E-safety Policy

Including Internet and Email

Portsdown Primary School and Early Years

Approved by: Governing Body	**Date:** April 2023
Last reviewed on: April 2023	
Next review due by: April 2024	

Contents

.....

1. Aims

Portsdown Primary School and Early Years recognises the importance of ICT to the whole school community and sees the Internet and related technologies as being a valuable resource. At Portsdown Primary School and Early Years we encourage the pupils' use of the rich information and communication resources available through the Internet, together with the development of appropriate skills to analyse and evaluate these resources. These skills will be fundamental in the society our pupils will be entering.

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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

It is our intention to protect our pupils from inappropriate or undesirable material. The following criteria define inappropriate or undesirable materials;

- Obscene, offensive, illegal or inaccurate. Pupils should not feel or become uncomfortable, threatened or worried by material or information on websites or from email.
- Similarly, pupils must not harass, insult, attack others, violate copyright or trespass in others' folders.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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.

3. Roles and responsibilities

3.1 The governing board

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).

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 (appendix 5)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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

3.2 The headteacher

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the E-Safety manager and other staff, as necessary, to address any online safety issues or incidents, including incidents of cyber-bullying which will be dealt with appropriately in line with the school behaviour for learning policy. This includes contacting parents where there is a concern over the type of material accessed by a pupil.
- Imposing sanctions where there has been a misuse of the Internet.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

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

- Supporting staff to understand this policy and that it is being implemented consistently throughout the school
- Working with the staff including the computing and E-safety managers, to address any online safety issues or incidents
- 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 governing board

This list is not intended to be exhaustive.

3.4 The E-Safety manager

The E-Safety manager is responsible for:

- Ensuring that skills are planned into the curriculum at suitable levels for the children, liaising with the PSHE manger and Computing manager.
- Ensuring that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy and in conjunction with the headteacher.
- Liaising with the IT support worker to ensure that appropriate filtering and monitoring systems are in place and updated on a regular basis
- Liaising with the IT support worker to ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Liaising with the IT support worker to block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy and implementing it consistently
- Adhering to the terms on acceptable use of the school's ICT systems and the Internet (see section 7), and ensuring that pupils follow these too
- Reporting to the E-Safety manager any online safety incidents to ensure they are logged using the school's CPOMS safeguarding programme or on a paper form (see appendix 2). In the first instance, the class teacher should deal with any misuse of the Internet with the pupil. However, all incidents must be logged with the E-Safety manager.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour for learning policy and in conjunction with the headteacher.

These lists are not intended to be exhaustive.

3.6 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 (see section 7.1)
- Support their child to access remote learning in a safe and secure way, monitoring their child's use of the online learning system

- Use staff email addresses for the purposes of learning enquiries and short messages.

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advicecentre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: https://www.childnet.com/ufiles/parents-factsheet-11-16.pdf

3.7 Visitors and members of the community

Visitors and 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.

4. Access to the Internet

4.1 Internet Access/Filters

Access to the Internet is possible using computers, tablets and Interactive whiteboards. All computers/tablets linked to the internet incorporate automatic antivirus protection. Pupils must not bring in software from home to upload onto the system. Teachers must have appropriate antivirus software on teacher laptops to transfer files between home and school. The broadband internet connection is provided by Portsmouth LEA and incorporates a filtering system or "firewall" appropriate to the age of our pupils which screens undesirable sites at a proxy server.

Due to the nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school nor Portsmouth LEA can accept liability for the material accessed or any consequences thereof.

4.2 Monitoring of Internet Sites/School Network

Although filter systems are in place, all teachers are expected to monitor the range of sites used and ideally should preplan sites to be used with the pupils. Any concerns with websites should be reported to the E-Safety manager who will inform the IT support worker who in turn will inform the LA if needed. Antivirus software will be monitored regularly by the IT support worker. Pupils and staff will be informed that all files in the system can be checked by the E-Safety manager, headteacher and IT support worker. Websites visited by pupils, staff, volunteers, governors and visitors, may be monitored to ensure they comply with the terms for acceptable use as detailed in section 7.

5. Educating about online safety

5.1 Educating pupils about online safety

Pupils will be taught about online safety as part of the computing and PSHE curriculum.

From September 2020 we will follow the Relationships and sex education and health education (2020) curriculum guidance which includes aspects about online safety.

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 then 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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

We follow Project Evolve for our computing curriculum. Our units are planned to give a focus to online safety at the beginning of each academic year. This learning is followed up throughout the year with objectives planned to be covered in PSHE lessons. The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5.2 Educating parents/carers about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website.

This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher who will seek support from the headteacher or a deputy DSL in the headteacher's absence.

Concerns or queries about this policy can be raised with any member of staff.

6. Cyber-bullying

6.1 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. (See also the school behaviour policy.)

6.2 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. Cyber-bullying will be addressed in assemblies.

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

The school also sends information/leaflets on cyber-bullying to 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.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (where the headteacher is absent or not available a deputy DSL is authorised to carry out a search) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or a deputy DSL in their absence.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the headteacher or a deputy DSL in the headteacher's absence to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's Relationships and Behaviour Regulation Policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the Internet in school

7.1 Pupils

When using the school's ICT systems and accessing the Internet in school, pupils will be taught about the rules for acceptable use. Pupils will:

- Only use ICT systems for educational purposes and with a member of staff present
- Access appropriate websites only, under the direction of a teacher
- Immediately let a teacher or other member of staff know if material is accessed which might upset, distress or harm themselves or others
- Not access any social networking sites, instant messaging or use chat rooms
- Not use any inappropriate language when communicating online, including in emails
- Not share their password with others, or use someone else's log in details
- Not give their personal information to anyone online without the permission of a teacher or parent
- Always use the school's ICT systems and Internet responsibly

These rules must also be followed when accessing remote learning through Google Classrooms.

7.2 Staff, governors, volunteers and visitors

When using the school's ICT systems and accessing the Internet in school, staff, governors, volunteers and visitors will be expected to:

- Only use the school's ICT systems and access the Internet in school, or outside school on a work device, for educational purposes or for the purposes of fulfilling the duties of their role
- Not access or attempt to access inappropriate material, including but not limited to material of a violent, criminal, pornographic, racist or offensive nature
- Not access any social networking sites, instant messaging or use chat rooms except for the school's own social media page for communicating school news with the school community
- Not use any improper language when communicating online, including in emails
- Be responsible for all emails sent, not forwarding anonymous email or chain email, and reporting any emails received that are of an offensive manner, to the E-Safety manager
- Respect the copyright of materials on the Internet and school network
- Not install any unauthorised software
- Not share their password with others or use someone else's log in details
- Inform the E-Safety manager or headteacher if a pupil informs them that material which might upset, distress or cause harm to others has been accessed
- Inform the E-Safety manager or IT support worker if any unsuitable sites are discovered by pupils
- Always use the school's ICT systems and Internet responsibly and ensure that pupils in their care do so too.

8. Pupils using mobile devices in school

Year 5 and 6 pupils are permitted to bring in mobile phones into school but under strict compliance rules which parents have to sign for.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in section 7.2 .

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the headteacher.

Work devices must be used solely for work activities.

10. Remote Learning

Google Classroom will be one of the ways in which the School will deliver remote learning to groups of children and entire year groups who are isolating at home due to the coronavirus pandemic. Our offer for remote learning is adapted to the age of the child and as such, different year groups will engage with Google Classroom differently.

All children are set up with a Google login so they can access the Classroom. For safeguarding reasons, the email aspect of this has been switched off and as such, children cannot send and receive emails to each other or to members of staff. Children are able to access their own Classroom only, to complete homework and watch learning videos and PowerPoints. If children will be using the Stream function to discuss learning with their class, the teacher will remind children about the rules for acceptable use as set out in section 7.1. Teachers will be able to record videos, record their screen and add their voice to presentations. This is done securely over Google Classroom and is only done by school staff, not by children.

We may also use the school's website to publish work the same safety methods described as above.

It is the responsibility of the teaching staff within each Classroom to monitor the work and raise any safeguarding or E-safety concerns to the E-safety manager and the DSL as appropriate (see section 3).

Teacher's email addresses are made to available to parents/carers to enable communication throughout the pandemic. Parents are reminded through newsletters and social media about the acceptable use of these emails.

11. 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 the behaviour for learning policy. 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, 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. 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.

12. Training

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 (for example through emails, e-bulletins and staff meetings).

The E-Safety manager will conduct an annual audit of staff training needs (appendix 1).

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Relationships and Behaviour Regulation Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

:

Appendix 1: online safety training needs – self-audit for staff

Online safety training needs audit

Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 2: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature**

Appendix 3: EYFS (including nursery) and KS1 acceptable use agreement (pupils)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**

Appendix 4: KS2 (Years 3,4,5 and 6) acceptable use agreement (pupils)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**

Appendix 5: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**