eSafety Policy

Priory Primary School
At the heart of the community

Approved by:	[Name]	**Date:** [Date]
Last reviewed:	Spring Term 2021	
Next review due by:	Spring Term 2023	

Contents

---

1. School Intent and Aims of the Policy

Our school's eLearning intent is to:

- Develop in our pupils, a confidence, curiosity and responsibility towards the use of technology to enhance their lives and their learning; to research, explore, deepen knowledge and to communicate effectively.

Therefore, this policy aims to:

- Ensure robust processes are in place for 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 (DfE) 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 headteachers and school staff
- Relationships and sex education
- 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 Governors

The governing body has overall responsibility for monitoring this policy and holding the head teacher 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

3.2 The Head Teacher

The head teacher 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 DSLs are set out in our child protection and safeguarding policy.

The DSL who takes lead responsibility for online safety in school is Mrs Paula Wakeling, whose role is:

- Supporting the head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head teacher, ICT support and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 3) 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 2 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 teacher and/or governing board

3.4 The ICT Providers

The ICT provider is Partnership Education, and 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 regular 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 3) 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

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
- Class teachers are responsible for monitoring the use of technology by their own class
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, 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 3) 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
- Ensuring they use a secure Priory Primary email address for communication within the school community and for correspondence with outside agencies for work purposes. This also enables the use of Google Classroom as a teaching, learning and communication tool.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the head teacher 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
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

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 1).

4. Educating pupils about online safety

4.1 Curriculum

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

In **Key Stage 1**, pupils will be taught to:

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

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

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

By 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

The safe use of social media and the internet will also be referenced and / or covered in other subjects whenever a relevant topic or discussion arises.

4.2 School email and social media

Pupils from Year 2 onwards receive a Priory Primary secure email address. This is to be used for correspondence within the school community and for learning to use email safely and responsibly. The log-ins enable a secure introduction to the use of social media through chatrooms with adult verification, alongside secure access to e-twinning and e-pals sites.

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 and communication platform, SeeSaw. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head teacher and/or the DSL.

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

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 anti-bullying 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 teachers will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

The school has embedded opportunities within 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.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti-bullying 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 and the school's COVID-19 risk assessment.

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

7. Acceptable use of the internet in school

7.1 Acceptable Use Agreements

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.

7.2 Personal Safety

Everyone is encouraged to observe personal safety rules when accessing technology. The following should be **withheld** when accessing unrestricted / unsecured social media, emails and websites:

- Full name
- Address
- Photograph
- Email address
- School name
- Clubs attended
- Age / DOB
- Names of parents
- Routes to / from school
- Other identifying information

Photographs should only be uploaded with approval from a member of staff.

7.3 Videos and photographs

Photos taken by school members should be for the benefit of parents, school documentation, displays and school media only. Photos should be stored in the Priory Photo Bank in the secured GoogleDrive. The sharing of images via the school website, FaceBook and other mediums on line will only occur if permission has been given by a parent/carer (annually renewed permission forms) or member of staff. Any individual photographs or video clips uploaded should not be named, though group photos may be (for example "Year 3 pupils"). No images should be taken of individuals in compromising positions or clothing e.g. swim kit.

NB The term 'image' refers to any video or photographic footage, regardless of the medium used.

8. Pupils mobile devices in school

Pupils are not allowed to have mobile phones or other personal devices in school.

The only exception to this is pupils in Year 5 and Year 6 who have permission to walk to and from school; they may only bring mobile devices into school, if parents require them to carry a phone for the walk between home and school, and the mobile must be handed into the school office before entering the classroom

9. Staff using work devices outside school

Staff members who are issued with a school laptop and/or iPad 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)
- Changing the password at least once a year
- 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
- Making the device available for regular installing / updating of anti-virus and anti-spyware software
- Keeping operating systems up to date – always install 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 Paula Wakeling.

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 our policies on behaviour and/or anti-bullying, as appropriate to the issue. 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.

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 DSLs 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 3.

This policy will be reviewed every two years by the head teacher. 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
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Acceptable Use Agreements

EYFS & KS1 Pupil
Acceptable Use Policy (AUP)

This is how we stay safe when we go online

- I will ask an adult if I want to use the computers or tablets
- I will only use activities that an adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong
- I will tell an adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

I have talked with my child ..... and confirm that they understand the eSafety rules.

Signed (parent): .....

Date: .....

Lower Key Stage 2 (Year 3 & 4)
Pupil Acceptable Use Policy (AUP)

<table>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">When I use the school's ICT systems (like computers) and get onto the internet in school I will:
Ask a teacher or adult 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
I will 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.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Upper Key Stage 2 (Year 5 & 6)

Pupil Acceptable Use Policy (AUP)

Name of pupil:	
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 username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address, telephone number or name of school to anyone without the permission of my teacher or parent/carer • Tell a teacher 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'm 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 • 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 to school:** • I will leave it in the school office before going to my classroom • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language on the way to and from school, and when communicating with my school friends **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:**
Parent/carer's agreement: I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal mobile phones, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Staff Acceptable Use Policy (AUP)

Acceptable Use of ICT in Priory Primary School

School Policy

New technologies have become integral to the lives of children and young people, both within school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

The purpose of this acceptable use policy is to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of technology in their everyday work

The school will try to ensure that staff will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and to agree to be responsible users.

Acceptable Use Policy Agreement

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 the school's ICT systems in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others
- Take photographs of pupils without first checking their parental permissions
- 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

For my professional and personal safety:

- I understand that Priory Primary School will monitor my use of the school digital technology and communications systems
- I will not disclose my username or password to anyone else
- I understand that I should not write down or store a password where it is possible that someone may steal it
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the eSafety lead, Paula Wakeling

I will be professional in my communications and actions when using Priory Primary School's systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner; I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will only communicate with pupils and parents/carers using official school systems; any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities

I understand that I am responsible for my actions in and out of Priory Primary School:

- I understand that this acceptable use policy applies not only to my work and use of Priory Primary's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name: .....

Signed: .....

Date: .....

Volunteer & Trainee Acceptable Use Policy (AUP)

Acceptable Use of ICT in Priory Primary School

School Policy

New technologies have become integral to the lives of children and young people, both within school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for volunteers and trainees to be more creative and productive in their work with pupils. All users should have an entitlement to safe access to the internet and digital technologies at all times.

The purpose of this acceptable use policy is to ensure:

- that volunteers and trainees will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that volunteers and trainees are protected from potential risk in their use of technology in their everyday work

The school will try to ensure that volunteers and trainees will have good access to digital technology to enhance their role, and will, in return, expect volunteers and trainees and to agree to be responsible users.

Acceptable Use Policy Agreement

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 the school's ICT systems in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Take photographs of pupils without first checking their parental permissions
- Share confidential information about the school, its pupils, staff, volunteers or trainees, 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

For my professional and personal safety:

- I understand that Priory Primary School will monitor my use of the school digital technology and communications systems
- I will not disclose my username or password to anyone else
- I understand that I should not write down or store a password where it is possible that someone may steal it
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to my main contact in school, who will pass the report on to the eSafety lead, Paula Wakeling

I will be professional in my communications and actions when using Priory Primary School's systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner; I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will not engage in any on-line activity that may compromise my professional responsibilities

I understand that I am responsible for my actions in Priory Primary School:

- I understand that this acceptable use policy applies not only to my work and use of Priory Primary's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a ban, referral to Governors and your organisation (where relevant) and in the event of illegal activities, the involvement of the police

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Volunteer / Trainee Name: .....

Signed: .....

Date: .....

Appendix 2: online safety training needs – self audit for staff

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?	
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 3: online safety incident report log

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