

ONLINE SAFETY POLICY FOR PUPILS

April 2026

*Together, creating opportunity
and aspiration for every child*



Contents

| | |
|---|---|
| 1. Feeling safe and happy at school..... | 2 |
| 2. What does online safety mean? | 2 |
| 3. Online dangers..... | 3 |
| Using AI safely..... | 3 |
| Online behaviour and kindness | 3 |
| 4. Cyberbullying | 3 |
| 5. Sharing pictures and messages..... | 4 |
| 6. Who to talk to | 4 |
| 7. Internet access..... | 5 |
| 8. Filtering and monitoring online activity..... | 6 |
| 9. Network security..... | 6 |
| 10. Mental health..... | 7 |
| Appendix 1 – Pupil technology acceptable use agreement..... | 8 |

| First Version Implemented | Revision Level | Current Version Adopted by Trust | Review Date | Responsible Person |
|---------------------------|----------------|----------------------------------|-------------|--------------------|
| April 2026 | V1.0 | April 2026 | July 2027 | DoSI |

1. Feeling safe and happy at school

At The Priestley Academy Trust, we want pupils to feel looked after, safe and happy in school, at home and when they are online. Internet safety is a big part of keeping children safe in education. We have special rules, lessons and people that can help pupils have any worries.

Computers, tablets and phones help us learn, play and talk to friends and family. But sometimes people can use them in ways that are not kind or safe. That is why we teach pupils how to protect themselves online and what to do if they feel unsure, worried or upset.

Computers, tablets and mobile phones help us learn, play and talk to friends and family. But sometimes people can use them in ways that are not kind or safe. That is why we teach pupils how to protect themselves online and what to do if they feel unsure, worried or upset.

We can help by:

- Teaching what online safety means
- Showing what to do if pupils feel worried or scared
- Making sure pupils know who you can talk to

There is always someone who can help.

2. What does online safety mean?

Online safety means learning how to use the internet, games and technology, safely and kindly.

It is about protecting pupils whilst they are online and helping them to make good choices when they use apps, games, videos or websites. We teach pupils how to tell when something online might not be true or real.

We follow the rules in a document called 'Keeping children safe in education' to help everyone stay safe online.

If pupils ever see, hear or read something online that upsets them or makes them feel uncomfortable, they are taught to tell an adult at school or at home. We can help make it right and keep them safe.

Follow the **SMART** rules to keep safe online:

S - SAFE: Keep personal information private (like your full name, address or school).

M - MEETING: Never meet anyone you only know online.

A - ACCEPTING: Do not open messages or files from people you do not know.

R - RELIABLE: Not everything you read or see online is true.

T - TELL: Tell an adult you trust if something online worries you.

3. Online dangers

The internet is full of fun things, like chatting, games, learning and videos, but there are also dangers to be aware of.

Some examples include:

- Cyberbullying, which is when people send unkind or scary messages or images
- Strangers pretending to be someone they are not
- Websites or videos that show things that are not suitable for children
- ‘Viruses’ that can harm computers or steal information
- People who try to get your personal details
- False or unkind information designed to trick or upset you (this is sometimes called ‘misinformation’)
- People who try to get you to do or believe something mean or unsafe (this can be part of ‘radicalisation’)
- Online games, chats or livestreams where others behave in ways that are not kind or safe

Using AI safely

Sometimes websites, games or apps use something called artificial intelligence (AI). AI can do things like chat, draw pictures or answer questions.

AI can be fun and helpful, but it can also make mistakes or show pupils things that are not true. We teach pupils to always check with an adult if something an AI shows them feels strange, unkind or confusing.

Online behaviour and kindness

When pupils are online, they need to be as kind as they would be face-to-face. They need to think before they post, share or comment.

We encourage pupils to ask themselves: “Would I say this in real life?” If the answer is **no**, do not say it online either. Being kind online helps make the internet a safe and happy place for everyone.

4. Cyberbullying

Cyberbullying includes any kind of bullying which takes place online. Cyberbullies (online bullies) send unkind messages over the internet and sometimes share private information online to hurt someone’s feelings.

Cyberbullying happens when someone uses technology to be unkind. It can include:

- Sending mean, scary or upsetting messages or pictures
- Sharing private or embarrassing photos or videos
- Pretending to be someone else online to cause trouble
- Posting nasty comments or rumours

Cyberbullying is never okay. If you see it happen, or it happens to you, pupils should tell an adult they trust. Our school will deal with incidences quickly and help keep everyone safe.

Cyberbullying is sometimes done by a group of people 'ganging up' on someone. If you ever see or hear of someone being cyberbullied, please let the school know as quickly as possible. Pupils are taught never to join in and always must tell a grown-up they trust.

A cyberbully could be anyone, like a friend, a brother or sister, or even an adult. It is really important that pupils and/or adults tell someone if they think someone is being a cyberbully, or a victim of cyberbullying.

5. Sharing pictures and messages

Sometimes people online might ask pupils to send or look at pictures or messages that show private parts of their own or somebody else's body. This is never okay.

It is against the law to share these kinds of pictures, even if individuals take them themselves. Pupils must tell an adult they trust straight away if they receive such images. They will never be in trouble for telling the truth or asking for help.

It is against the law to have intimate pictures or videos of someone who is under the age of 18, even if you are not the person sending them, and even if you took the photos or videos of yourself.

6. Who to talk to

If pupils are worried about something, they can talk to an adult at school. This could be a teacher or any member of staff. If they need to talk, we will always listen.

At home

Pupils can talk to their parents or carers about how to stay safe online. They can help with privacy settings, check games, and help if they see something upsetting.

Pupils should always walk away or close a game, app or computer programme if something online makes them feel worried, upset or confused. Pupils should tell someone they trust if something makes them feel like this. They will not be in trouble for asking for help.

At school

Staff at school have training to protect children.

It is really important to get help if you are worried or unhappy about something online, and we will do our best to solve the problem.

It is important that pupils tell someone they trust if someone is:

- Cyberbullying
- Saying things online that make you feel upset or uncomfortable
- Sending unkind or false messages on the internet or to your phone
- Asking you to do things that you are uncomfortable with

Important members of staff

DSL stands for **Designated Safeguarding Lead**.

In every school there is always somebody who has special training to keep pupils safe. That is their job. All teachers and other staff members have to tell the DSL if they are worried about pupils in their school.

The DSL may have other job titles, like **safeguarding officer** or **safeguarding manager**.

Teachers and other staff members also have training on how to keep pupils safe. It is the most important part of their job.

Here's a list of the people at school you can speak to if you are worried or need help:

| School | DSL |
|----------------------------------|--|
| Atlas Community Primary School | Lisa Simpson, Headteacher |
| Green Lane Primary School | Jo Baxendale, Headteacher |
| Lilycroft Primary School | Leah Florence, Headteacher |
| Margaret McMillan Primary School | Sarah Hodge and Sarah Johnson, Co-Headteachers |
| Miriam Lord Primary School | Bryan Harrison, Headteacher |
| Westbourne Primary School | Jo Marwood, Headteacher |

A list of deputy DSLs can be obtained from the school office.

If you ever need extra help, you can also speak to:

- Childline on 0800 11 11 or visit www.childline.org.uk
- NSPCC on 0800 800 5000 or visit www.nspcc.org.uk
- Kidscape on 020 7730 3300 or visit www.kidscape.org.uk
- Youth Access on 020 8772 9900 or visit www.youthaccess.org.uk

We will always make time to listen and talk if pupils need us.

Remember: for pupils

- You are important to us
- It is never your fault if someone is upsetting you
- There is always someone that can help you
- You will not be in trouble

7. Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once parents/carers have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the school office.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

8. Filtering and monitoring online activity

The Trust will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's '[Filtering and monitoring standards for schools and colleges](#)'. The school will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network and the proportionality of costs compared to the risks. Regular checks on the filtering and monitoring systems will be undertaken to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Any changes made to the system will be recorded by relevant staff. Reports of inappropriate websites or materials will be made to an SLT member immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and Trust, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the school's Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Trust's Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Trust's Child Protection and Safeguarding Policy.

9. Network security

Pupils on each site share the same generic account with a basic 2 digit password. Once in a Year 4, pupils are given their own unique account – each class receives the same 3 digit password which pupils have to change the first time they log in.

Pupils should not share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

10. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will always be taken seriously and dealt with by school leaders in a sensitive and appropriate manner.

Appendix 1 – Pupil technology acceptable use agreement

At The Priestley Academy Trust, we know that using technology is an important part of a pupil's learning experience. We want everyone to be able to use technology, such as the internet and laptops, safely and responsibly. This agreement sets out the rules for using technology and devices.

This agreement supports the Trust's Online Safety and Safeguarding Policies, in line with the Online Safety Act 2023, Keeping Children Safe in Education and the Data Protection Act 2018 (UK GDPR).

If you have any questions about anything in this agreement, speak to the class teacher.

Definitions

Before you read the agreement, here are some key terms you should understand:

- **Technology** – this includes any ICT systems at the school, including the internet.
- **School-owned devices** – any devices that are owned by the school, including laptops and tablets.
- **Personal devices** – any device that belongs to you that you bring into school, including mobile phones.

Using technology in school

My child will:

- Only use technology and devices that they have been given permission to use
- Only access websites, apps and other online platforms that they have been given permission to use
- Only use the school's ICT facilities, technology and devices to complete schoolwork
- Only go on the internet for something other than schoolwork during break and lunch times
- Only use artificial intelligence (AI) tools, e.g. ChatGPT, if they have permission from a teacher

My child will not:

- Install any software onto school ICT systems
- Search for, view, download, upload or send anything inappropriate when using the internet
- Try to get around any security measures the school has put in place on the internet or school-owned devices
- Share any of my passwords with other people

Emails

My child will:

- Only use the email account that has been set up for them by the school when sending emails related to my schoolwork

My child will not:

- Open any emails from people they do not know
- Use a personal email address for schoolwork, unless told to do so by a member of school staff

School-owned devices

My child will:

- Only use school-owned devices to carry out my schoolwork.
- Only use websites and apps that a member of staff has said they can use
- Understand that the school will monitor how they use school-owned devices
- Take care of school-owned devices when I am using them
- Tell a member of staff if a school-owned device is damaged or lost
- Tell a member of staff if something has happened in relation to the security of the device, e.g. downloading an attachment from an email from someone they do not know

My child will not:

- Use school-owned devices to send inappropriate messages, images, videos or other harmful content
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content
- Use school-owned devices to go on personal social media accounts

Personal devices

My child will:

- Ensure personal devices are switched off or on silent mode during lessons and kept somewhere safe
- Understand that if personal devices are lost, damaged or stolen, it is not up to the school to pay for any costs

My child will not:

- Use personal devices to send inappropriate messages, images, videos or other content
- Use personal devices to view, store, download or share any inappropriate, harmful or illegal content

Social media

My child will:

- Think about what they post about the school on social media and make sure they do not post anything that could be harmful to any member of the school community

My child will not:

- Try to speak to any member of staff on social media
- Accept or send 'friend' or 'follow' requests from members of staff on social media
- Send any abusive, threatening or otherwise inappropriate messages on social media
- Bully anyone through social media

Reporting misuse

I understand:

- That my child's use of the internet will be monitored by the school and recognise there will be consequences if this agreement is not followed
 - Understand the headteacher may decide to take disciplinary action, in accordance with the school's Behaviour Policy, if this agreement is not followed
-

Agreement

I confirm that I have read and understood the Pupil Technology and Acceptable Use Agreement and my child will abide by each principle.

| | |
|----------------------------|--|
| School | |
| Name of pupil | |
| Class | |
| Signature of pupil | |
| Name of parent | |
| Signature of parent | |
| Date | |