Pensilva Primary School

Online 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 aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

The governing body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Alex Hunt.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- Do all they can to limit children's exposure to risks from the school's IT systems.
- Ensure the school has appropriate filtering and monitoring systems in place and regularly review their effectiveness.
- Ensure that the leadership team have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. 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 Online Safety Lead (regular meetings with the Online Safety Lead 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 Online Safety Lead is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

The Designated Safeguarding Lead (DSL)

Details of the school's DSL are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, computing lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board.

Computing Lead

The computing lead is responsible for:

- In coordination with NCI, putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- In coordination with ICT4 ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Reviewing the online safety policy on an annual basis and providing a copy to the headteacher and governors to agree.

All staff

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.

All staff, including agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Employing methods of good practice and acting as role models for pupils when using the internet and other digital devices
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy. A safeguarding concern form is available in the staffroom
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

Parents will get communications in the newsletter to reinforce the importance of being safe online. A list of sites that children may accessing through the delivery of our computing curriculum can be found in appendix A of this policy.

Any visitors or members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum on a regular basis and as part of Safer Internet Day which is usually in February of every year:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Cyber-bullying

Definition:

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying:

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, and health education (PSHE), and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also puts any available information/leaflets on cyber-bullying on the school website for parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Internet access will be authorised once the signed consent form as part of our Acceptable Use Policy has been returned to the school. 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.

Any requests by staff for websites to be added or removed from the filtering list will first be authorised by the Headteacher. The master users' passwords will be available to the Headteacher for regular monitoring of activity.

Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

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 Lead 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 must not post 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.

Virus Management

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

Passwords and security

Recent data breach reports say that 63% of hackers take advantage of weak passwords. What's more, almost all (93%) took mere minutes to compromise systems. It is, therefore, very important that the best possible practices are followed for the use of our various system accounts and passwords.

The following password points must be followed to ensure that Pensilva Primary School's systems and applications are kept secure and that we continue to meet the requirements of the UK General Data Protection Regulations (GDPR) and other applicable UK data protection law and security legislation.

Strong passwords

Passwords should be of a minimum length of eight characters and should include a mix of uppercase, lowercase, numbers and symbols. Do not use sequences of characters (123, abc etc.) and try and spread the mix of character types through the password.

Password tips

Create a unique acronym for a sentence or phrase you like and then include phonetic replacements, such as 'Luv 2 Laf' for 'Love to Laugh.'

Don't reuse passwords

The passwords you use to access School / Academy Name systems and accounts should be unique. NEVER use the same password for other systems, services, website or apps.

Don't make a password 'personal'.

Do not include your name or date of birth – or any other personally identifiable information.

Avoid abbreviations and acronyms.

Never use these as a shortcut within a password to identify your department or role – 'admin', 'head' or 'SENCO' for example.

Avoid dictionary words.

Don't use real words – hackers have programs that can search through tens of thousands of dictionary words.

Google

Don't search the web for such as "strong password example" and use one that you find (and don't use the 'Luv 2 Laf' example above!)

Storing passwords

Never write your password down, especially not anywhere near your computer. Do not store your password in a plain text file on your computer.

Sharing passwords

Do not share your password with other users and never send a password by email.

Staff using work devices outside of school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the Computing Lead and ICT4.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and Acceptable Use Agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance

with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training
All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required.
By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.

	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	