



This Statement has been adopted and approved by Oxlip Learning Partnership and is to be used by all members of the Trust.

Online Safety – TRUST STATEMENT

Approved by Trust	13 th September 2024
Date of next Review	Autumn Term 2025-2026 (Annually and in line with KCSIE)
Responsible Officer	
Policy Number	

Definition of a Parent

For the purposes of education law, section 576 of the Education Act 1996 defines 'parent' as:

- all natural (biological) parents, whether married or not;
- any person who, although not a natural parent, has parental responsibility for the child or young person (this could be a step-parent, guardian or other relative);
- any person who, although not a natural parent, has care of a child or young person.

A person has care of a child or young person if they are the person with whom the child lives and who looks after the child, irrespective of what their relationship is with the child.

Introduction

All Online Safety policies in schools affiliated to Oxlip Learning Partnership should reflect the duty of care to students and employees, promote learning and teaching and high standards of attainment and progress.

Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and those in governance
- Identify and support groups of learners 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 school 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

Legislation

Our Online Safety policies will be 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](#)

They will also refer to the DfE's guidance on [protecting children from radicalisation](#) and reflect 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, policies will reflect 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 learners' electronic devices where they believe there is a 'good reason' to do so.

Our school policies comply with our funding agreement and articles of association.

Principles

Schools must, through their Online Safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.

The Trustees expect that the requirements set out in 'Keeping Children Safe in Education' are in place. Schools will ensure that appropriate filters and appropriate monitoring systems are in place and that children should not be able to access harmful or inappropriate material from the school's IT system.

In addition, the Policy should establish clear systems for monitoring and responding to misuse e.g. cyberbullying, accessing inappropriate materials.

The Policy should make it clear how learners will be taught about online safety as part of the school's curriculum, as well as how parents and carers will be informed and able to support this.

Categories of risk

Our approach to online safety is based on addressing the following four 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