**ONLINE SAFETY POLICY
PRIMLEY WOOD PRIMARY SCHOOL**

Date of approval: February 2023

Review date: February 2024



Contents

1. Aims .................................................................................................................................................. 2

2. Legislation and guidance................................................................................................................... 2

3. Roles and responsibilities.................................................................................................................. 2

4. Educating pupils about online safety................................................................................................. 5

5. Educating parents about online safety.............................................................................................. 6

6. Cyber-bullying.................................................................................................................................... 6

7. Acceptable use of the internet in school........................................................................................... 8

8. Pupils using mobile devices in school ............................................................................................... 8

9. Staff using work devices outside school............................................................................................ 8

10. How the school will respond to issues of misuse ........................................................................... 9

11.Training............................................................................................................................................. 9

12. Monitoring arrangements............................................................................................................... 10

13. Links with other policies.................................................................................................................. 10

Appendix 1: online safety training needs – self-audit for staff............................................................. 11

Appendix 2: online safety incident report log....................................................................................... 12

1. **AIMS**

Our school aims to:

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

**THE 4 KEY CATEGORIES OF RISK (KCSiE 2022)**

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

* **Content** –being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
* **Contact** – being subjected to harmful online interaction with other users; for example: 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** – online behaviour that increases the likelihood of, or causes, harm; for example, 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.
1. **LEGISLATION AND GUIDANCE**

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

* Teaching online safety in schools
* Preventing and tackling bullying and cyber-bullying: advice for head teachers and school staff
* Searching, screening and confiscation

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

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

**3. ROLES AND RESPONSIBILITIES**

**3.1 The Board of Trustees**

The Board of Trustees has overall responsibility for monitoring this policy and holding the head of school 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 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.

**3.2** **The Head of School**

The head of School is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

**3.3 The Designated Safeguarding Lead**

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

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

* Supporting the head of school in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
* Working with the head of school, ICT manager, PHSCE lead, Online Safety Co-ordinator and other staff, as necessary, to address any online safety issues or incidents
* Managing all online safety issues and incidents in line with the school child protection policy
* Ensuring that any online safety incidents are logged (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 behaviour 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 head of school and/or board of trustees.

This list is not intended to be exhaustive.

**3.4 The ICT Manager**

The ICT manager is responsible for:

* Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
* 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 a weekly 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 dealt with appropriately in line with the school behaviour policy

 This list is not intended to be exhaustive.

**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 (**Letter to parents**)
* Working with the DSL to ensure 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 dealt with appropriately in line with the school behaviour policy
* Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of ‘it could happen here’

This list is not intended to be exhaustive.

**3.6 Parents**

Parents are expected to:

* Notify a member of staff or the head of school 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 (Letter to parents)

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

* What are the issues? – https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
* Hot topics – http://www.childnet.com/parents-and-carers/hot-topics
* Parent resource sheet – <https://www.childnet.com/resources/parents-and-carers-resource-sheet>

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

1. **EDUCATING PUPILS ABOUT ONLINE SAFETY**

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

* **Relationships Education and Health Education** in primary schools
* **Relationships and Sex Education and Health Education** in secondary schools

**Pupils in Key Stage 1 will be taught to:**

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

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

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

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

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

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

1. **EDUCATING PARENTS ABOUT ONLINE SAFETY**

The school will raise parents’ awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents. Online safety will also be covered during parents’ evenings. The school will let parents 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 have any queries or concerns in relation to online safety, these should be raised in the first instance with the head of school and/or the DSL.

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

**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 1 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. Teachers will discuss cyber-bullying with their classes.
* 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.
* All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
* 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so

**6.3 Examining Electronic Devices**

The head of school, and any member of staff authorised to do so by the head of school 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 head of school and assistants.
* 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 head of school or assistants 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 <https://www.gov.uk/government/publications/searching-screening-and-confiscation> and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes

<https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>: 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 <https://www.gov.uk/government/publications/searching-screening-and-confiscation>
* UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
* <https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>
* Our behaviour 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.

1. **ACCEPTABLE USE OF THE INTERNET IN SCHOOL**

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet. 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.

1. **PUPILS USING MOBILE DEVICES IN SCHOOL**

Pupils may bring mobile devices into school, but are not permitted to use them during: Lessons Clubs before or after school, or any other activities organised by the school Mobiles need to be taken to the school office for the day and collected at the end of the day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Letter to parents).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

1. **STAFF USING WORK DEVICES OUTSIDE SCHOOL**

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

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

Staff members must not use the device in any way which would violate the school’s terms of acceptable use.

Work devices must be used solely for work activities.

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

1. **HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE**

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

Where a staff member misuses the school’s ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [staff disciplinary procedures/staff code of conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

1. **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).

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 and other children online through:
* Abusive, harassing, and misogynistic messages
* Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
* Sharing of abusive images and pornography, to those who don’t want to receive such content
* Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

• Develop better awareness to assist in spotting the signs and symptoms of online abuse

• Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh 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 DSLs and assistant heads 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.

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

1. **MONITORING ARRANGEMENTS**

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5. This policy will be reviewed every year by the Computing lead and PSHCE lead. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

1. **Links with other policies**

This online safety policy is linked to our:

* Child protection and safeguarding policy
* Behaviour policy
* Staff disciplinary procedures
* Data protection policy and privacy notices
* Complaints procedure
* ICT and internet acceptable use policy

**Appendix 1: ONLINE SAFETY TRAINING NEEDS – Self-Audit for Staff**

This can be adapted.

|  |
| --- |
| **ONLINE SAFETY TRAINING NEEDS AUDIT** |
| **Name of Staff Member/Volunteer:** | **Date:**  |
| **QUESTION** | Yes/No (add comments if necessary) |
| Do you know the name of the person who has lead responsibility for online safety in school? |  |
| Are you aware of the ways pupils can abuse their peers online? |  |
| 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? |  |

**APPENDIX 2: ONLINE SAFETY INCIDENT REPORT LOG**

|  |
| --- |
| **ONLINE SAFETY LOG** |
| **Date**  | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |