



Online Safety Policy

Adopted by the Governing Body:	September 2020
Review cycle:	Annually
Review date:	Summer 2021
Governors Committee:	Learning and Teaching
Staff Responsible:	Designated Safeguarding Lead

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	5
5. Educating parents about online safety	5
6. Cyber-bullying.....	6
7. Acceptable use of the internet in school.....	7
8. Pupils using mobile devices in school	7
9. Staff using work devices outside school.....	7
10. How the school will respond to issues of misuse.....	7
11. Training.....	8
12. Monitoring arrangements	8
13. Links with other policies	8
Appendix 1: acceptable use agreement (pupils and parents/carers)	10
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors).....	10
Appendix 3: online safety training needs – self-audit for staff.....	11
Appendix 4: online safety incident report log	12
Appendix 5: Google meet protocol for remote sessions	13

1. Aims

Online safety in schools is of paramount importance. As the online world evolves, so do both the online harms and risks facing our children and the relevant legislation, both statutory and non-statutory, which directs and guides how schools should meet their online safety requirements.

School staff and governors play a vital role in setting an example for the whole school and are central to implementing policy and process. It is imperative that a whole school community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This will support a robust online safety ethos and ensure that schools are providing the best online safety provision they possibly can.

The Priory 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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the Department's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the [National Curriculum computing programmes of study](#).

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

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

The governor who oversees online safety is Kim Oakley. Their role in school should include, but is not limited to:

- Ensure that everyone has read and understood this policy and had sufficient training.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensuring that students are provided with a safe environment in which to learn and develop.
- Ensuring that the school has appropriate filters and monitoring systems in place.
- Auditing and evaluating online safety practice.
- Ensuring that there are robust reporting channels.

3.2 The headteacher

The headteacher 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 – Hannah Taylor) and deputies are set out in our child protection and safeguarding policy.

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

- Supporting the headteacher and CEOP in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager, CEOP and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 3 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

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 fortnightly 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 4) 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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

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

- What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught specifically about online safety as part of the curriculum in both Computing lessons and in PSE (Personal and Social Education) lessons.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

However the safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. 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. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents through Tootoot 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. Form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. 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 as well as putting information onto the website.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

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

7. Acceptable use of the internet in school

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 (appendices 1 and 2). 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.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

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.

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 appendix 2.

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

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

Work devices must be used solely for work activities.

10. 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 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 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. 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.

11. 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).

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.

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

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4. If words or articles which contain the following are searched for or loaded then they are flagged up in our software so the incident can be looked into:

- Radicalisation
- Abuse
- Adult content
- Bullying
- Substance use
- Suicidal/self harm
- Criminal activity

This policy will be reviewed annually by the DSL and CEOP. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- GDPR
- Complaints procedure
- Admissions arrangements
- Anti-bullying
- Capability and disciplinary procedure (staff)
- Staff discipline, conduct and grievance procedures
- Educational visits and off-site activities
- Inclusion and SEND

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parents/carers may be contacted.

- I will only use ICT systems in school, for school work, including the internet, e-mail, etc.
- I will not download or install software on the school system.
- I will only logon to the school network/Learning Platform with my own username and password and will not give anyone else my login details.
- I will only use my school email address and that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I will not violate copyright laws

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the 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, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- 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
- Share my password with others or log in to the school's network using someone else's details

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.

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 3: 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 5: Using google meet for remote sessions

Please have a look at the following link for advice and support in how to use Google Meet if you have never used it before;

https://www.youtube.com/watch?v=44sGlczM_po

- This is not a compulsory method of communicating with our students. It is an option which we have enabled for staff to use to get more face to face time with our students, during lockdown sessions.
- This platform allows you to mute all students, there is a “chat” facility on the edge of the screen where students can ask questions by typing them. You as the host can then unmute them so you can talk to them whilst everyone else listens. As the host you need to wait until all students have left and then close the meeting, otherwise they can stay on line and continue talking.
- Please know that if you use Google Meet you can send a calendar invitation out to students which will also send them the link to log in to your meeting.
- If this platform is being used to deliver a tutor time then it is up to the tutor to decide on when the tutor session will happen and inform their tutor group. The relevant HoY should also be made aware. It is important that we are also using this session for tracking the wellbeing and safety of our students.

Protocol and advice for using Google Meet for lessons or tutor times

- Students/staff using Google Meet must do so only using their school email address - It is important that this is checked if using your own devices.
- If working from home, staff must ensure that they are working in an area that does not reveal anything about their personal life. Make sure you have a plain wall or door behind you where possible.
- Students must not be in their bedroom but in a family area.
- Students/staff must be suitably dressed before engaging with any live sessions.
- Do not have a 1:1 live session with students.
- We must try not to allow students to be online when the teacher is not present. To ensure this does not happen, please ensure that you give the meet a “nickname”. This way the students cannot join before the teacher.
- The teacher must be the last to leave the meet. This will ensure that students cannot rejoin without the teacher being present.
- Please follow the school behaviour policy and do not accept inappropriate comments or behaviour. If this does happen then please inform the parent/carer and do not allow them to participate in the next session.
- If any safeguarding concerns arise then please use TooToot to report it straight away. Using the live chat enables conversations to be monitored whilst using it on its own or with Google Meet.
- Remind users about respecting others and using the chat box for commentary.
- As with any on-line learning platform please encourage all users to clear their browser after each use. This will help to prevent cookies tracking your internet use.
- Ensure that you learn how to mute and unmute participant microphones. It is good practice for all students to have their microphone muted unless they are asked to contribute at any point.
- If at any point you need to remove a student from the meet then press the button next to the “mute participant” button.
- Ensure students are aware of the etiquette of how to answer questions or participate in conversations.
- Staff do not have to record the meeting. However, as a school we advise you to do so. If you wish to record the meeting you need to manually press the record button.
- The recording of the meeting is stored in the “cloud” and not directly onto the laptop/computer etc. Therefore staff can use their own equipment.
- Staff can turn off their own camera if they do not want students to see them. Please ensure that there is nothing else on your screen that you would not want students to see.