UNICORN SCHOOL

IT ACCEPTABLE USE AND ONLINE SAFETY POLICY (PUPILS)

This policy applies to all pupils at Unicorn School, including those in the EYFS.

This policy links to the Privacy Notice and the Data Protection policy.

RESPONSIBILITY

Staff Member: Deputy Head/Bursar

Last Reviewed: February 2026

Next Review: September 2026

1. Policy Statement

Unicorn is committed to safeguarding and promoting the welfare of all children. Online safety is a key part of this responsibility, recognising that technology is a significant factor in many safeguarding concerns.

This policy sets out how we protect pupils from harm when using digital technologies, both in school and beyond, in line with statutory requirements, particularly **Keeping Children Safe in Education (September 2025)**. It should be read in conjunction with the Unicorn AI policy.

---

2. Legislative and Statutory Framework

This policy has regard to:

- *Keeping Children Safe in Education* (DfE, 2025)
- *Working Together to Safeguard Children*
- Education Act 2002 (Section 175)
- Data Protection Act 2018 and UK GDPR

---

3. Responsibilities

3.1 Governing Body

- Ensures this policy is implemented and reviewed annually
- Ensures appropriate filtering and monitoring systems are in place and effective
- Receives safeguarding and online safety training at induction and regularly thereafter

3.2 Headteacher

- Has overall responsibility for online safety
- Ensures staff receive appropriate training and updates
- Ensures safeguarding concerns are acted upon immediately

3.3 Designated Safeguarding Lead (DSL)

- Has lead responsibility for safeguarding and online safety
- Understands and oversees filtering and monitoring systems
- Manages referrals and information sharing
- Ensures online safety issues are recorded and escalated appropriately

Deputy DSLs are trained to the same standard.

---

4. Online Safety Risks (The 4Cs)

Being online can be a great source of fun, entertainment, communication and education. Some people's online behaviour places others at risk. The number of issues covered under online safety is large and constantly growing. They are categorised into these 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, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

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 children for sexual, criminal, financial or other purposes.

Conduct: 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. If children or members of staff report any issues, we will report it to the Anti-Phishing Working Group (https://apwg.org/).

---

5. Filtering and Monitoring

To limit children's exposure to online risks from Unicorn's IT systems, we have strong and effective filtering and monitoring systems, following the government's Meeting digital and technology standards in schools and colleges guidance. We will make sure that:

- specific staff have assigned roles and responsibilities to manage systems
- staff know about the systems in place and how to escalate concerns
- there are annual reviews of the systems, or more frequently if there is a significant change or issue
- our governing body reviews the systems with the DSL to find out what more can be done to keep children safe
- the systems are effective for the age range of children and consider children potentially at greater risk of harm
- when we block online content, it does not impact teaching and learning
- filtering works across all devices including mobile devices and smart technology

We currently use Untangle Firewall as our primary filter, and all staff use Apple Classroom when ipads are in use. At least once a year, laptops and ipads are checked using Testfiltering.com.

Information security and access systems
We have procedures in place to protect our IT systems and staff and learners from cybercrime, i.e. when criminals seek to exploit human or security vulnerabilities online to steal passwords, data or money directly. We will follow the government's Cyber security standards guidance. Our procedures and systems are reviewed regularly to keep up with the constant changes to cyber-crime technologies.

---

6. Mobile Devices and Smart Technology

Including how mobile phones, cameras and other electronic devices with imaging and sharing capabilities are used in the EYFS setting.

Our 'Use of Mobile Phones and Cameras Policy' sets out measures for safeguarding children in this area. There are also guidelines in the Staff Handbook. Key points are:

- Mobile phones are not used in EYFS.
- Staff must not consult their phones when they are responsible for children, both in classroom situations and in the playground.
- Staff should not use their mobiles to take photographs of children – the school cameras/ipads should be used for this purpose.
- At events, parents may take photographs on their phones on the strict understanding that the images are for personal use and must not be put into the public domain.
- Children should not bring smart phones, watches or any other smart technology to school without the express consent of the Headteacher. Consent will generally only be given in cases of medical or SEND need
- Children in Violet (Year Five) and below must not bring mobile phones into school.
- Ultra Violet children (Year Six) who are travelling to / from school on their own may bring a mobile phone but it must be a 'dumb' phone with no Smart capability, and kept in the School Office during the day.

Media recordings, audio, image and video (including digital files)

Parental permission must be granted before images are used on the school website or in printed publications. This is sought when the child starts at the Unicorn and parents have the right to alter their consent at any time. Where a photograph is used, the child is not named; if a pupil is named, their photograph is not used.

---

7. Teaching Pupils About Online Safety

IT and online resources are increasingly used across the curriculum. The School believes it is essential for online Safety guidance to be given to the pupils, parents and Staff on a regular and meaningful basis. Online safety is embedded within our curriculum and the School continually looks for new opportunities to promote it.

- The School has a framework for teaching online safety in Computing. These lessons are age-appropriate and progressive, inclusive of SEND pupils and focused on keeping safe rather than blame.
- The School also provides opportunities within a range of curriculum areas to teach about online safety;
- At least twice a year there are assemblies given on online safety;
- Staff receive training on online safety issues;
- The School invites outside experts to run regular workshops on online safety for children throughout the School (eg. Childnet)
- The School also invites outside experts to run regular parent workshops on online safety;
- Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also taught where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.
- Cyberbullying will not be tolerated and any instances will immediately be dealt with under the Anti-Bullying policy.

Remote education

When our children are being taught remotely e.g. at home, we will be in regular contact with parents and carers. We will make sure parents and carers are aware of:

- what their child/ren are being asked to do online, including the sites they will be accessing and who from the school will interact with their child/ren
- the importance of children being safe online and offering advice on how to do so
- what systems our school uses to filter and monitor online use

8. Generative Artificial Intelligence

Generative artificial intelligence (Gen AI) refers to technology that can be used to create new content (e.g. text, code and images) based on the data the models have been trained on. Our school is aware of the potential benefits of using Gen AI, such as for reducing staff's workload and freeing up teachers' time. At the same time, our school is aware of the risks and dangers associated with using Gen AI. We will use the Department for Education's advice and guidance on using Gen AI in education to ensure we integrate Gen AI tools safely and with children's best interests at the centre. Safeguarding concerns that arise through an individual's use of artificial intelligence will be responded to in line with our safeguarding policies. Our school's approach to using Gen AI is detailed in our separate AI Policy that can be found on the school's website.
