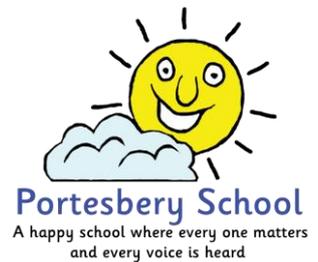


Online Safety Policy

Reviewed: **February 2022**

Review period: **2 yearly**

Review date: **Spring 2024**



Online Safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour, safeguarding, data handling and the use of images.

Using this policy

- Our Online Safety policy has been written by the school, building on best practice and government guidance. It has been agreed by the senior leadership team and approved by governors.
- The Online Safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The Online Safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Teaching and Learning

- The school has a duty to provide pupils with safe, high quality internet access as part of their learning experience and to provide staff and visiting professionals access in order to carry out their roles.
- We will enable pupils to communicate using a range of relevant technologies including Augmentative and Alternative Communication (AAC) devices such as iPads and other tablets or portable computers.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform Online Safety policy.
- The security of school IT systems will be reviewed regularly.

- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.
- Individuals should keep their user log in and email details confidential and NOT share this information with any other user.
- Individuals should always either lock their computer screen or log out of their account when leaving their computer for any period of time.

Internet Use

The school will provide an age-appropriate/developmentally appropriate Online Safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff and pupils or families will take place using school equipment and/or school accounts.

Wherever possible, pupils will be taught how to keep themselves safe when online.

E-mail

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Use of the school's email system should be for professional communication only
- Pupils will always be supported when writing or opening emails.

Published content: eg school website, school social media accounts

- The contact details will be the school address, email and telephone number.
- Staff or pupils' personal information will not be published.
- The Senior Leadership Team and ICT Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Parents and Carers will be informed of the school policy on image taking, publishing and storing.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website or any school-run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children.

Use of social media including the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Use of video services such as Google Meet, Microsoft Teams, Zoom and Facetime will be monitored by staff.
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

- Under no circumstances must photographs of pupils be used by staff on personal social media pages/sites or any external websites.
- Social media can be used to promote Portesbery school events through staff personal accounts, but discretion is advised and pupil names and images must not be displayed or disclosed.

Use of personal devices

- Personal equipment may be used by staff to access the school IT systems provided their use complies with the Online Safety policy and the Acceptable Use policy
- **Staff must not take and store images of pupils or pupil personal data on personal devices – school equipment is provided for this purpose.**
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data

- The school has a separate Data Protection Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

Policy Decisions

Authorising access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT staff and governors) must read **and mark as read** the electronically circulated 'Acceptable Use Policy' before accessing the school IT systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- All internet access for pupils will be assessed on an individual basis according to the pupil's level of need and understanding – typically a 'PG' rating.
- People not employed by the school who are accessing the internet are expected to follow the guidelines set out within the Acceptable Use Policy.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.

Handling online safety complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Communication of the Policy:

To staff

- All staff will be shown where to access the Online Safety policy and its importance explained.
- All staff must read and agree to comply with the staff Acceptable Use Policy in order to gain access to the school IT systems and to the internet
- All staff will receive Online Safety training on an annual basis through whole school meetings/class meetings

To parents

- The school will ask all new parents to sign relevant consent forms when they register their child with the school.
- Parents and carers can access this Online Safety Policy on the school website.
- Parents will be offered Online Safety training

Introducing the policy to pupils

- Certain elements of the Online Safety policy will be shared with pupils as appropriate.

Monitoring of this policy will be the responsibility of the Senior Leadership Team and the ICT Manager, Neil Thomas.