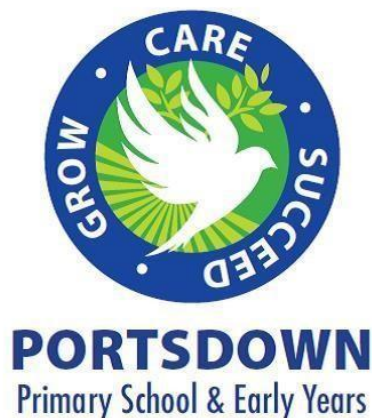


E-safety Policy

(Including ICT and Internet Acceptable Use and Email Usage)

Portsmouth Primary School and Early Years



Approved by: Governing Body

Date: September 2026

Last reviewed on: June 2026

Next review due by: June 2027

Contents

1. Aims	3
2. Legislation and guidance	3
Definitions	4
Unacceptable use.....	4
3. Roles and responsibilities	5
3.2 The headteacher	6
3.4b The E-Safety manager.....	7
3.9 Parents.....	9
3.10 Visitors and members of the community	10
4. Access to the Internet.....	10
4.1 Internet Access/Filters	10
4.2 Monitoring of Internet Sites/School Network	10
5. Educating about online safety.....	11
5.1 Educating pupils about online safety	11
5.2 Educating parents/carers about online safety	12
6. Cyber-bullying.....	12
6.1 Definition	12
6.2 Preventing and addressing cyber-bullying	12
6.3 Examining electronic devices.....	12
7. Acceptable use of the Internet in school	14
8. Pupils using mobile devices in school (see mobile phone policy for more details)	14
9. Staff using work devices outside school	14
11. Further information on how the school will respond to issues of misuse	15
12. Training	17
13. Monitoring arrangements.....	18
14. Links with other policies.....	18
Appendix 1: online safety training needs audit for staff.....	19
Appendix 2: record sheet (should CPOMs be unavailable).....	20
Appendix 3: EYFS (including nursery) and KS1 acceptable use agreement (pupils)	21
Appendix 4: KS2 (Years 3,4,5 and 6) acceptable use agreement (pupils)	22
Appendix 5: acceptable use agreement (staff, governors, volunteers and visitors)	23
Appendix 6: Facebook cheat sheet for staff.....	24
Appendix 7: Glossary of cyber security terminology.....	26
Appendix 8: AI Safeguarding: Quick reference guide for staff	27
.....	

1. Aims

Portsmouth 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 Portsmouth 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.

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, antisemitism, 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 scams

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Relationships and Behaviour Regulation Policy /staff discipline policy/staff code of conduct policies as appropriate.

2. Legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- [Data Protection Act 2018](#)
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Computer Misuse Act 1990](#)
- [Human Rights Act 1998](#)
- [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)
- [Education Act 2011](#)

- [Freedom of Information Act 2000](#)
- [Education and Inspections Act 2006](#)
- [Keeping Children Safe in Education 2023](#)
- [Searching, screening and confiscation: advice for schools 2022](#)
- [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)
- [Education and Training \(Welfare of Children\) Act 2021](#)
- UK Council for Internet Safety (et al.) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- [Meeting digital and technology standards in schools and colleges](#)
- Portsdown Primary School Data Protection and Artificial Intelligence (AI) Policy

Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 7 for a glossary of cyber security terminology.

Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel

- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour/discipline/staff discipline/staff code of conduct/etc. as appropriate. Copies are available on the school's website, or on the staff intranet as appropriate.

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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.
- The governor who oversees online safety is the safeguarding governor

All governors will:

- Ensure 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 3)
- 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.
- (See section 4.1 for specific roles regarding monitoring and filtering for the Full Governing Body)

The governing board will receive regular reports on the school's use of AI tools, including any incidents or concerns, as part of their safeguarding monitoring responsibilities. This will include updates on:

- Which AI tools are being used by staff and pupils
- Any AI-related safeguarding incidents
- Compliance with the school's AI usage policies
- Staff training on AI safeguarding risks

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 (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies in support of the DSL are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL and the deputies in support of the DSL (and instead of the DSL in their absence) 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager 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's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) 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 Relationships and Behaviour Regulation Policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- 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
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4a The ICT support worker (in this case this role will be undertaken on behalf of the school by Rocket)

The ICT support worker is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on at least a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are referred to the DSL to be dealt with appropriately in line with the school Relationships and Behaviour Regulation Policy

This list is not intended to be exhaustive.

3.4b 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 manager and Computing manager.
- Ensuring that any online safety incidents reported to them are logged (on the school's safeguarding monitoring system CPOMS) 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
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting the DSL/ or a deputy DSL.
- Following the correct procedures by discussing with the DSL/ or a deputy DSL if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (on CPOMS) 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 Relationships and Behaviour Regulation 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'

This list is not intended to be exhaustive.

3.6 Personal use by staff

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time.
- Does not constitute 'unacceptable use'
- Takes place when no pupils are present unless it is to access a school account e.g. to complete two factor authorisation
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media and use of email protect themselves online and avoid compromising their professional integrity.

3.7 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 6).

3.7 Remote access

We allow staff to access the school's ICT facilities and materials remotely, using Google Drive

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the headteacher or others on their behalf may require against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Please see the school's data protection (as found on the school's website and intranet).

3.8 School social media accounts

The school and nursery have official Facebook accounts, managed by the leadership team of the school and nursery. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

3.9 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](#)
- Hot topics – [Childnet](#)
- Parent resource sheet – [Childnet](#)

3.10 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. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Access to the Internet

4.1 Internet Access/Filters

Computers and equipment are available to pupils only under the supervision of staff. 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 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 pre-plan 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 Local Authority 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 Headteacher, DSL and deputy DSLs 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.

The school uses Classroom.Cloud and BroadBand4 Scheduled Monitoring to monitor the internet access and this provides a record of the checks made on potential words and phrases requiring investigation and sites where access has been prohibited. The DSL/deputy DSL will record the outcome of the investigation on Classroom Cloud. Where there is a monitoring concern, the incident will also be recorded on CPOMs

The school's monitoring systems also track access to AI tools and chatbots to ensure compliance with the school's AI usage policy and to identify any safeguarding concerns. Where monitoring identifies potential misuse of AI tools, the DSL/deputy DSL will investigate and record the outcome on CPOMs, following the same procedures as for other online safety concerns.

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. Where appropriate, we will inform parents/carers where monitoring and filtering has resulted in a need to discuss with their children and any action we have taken as a result, including sanctions.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's [filtering and monitoring standards](#)
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
 - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

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.

All schools have to teach:

- [Relationships education and health education](#) in primary schools

In the school's nursery and Year R, pupils will be taught about online safety via stories and role play (appropriate to their age).

In **Key Stage (KS) 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
- 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 throughout the year. The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will also 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/ Facebook page.

This policy will also be shared with parents/carers via the school's website.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use via this policy
- 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 via the curriculum information on our website.

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.

Parent/Carer Photography at School Events

Parents and carers should be aware of the school's rules regarding photography at school events:

- Permitted: Photographing your own child for personal/family use
- NOT permitted:
 - Photographing other children
 - Sharing photographs containing other children on social media or public platforms
 - Taking photographs during designated "no photography" periods

Where possible, the school will provide dedicated time during or after events for parents to photograph their own child without other children present. The school will monitor compliance with this policy and may need to review whether parent photography can continue at future events if the policy is not followed.

For full details, please refer to Section 13 of the school's Data Protection and Artificial Intelligence (AI) Policy, available on the school website.

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 Relationships and Behaviour Regulation 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 Relationships and Behaviour Regulation 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 (therefore, 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.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini (formerly known as Google Bard).

What are deepfakes?

'Deepfakes' are AI-generated images, audio, or video that appear real but are fake. This includes pornographic content created using AI to include someone's likeness without their consent. Deepfakes can be highly convincing and pose significant safeguarding risks to pupils.

Our approach to AI

Portsmouth Primary School and Early Years recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of deepfakes, where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Portsmouth Primary School and Early Years will treat any use of AI to bully pupils in line with our anti-bullying/Relationships and Behaviour Regulation Policy/safeguarding policies.

Risk assessment for new AI tools

Before introducing any new AI tool, staff must complete a safeguarding risk assessment and, where the tool processes personal data, a Data Protection Impact Assessment (DPIA) as set out in Section 14.9 of the school's Data Protection and AI Policy. The E-Safety manager and DSL will review all AI tool risk assessments to ensure appropriate safeguards are in place.

Staff responsibilities

Staff must also refer to Section 14 of the school's Data Protection and Artificial Intelligence (AI) Policy for:

- Detailed guidance on prohibited data inputs when using AI tools (Section 14.3)
- The list of approved AI tools for staff use (Section 14.5)
- Anonymisation requirements (Section 14.6)
- Data Protection Impact Assessment (DPIA) requirements (Section 14.9)
- The AI-specific data breach response procedure (Appendix 2)

For full details on approved AI tools, prohibited data inputs, anonymisation requirements, and the AI-specific data breach response procedure, see Sections 14.3-14.11 and Appendix 2 of the Data Protection and AI Policy.

Data breach reporting

Any incident where personal or sensitive data is entered into an unauthorised AI tool must be treated as a data breach and reported immediately following the procedure in Appendix 1 of the Data Protection and AI Policy.

6.5 Photography and Image Security

To protect pupils from emerging online risks including AI-generated imagery misuse and potential blackmail/extortion attempts, the school has implemented enhanced protective measures regarding pupil images.

Staff must refer to Section 13 of the school's Data Protection and Artificial Intelligence (AI) Policy for detailed guidance on:

- Taking photographs for public-facing platforms (website, social media, newsletters)
- Using alternative photography approaches (distance shots, over-the-shoulder images, etc.)
- Metadata removal procedures before uploading images online
- Parent/carers photography rules at school events
- Social media privacy settings

Key principles:

- Do NOT publish clear, front-facing photographs of children's faces on public platforms
- NEVER publish a child's full name alongside their photograph
- ALWAYS remove metadata from digital photographs before uploading online
- USE approved software (ExifCleaner or ImageOptim) for metadata removal

Metadata Removal Process:

1. Take photos on school-managed devices where possible
2. Store original images securely on the school network
3. Export reduced-resolution "web-safe" copies
4. Remove metadata using ExifCleaner (<https://exifcleaner.com>) or ImageOptim (Mac: <https://imageoptim.com/mac>)
5. Upload only processed images to public platforms

All staff must include image security awareness in their ongoing safeguarding training.

Cross-reference to Data Protection and AI Policy

For detailed operational guidance on image security, staff should refer to Section 13 of the school's Data Protection and Artificial Intelligence (AI) Policy, which includes:

- Step-by-step metadata removal procedures (Section 13.4)
- Approved software for metadata removal (ExifCleaner and ImageOptim)
- Social media privacy settings (Section 13.6)
- Parent/carers photography rules at school events (Section 13.5)
- Third-party use of pupil images (Section 13.8)

7. Acceptable use of the Internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school (see mobile phone policy for more details)

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. Phones are not to be with the child during school hours and so will need to be handed in to the school's staff at the start of the school day.

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. Wherever possible USBs should not be used.

If staff have any concerns over the security of their device, they must seek advice from the Headteacher or a deputy DSL in their absence.

Work devices must be used solely for work activities.

10. Use of school phones system and email (see also the mobile phone policy)

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the headteacher immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Recordings of phone conversations would only be listened to in order to discuss a complaint raised by a parent/carer or member of the public.

11. Further information on 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.

Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has 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 (see the safeguarding policy), **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

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.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if the pupil refuses to co-operate, we will proceed according to the safeguarding policy)

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a 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 a device, the staff member should only do so if they reasonably suspect that the data has been, 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 headteacher 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 whether there is a good reason to erase data or files from a device, staff members will consider whether 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 is 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
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [searching, screening and confiscation](#) and the UK Council for Internet Safety (UKCIS) et al.'s 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 et al.'s guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Relationships and Behaviour Regulation policy if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community

- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

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

Training will cover:

Online Safety:

- Technology as a significant component in safeguarding and wellbeing issues
- Children at risk of online abuse
- How children can abuse their peers online
- Physical abuse, sexual violence and initiation/hazing type violence with an online element
- Spotting signs and symptoms of online abuse
- Ensuring pupils can recognise dangers and risks in online activity
- Influencing pupils to make healthy long-term choices
- Recognising and responding to AI-generated inappropriate content, including deepfake imagery and deepfake pornography, and understanding the safeguarding risks these pose to pupils

AI and Data Protection:

- Safe use of generative AI tools
- Prohibited data inputs and permitted uses
- Recognising and reporting AI-related data breaches
- Understanding AI risks including deepfakes and image manipulation
- Data Protection Impact Assessments (DPIAs)
- Understanding what deepfakes are and how to respond to incidents involving AI-generated imagery

Image Security and Safeguarding:

- Protective photography practices (distance shots, anonymisation)
- Metadata removal procedures
- Social media privacy settings
- Responding to AI image misuse concerns
- Parent photography guidelines at school events

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, threatening, 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 up the risks
- 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 and deputies 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.

Training records will be maintained and reviewed annually. Training will be delivered in conjunction with the requirements of the school's Data Protection and Artificial Intelligence (AI) Policy.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Monitoring arrangements

Staff log behaviour and safeguarding issues related to online safety on CPOMs. This is monitored by the DSL/deputy DSLs with appropriate action and referrals to external agencies undertaken where appropriate.

This policy will be reviewed every year by the headteacher. At every review, the policy will be shared with the governing board.

14. Links with other policies

This esafety policy is linked to our:

- Data protection and Artificial Intelligence (AI) policy (particularly sections 13 (Photographs and videos), 14 (Artificial intelligence), and Appendices 1 and 2 (breach procedures))
- Child protection and safeguarding policy
- Relationships and Behaviour Regulation Policy
- Staff disciplinary procedures
- Complaints procedure
- Mobile Phone Policy
- CCTV policy

**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 (only if CPOMs etc are offline)
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

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:

Appendix 6: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

**10 rules for
school staff**

on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
 2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
 3. Check your privacy settings regularly
 4. Be careful about tagging other staff members in images or posts
 5. Don't share anything publicly that you wouldn't be happy showing your pupils
 6. Don't use social media sites during school hours
 7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
 8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
 9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
 10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)
-

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if ...

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
 - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
 - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 7: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

AI Safeguarding: Quick Reference Guide for Staff

Portsmouth Primary School and Early Years

What are deepfakes?

'Deepfakes' are AI-generated images, audio, or video that appear real but are fake. This includes pornographic content created using AI to include someone's likeness without their consent. Deepfakes can be highly convincing and pose significant safeguarding risks to pupils. (e-safety policy September 2026)

What to do if a pupil reports AI-generated inappropriate content

IMMEDIATE ACTIONS:

1. **Listen and reassure** – Take the report seriously and thank the pupil for telling you
2. **Do NOT view the content** – If it's an indecent image, do not look at it
3. **Report to the DSL immediately** – Contact the Designated Safeguarding Lead without delay
4. **Record on CPOMs** – Log the incident with all relevant details
5. **Preserve evidence** – If appropriate, secure the device (do not delete anything)

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 deemed necessary. (e-safety policy September 2026)

Red flags to watch for

Pupil behaviour that may indicate AI-related concerns:

- Distress about images or videos circulating online
- Mentions of "fake" photos or videos of themselves or peers
- Reluctance to use school devices or be photographed
- References to AI tools being used to create inappropriate content
- Concerns about blackmail or threats related to images

Staff practices that breach policy:

- Colleagues entering pupil names/data into unauthorised AI tools
- Clear, front-facing pupil photos being published on public platforms
- Photos being uploaded without metadata removal
- Parent photography rules not being enforced at school events

Where to get help

For safeguarding concerns	Designated Safeguarding Lead
For AI/data protection queries	Headteacher or SLT
For technical support	IT Support (Rocket)
Emergency data breach	Report to Headteacher immediately

Remember:

- ☒ Portsmouth Primary School will treat any use of AI to bully pupils in line with our anti-bullying/Relationships and Behaviour Regulation Policy/safeguarding policies e-safety policy September 2026
- ☒ If personal data is accidentally entered into an AI tool, it must be treated as a data breach Data protection, AI and biometric 2026 p...
- ☒ All incidents where AI-generated inappropriate content is reported mandate a safeguarding response e-safety policy September 2026
- ☒ When in doubt, report it – safeguarding is everyone's responsibility

Full policies available: School website and staff intranet
Training: Speak to SLT if you need additional support