



# Online Safety Policy

## TPAT Policy Management

### Document history

<b>Review date</b>	<b>Version</b>	<b>Reviewer / owner</b>	<b>Executive approval</b>	<b>Approving body</b>	<b>Meeting date of policy approval</b>
11/2023	1	Director of IT	11/2023	FRAC	email approval 16 November 2023
11/2024	2	Director of IT	11/2024	FRAC	25/11/2024

### Material changes since last publication

<b>Section</b>	<b>Changes</b>
Version 2	No changes

This policy is reviewed annually. The next review is due by November 2025.

## **1. Introduction**

The Trust intends and expects that all decisions, policies and procedures will be underpinned at all times by its vision and values:

### **Our aim:**

To create centres of educational excellence that inspire all pupils to turn their potential into performance.

To achieve this our schools will:

- Provide a broad and balanced curriculum that allows pupils to develop their talents and ambitions.
- Deliver the highest quality learning opportunities facilitated by excellent teachers.
- Inspire our pupils to become confident, motivated and respectful individuals ready to make a positive contribution to society.

The Trust will support our schools by:

- Maximising the resources and expertise available to individual schools.
- Providing a platform for the sharing of excellent practice.
- Challenging and developing staff to turn their potential into performance.

### **1.1 Aims**

This policy is to ensure the online safety of all children, staff members, trustees, volunteers and visitors.

This will be accomplished through:

- Robust processes in place to ensure the online safety of everyone.
- Deliver an effective approach to online safety, cross Trust, which empowers us to protect by establishing clear mechanisms to identify, intervene and record.
- Providing clear boundaries of acceptable online behaviour.
- Appropriate use of Trust resources, both internally and remotely.
- Provide clarity of when schools should intervene with online safety issues.
- Regular information sharing and sign posting for parent advice.

## 1.2 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 Department's guidance on [protecting children from radicalisation](#), [Teaching about relationships, sex and health](#) and sharing nudes and semi-nudes: advice for education settings working with children and young people.

For additional information and guidance, please refer to the links above.

## 2. Roles and Responsibilities

School	Staff member	Role	Contact details	In position from
Abbey Park School	Mrs C Hopkinson	Online Safety Lead	HopkinsonC@abbeyparkschool.org.uk	Sept 2020
Bridlewood Primary School	Mr D Hilliker	Computing and Online Safety Lead	HillikerD@bridlewood.org.uk	Sept 2024
The Deanery C of E Academy				
Highworth Warneford School	Mr M Nye	Deputy Head	NyeM@warnefordschool.org.uk	Sept 2024
Kingfisher C of E Academy	Miss H Baddeley	Computing and Online Safety Lead	BaddeleyH@kingfishercofe.org.uk	Sept 2024
Orchid Vale Primary School	Mrs R Lee	Computing and Online Safety Lead	LeeR@orchidvale.org.uk	Sept 2024
Lydiard Park Academy	Mr W Day	Online Safety Lead	DayW@lydiardparkacademy.org.uk	May 2023
Red Oaks Primary School	Mr D Carter	Computing and Online Safety Lead	CarterD@redoaks.org.uk	Sept 2021

Red Oaks Primary School	Mrs B Taylor	Designated Safeguarding Lead	TaylorB@redoaks.org.uk	Sept 2015
Abbey Park School	Mrs K Stevens	Designation Safeguarding Lead	StevensK@abbeyparkschool.org.uk	
The Park Academies Trust	Mr G Bryan	Director of IT	BryanG@theparkacademiestrust.com	Feb 2014

### **\*Appendix I Reporting Concerns Flowchart**

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, 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 least annually.

Trust Board members 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 safeguarding and child protection policy.

Reporting will be overseen by the DSL / DDSL / OSL

### **2.1 The Trust Board**

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

The Trust 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 Trust Board members 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 (see Trust ICT Acceptable Usage Policy).

## **2.2 The Headteacher / Principal**

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school, with guidance from the Online Safety Lead.

## **2.3 The Designated Safeguarding Lead and Deputy Designated Safeguarding Lead**

Details of the school's DSL, DDSL and OSL 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 in ensuring that staff understand this policy and that it is being implemented consistently throughout the school through engagement with the Online Safety Lead.
- Working with the headteacher, Trust IT Support and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of online bullying are logged and dealt with appropriately in line with the school behaviour policy.
- CPOMS entries that are related to Online behaviours or incidents are shared with the Online Safety Lead when/if appropriate.
- Updating and delivering staff training on online safety with support from the Online Safety Lead.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or Trust Board with input from the Online Safety Lead.
- Regularly reviewing the monitoring alerts and logs produced by the Securus managed monitoring service

This list is not intended to be exhaustive.

## **2.4 The Online Safety Lead**

The lead for online safety is responsible for:

- Ensuring effective teaching and learning of online safety.
- Ensuring online safety issues are embedded in all aspects of the school.

- Raising awareness of online safety issues within the school and wider community.

## **2.5 Trust IT Support**

The Trust IT Support team is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis, blocking access to potentially dangerous sites and where possible preventing the downloading of potentially dangerous files.
- Ensuring that the Trust IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Ensuring that any online safety or cyber-bullying incidents are referred to the relevant parties as described in this policy.
- Ensuring that Monitoring solutions are active and fit for purpose.

This list is not intended to be exhaustive.

## **2.6 All staff and volunteers**

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Adhering to this policy consistently alongside the Trust ICT Acceptable Usage Policy.
- Ensure that any online safety or cyber-bullying incidents are logged.
- Making sure that children are regularly reminded of their responsibilities regarding online safety and behaviour.

This list is not intended to be exhaustive.

## **2.7 Parents**

Parents play a crucial role in ensuring that their children understand the need to use the technology in an appropriate way. The Trust will support parents to understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature.

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 the Trust ICT Acceptable Usage policy.

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

- What are the issues? - [UK Safer Internet Centre](#)
- Help & Advice for Parents - [Childnet International](#)
- Trust Online Safety Page - [The Park Academies Trust - Online Safety](#)

## **2.8 Visitors and members of the community**

Visitors and members of the community who use the Trust 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 IT and Acceptable Usage and Mobile Telephones.

**All staff should be aware of the content of this policy, and how it applies to themselves, children Parents/Guardians, Visitors, and members of the community.**

## **3. Educating children about online safety**

Children will be taught about online safety and the potential harm, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Children will receive the help and support of the school to recognize and avoid online safety risks and build their resilience.

Children will be taught the breadth of issues categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful content, for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: being subjected to harmful online interaction with other users; for example, peer-to-peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and non consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The computing curriculum covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact

on the internet or other online technologies.

Children should learn what positive, healthy and respectful relationships look like, following a scheme of work. In addition, teachers will also respond to any particular issues and concerns with individuals and classes as and when they arise, referring to the Online Safety Lead when appropriate.

Key online safety messages will also be reinforced across all areas of the curriculum. Children will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information. Children will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Schools will use assemblies to raise children's awareness of the dangers that can be encountered online and may also invite speakers to talk to children about this.

The Trust will raise parents' awareness of online safety in letters or other communications home, and in information via our website. This policy will also be shared with parents via newsletter and online link on Trust website.

#### **4. Educating parents about online safety**

There is information about keeping children safe online (including social media, apps and gaming) available on the Trust and School websites.

This can be accessed directly at:

<https://www.theparkacademiustrust.com/onlinesafety>

#### **5. Child on Child abuse via digital technologies**

All staff should be aware that children can abuse other children (often referred to as child-on-child abuse), and that it can happen both inside and outside of school and online. All staff should be clear as to the school's policy and procedures with regard to child-on-child abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it.

Child-on-child abuse via digital technologies is most likely to include, but may not be limited to:

- Bullying (including cyberbullying, prejudice-based and discriminatory bullying)



- Consensual and non-consensual sharing of nude and semi-nude images and/or videos  
(also known as sexting or youth produced sexual imagery)

[Keeping Children Safe in Education](#) references the following for guidance:

<https://www.farrer.co.uk/globalassets/clients-and-sectors/safeguarding/addressing-child-on-childabuse.pdf>

## **6. Digital Communications**

The Trust expects that all staff will ONLY communicate with Students and Parents via secure Trust approved systems, that can be monitored.

Where these are outside or pre-existing relationships, please refer to the Staff Code of Conduct Policy.

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

Where a child misuses the Trust Technology, we will follow the procedures set out in the ICT Acceptable Usage 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 Trust technology or a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct and our allegations management policy. 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.

All children, parents, staff, volunteers, LAB Members and Trustees are expected to sign the Trust acceptable use policy. Use of Trust technology 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 children, staff, volunteers, LAB members, Trustees and visitors to ensure they comply with the above.

## **8. Links with other policies**

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy (school specific)
- Behaviour Policy (school specific)
- Disciplinary Policy
- Data Protection Policy and privacy notices
- Complaints Policy
- ICT Acceptable Usage Policy
- Social Media Guidance
- Staff Code of Conduct

## Appendix 1 – Reporting Concerns Flowchart

# Reporting an Online Safety Incident

