

# Online Safety Policy

Frequency of Review	Every 1 year
Author	COO/DSL/IT Manager
Approved by	Trust Directors
Reviewed	Sept 2023
Date of Next Review	Sept 2024 (unless there is a material change)

## Contents

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

---

### 1. Aims

The Propeller Academy Trust (PAT) aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole trust 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

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

- **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

## 2. 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 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](#) and [meeting digital and technology standard in schools and colleges](#)

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.

This policy complies with our funding agreement and articles of association.

## 3. Roles and responsibilities

### 3.1 Members and trustees

Members hold Trustees to account for the monitoring of this policy. Trustees have overall responsibility for monitoring this policy and holding the local governing board (LGB) to account for its implementation.

Trustees must ensure the trust has appropriate filtering and monitoring systems in place on trust devices and trust/school networks and the CEO will regularly review their effectiveness.

### 3.2 CEO/COO

The CEO/COO will review the DfE filtering and monitoring standards and discuss with the IT Network Manager and service providers what needs to be done to support the trust in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

### **3.2 The local governing board (LGB)**

Each LGB has responsibility for monitoring this policy for each school and holding the headteacher to account for its implementation.

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

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

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

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

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the trust/school's IT systems and the internet (see IT and internet acceptable use policy appendices)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or approach to safeguarding and related policies and/or procedures
- Ensure that teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and 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.

### **3.3 The headteacher**

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

### **3.4 The designated safeguarding lead**

Details of the school's designated safeguarding lead (DSL) and deputy/deputies are set out in each school's 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 headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the IT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, IT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 2) 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 1 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

### **3.5 The IT network manager**

The IT network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on trust/school devices and trust/school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the trust/school's IT 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 trust's IT systems on a monthly basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 2) 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 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 trust's IT systems and the internet, and ensuring that pupils follow the trust's terms on acceptable use (see IT and internet acceptable use policy appendices)
- Knowing that the IT network manager and DSL are responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by notifying the IT network manager and DSL immediately.
- Following the correct procedures by placing a formal request via the IT network manager and DSL if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the IT network manager and DSL to ensure that any online safety incidents are logged (see appendix 2) 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.

### **3.7 Parents/carers**

Parents/carers 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 trust/school's IT systems and internet (see IT and internet acceptable use policy appendices)

Parents/carers 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 resource sheet – [Childnet International](#)

### 3.7 Visitors and members of the community

Visitors and members of the community who use the trust's IT 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 (see IT and internet acceptable use policy appendices)

## 4. Educating pupils about online safety

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

The text below is taken from the [National Curriculum computing programmes of study](#).

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

**All** schools have to teach:

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

Due to being an SEND Trust, adaptations will need to be made to the following general coverage through key stages;

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
- 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

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

By the **end of Key Stage 4**, pupils will know:

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared, and used online
- How to identify harmful behaviours online (including bullying, abuse, or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

### **All schools**

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.

## **5. Educating parents/carers about online safety**

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers 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/carers 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 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 cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors, trustees 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/carers so 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**

Please refer to section 6.2 of the Trusts ICT and Internet Acceptable Use Policy for further information.

## **7. Acceptable use of the internet in school**

All pupils, parents/carers, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the trust/school's IT systems and the internet. See appendices of the IT and internet acceptable use policy. Visitors will be expected to read and agree to the trust's terms on acceptable use if relevant.

Use of the trust/school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

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

Pupils may not bring personal mobile devices into school, and when in school will use school authorised equipment only.

## **9. 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 that would violate the trust's terms of acceptable use, (see IT and internet acceptable use policy appendices).

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 the IT Manager.

## **10. How the trust will respond to issues of misuse**

Where a pupil misuses the trust/school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and IT and internet acceptable use. 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 trust/school's IT 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 trust will consider whether incidents that 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy/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 2.

This policy will be reviewed every year by the Chief Operations Officer. At every review, the policy will be shared with the trust 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.

## **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
- IT and internet acceptable use policy

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

ONLINE SAFETY TRAINING NEEDS AUDIT	
<b>Name of staff member/volunteer:</b>	<b>Date:</b>
<b>Question</b>	<b>Yes/No (add comments if necessary)</b>
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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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 INCIDENT LOG

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident