



Birdham CE Primary School

ONLINE SAFETY POLICY

Introduction

A safe electronic environment is not purely a technological issue. The responsibility for online safety must **not** be solely delegated to technical staff, or those with a responsibility for IT. This then makes that responsibility rest with of all those who work with young people whether in a paid or unpaid capacity.

Aims

- to create a safe environment where we can both work and learn. This environment should be safe for both young people and adults alike.
- to embed online safety within all safeguarding policies and practices.

Education

The education of young people is key to them developing an informed confidence and resilience that they need in the digital world.

The National Curriculum programme for IT at Key Stages 1 to 2 makes it *mandatory* for children to be taught how to use IT safely and securely. Together these measures form the basis of a combined learning strategy that can be supported by parents, carers, and staff working with children.

Educating young people in the practice of acceptable use promotes responsible behaviour and builds resilience. To support this, the following procedures are in place:

- online safety rules are posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils are informed that network and internet use will be monitored and appropriately followed up.
- online safety training will be embedded within the Computing scheme of work or the Relationship and Sex, Health Education (RSHE) curriculum.

We cannot realistically provide solutions to each and every potential issue arising in a rapidly changing world. As a result, young people must be able to transfer established skills and safe working practices to any new online activities they encounter.

We recognise that it is equally important to ensure that the people who care for young people should have the right information to guide and support young people whilst empowering them to keep themselves safe.

Policies

This policy sits beside many key documents. These include, but are not limited to:

- the Acceptable Use Policy (AUP);
- the TrustNET internet Filtering Policy;
- RSHE policy;
- Behaviour policy; and anti-bullying guidance;
- Use of AI in School Policy
- Safeguarding and Child Protection Policy
- photographic images of children guidelines; the staff guidance for the safer use of the internet; staff handbook and code of conduct for staff

Writing and reviewing the Online Safety policy

- The Computing subject leader (with support from the IT Technician) includes the role of online safety. They work closely with the member of staff responsible for Safeguarding and Child Protection. N.B. The online safety role is not a technical role.
- Our Online Safety Policy has been written by the school, building on the West Sussex online safety Policy and government guidance. It is shared with relevant staff and approved by governors.

Teaching and learning at Birdham CE Primary School

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
- internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. internet use will enhance learning
- Birdham 's internet access has been designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils are taught what kind of internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils are shown how to publish and present information to a wider audience. Pupils are taught how to evaluate internet content
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to crosscheck information before accepting its accuracy.
- Pupils are taught to report unpleasant internet content to the Headteacher, or their class teacher who will share this information with the online safety Lead so that a path of action can be agreed.

Managing internet Access and Information system security

- School IT systems security are reviewed regularly.
- Virus protection is updated regularly.
- Personal data will be recorded, processed, transferred and made available according to all GDPR legislation.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

E-mail

- Pupils do not use e-mail accounts on the school system.
- Pupils will learn about sending and receiving emails as part of the Computing curriculum.
- The school does allow e-mail from pupils to external bodies unless the classteacher has explicitly approved it.

Published content and the school web site

- Pupils details are not available on the website.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully with the permission of parents/guardians.
- Pupil's full names will not be used with their photographs anywhere on the school Website or other online space.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. Social networking and personal publishing
- The school filters do not allow access to major social networking sites.
- Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils are advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school works with TrustNET and other online safety sites to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported to the online safety Coordinator.
- Pupils will work with a supervising teacher when making or answering a video conference call.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. See our Use of AI in School policy
- The school understands that technologies such as mobile phone can present a new route to undesirable material and communications. Pupil mobile phones are not permitted in school.
- The sending of abusive or inappropriate messages is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- The use of our Learning Platform, J2E, is reviewed as needed.

Authorising internet access

- All staff must read and sign the "Staff AUP Agreement for IT" before using any school IT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents of pupils will be asked to sign and return a consent form. "Acceptable Use Agreement" before being allowed to access the internet.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor WSCC can accept liability for any material accessed, or any consequences of internet access.
- The school will audit IT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is fit for purpose.

Handling online safety complaints

- Complaints of internet misuse will be dealt with by a senior leader.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints against the curriculum policy).
- Pupils and parents will be informed of any pupil misuse of the internet.

Introducing the online safety policy to pupils

- online safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and internet use will be monitored and appropriately followed up.
- online safety training will be delivered as part of the Computing and PSHE curriculum.

Staff and the online safety policy

- Staff must be informed that network and internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor IT use will be supervised by the Headteacher and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

External media on portable devices

- Staff and children should be aware of the associated risks of connecting devices to networks outside the school, and the possible harm that any downloaded files might bring.