of inappropriate messages or images from mobile devices is prohibited. Mobile devices must not be used to take images or videos of pupils or staff. The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

Virus Management

Technical security features, such as virus software, are kept up-to-date and managed by the school’s computing technicians, ICT4.

The E-Safety Co-ordinators must ensure that the filtering of websites and downloads is up-to-date and monitored.

Cyber Bullying

For the purpose of this policy, “cyber bullying” is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.

The school recognises that both staff and pupils may experience cyber bullying and will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online. The school aims to create a learning and teaching environment which is free from harassment and bullying.

The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Behaviour and Anti-Bullying Policy. The Headteacher will decide whether it is appropriate to notify the police.

Reporting Misuse

Misuse by pupils:

Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use. Any instances of misuse will be logged and reported to the E-Safety Co-ordinators who will then report this to the Headteacher, preferably in writing. Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will be suspended from using it and a record will be kept and parents informed.

Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the E-Safety Co-ordinators. Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection Policy.

Misuse by staff:

Any misuse of the internet by a member of staff should be immediately reported to the Headteacher preferably in writing. The Headteacher will deal with such incidents in accordance with the Allegations Against Staff Policy, and may decide to take disciplinary action against the member of staff. The Headteacher will decide whether it is appropriate to notify the police or the LADO (Local Authority Designated Officers) of the action taken against a member of staff.

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√						√	
Use of mobile phones in lessons				√				√
Use of mobile phones in social time	√							√
Taking photos on mobile phones or other camera devices				√				√
Use of hand held devices eg PDAs, PSPs		√					√	
Use of personal email addresses in school, or on school network		√						√
Use of school email for personal emails				√				√
Use of chat rooms / facilities				√				√
Use of instant messaging		√						√
Use of social networking sites	√							√
Use of blogs	√					√		

Date agreed with Governors	
Approved by Headteacher	
Chair of Safeguarding Committee	
Chair of Governing Body	
Date of next review	