E-SAFETY POLICY

1. Introduction

The Ursuline Preparatory School recognises that safeguarding applies equally in the digital world as in the physical world. Online technologies provide powerful opportunities for learning, communication and collaboration; however, they also present potential risks.

This policy sets out how the school safeguards and promotes the welfare of pupils in relation to online safety in accordance with statutory guidance and inspection standards of the Independent Schools Inspectorate.

Pupils are taught how to stay safe online and how to mitigate risks including (but not limited to):

- Cyberbullying
- Grooming and sexual exploitation
- Radicalisation
- Harassment and stalking
- Identity theft and fraud
- Exposure to inappropriate content
- Online coercion and exploitation
- Misuse of artificial intelligence tools

Online safety is embedded within the school's safeguarding culture.

It is the duty of The Ursuline Preparatory School, Warley to ensure that every pupil in its care is safe; and the same principles apply to the digital world as it applies to the real world. ICT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe within an online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

This policy, supported by the IT Acceptable Use policy (for all staff, visitors, and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding
- Anti-Bullying;
- IT Acceptable Use Policy;
- Social Networking Policy;
- Artificial Intelligence (AI) Policy;
- E-Safety Policy

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of content online.

2. Scope of this Policy

This policy applies to:

- All pupils
- All teaching and non-teaching staff
- Governors
- Volunteers
- Visitors
- Contractors
- Parents and carers (where relevant)

It applies to:

- School-owned devices and networks
- Cloud-based systems (e.g. Office 365)
- Personal devices used on school premises (where permitted)
- Off-site use of school systems

3. Linked Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Behaviour Management Policy
- Anti-Bullying Policy
- IT Acceptable Use Policy
- Social Networking Policy
- Data Protection Policy / Privacy Notice

- Staff Code of Conduct

4. Governance and Leadership

4.1 Governing Body

The Governing Body:

- Ensures appropriate online safety and filtering systems are in place.
- Receives annual reports on filtering and monitoring effectiveness.

The Safeguarding Governor has specific oversight of online safety.
The IT Governor provides support when it comes to implementation of new initiatives to help improve the effectiveness of IT within the school, including the implementation of firewall's, internet filtering, IT Security, etc.

4.2 Headteacher and the Senior Leadership Team

The Headteacher and the Senior Leadership Team have overall responsibility for safeguarding, including online safety, and ensures:

- Effective implementation of this policy
- Adequate resourcing of filtering and monitoring systems
- Staff training and compliance
- Prompt response to online safety concerns

The Headteacher has delegated day-to-day responsibility to the IT Co-ordinator.

4.3 Designated Safeguarding Lead (DSL)

The DSL:

- Takes lead responsibility for online safety safeguarding concerns.
- Keeps up to date with national guidance and emerging risks.
- Liaises with local Safeguarding Partners.
- Refers cases to external agencies where appropriate.
- Maintains safeguarding records relating to online incidents.

The school's IT Co-ordinator and Designated Safeguarding Lead are responsible to the Headteacher for the day-to-day issues relating to e-safety.

4.4 IT Coordinator

The IT Coordinator:

- Maintains secure network infrastructure.

- Ensures appropriate filtering and monitoring systems are operational.
- Reviews filtering effectiveness termly.
- Escalates safeguarding concerns to the DSL.
- Oversees cyber-security procedures.

4.5 Teaching and support staff

All staff are required to sign the IT Acceptable Use Policy before accessing the school's systems.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

Pupils

Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

At the beginning of the year, pupils sign up to a ‘contract’ that outlines expectations on using any digital device both in school and at home. This contract is published on Showbie as an electronic reminder and displayed prominently in every classroom.

Parents and carers

Ursuline Preparatory School believes that it is essential for those with parental responsibility to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage.

The school organises a seminar to parents on an annual basis to provide information and training.

The school will always contact parents if it has any concerns about pupils’ behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school’s IT Acceptable Use Policy.

Education and training

- **Staff: awareness and training**

  New staff receive information on The Ursuline Preparatory School's E-Safety and IT Acceptable Use policies as part of their induction.
  All staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

  All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. These behaviours are summarised in the IT Acceptable Use Policy which must be signed and returned before use of technologies in school. Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

  A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's IT Coordinator and Designated Safeguarding Lead.

- **Pupils: E-Safety in the curriculum**

  ICT and online resources that are increasingly being used across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

  The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise. The school also arranges outside specialists to speak to pupils on a regular basis.

  At age-appropriate levels, pupils are taught about their e-safety responsibilities and to look after their own online safety. Pupils can report concerns to any member of staff at the school.

Pupils are also taught informally about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils may approach the Designated Safeguarding Lead as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

- **Parents**

  The school seeks to work closely with parents in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

  The school recognises that not all parents may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges a seminar for parents, which is led by external providers, giving advice about e-safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

5. Filtering and Monitoring

The school uses appropriate filtering and monitoring systems (LightSpeed Filter and Alert) to safeguard pupils from harmful and inappropriate content.

These systems:

- Block access to illegal and harmful material.
- Monitor network usage for safeguarding risks.
- Alert relevant staff to concerning behaviour.
- Are reviewed at least termly for effectiveness.
- Are overseen by the IT Coordinator and reported to Governors annually.
- Filtering and monitoring systems are age-appropriate and proportionate.

6. Education and Curriculum

Online safety is embedded across the curriculum and through:

- PSHE (Upper Two)
- Computing lessons
- Assemblies
- Form time discussions
- Visiting speakers and specialists

Pupils are taught:

- Safe online communication
- Privacy and digital footprints
- Critical evaluation of online content
- Respectful online behaviour
- Risks associated with social media
- The impact of cyberbullying
- Legal implications of online misuse
- Responsible and ethical use of Artificial Intelligence tools
- Online safety education is age-appropriate and progressive.

7. Artificial Intelligence (AI)

The school recognises the increasing use of AI tools.

Pupils:

- Must not use AI tools to generate harmful, inappropriate or misleading content.
- Must not input personal data into AI platforms.
- Must use AI only when authorised by staff.

Staff:

- Must ensure AI tools used in school comply with data protection law.
- Must not input confidential or personal data into public AI systems.
- Must supervise pupil AI use carefully.
- Must model responsible AI use.

The school monitors emerging risks associated with AI.

8. Use of Devices

8.1 Staff

- School devices must be password protected.

- Multi-Factor Authentication (MFA) is mandatory for accessing online platforms such as Office 365, CPOMS, Medical Tracker, etc.
- Personal devices may not be used in the presence of pupils unless authorised.
- Staff must not communicate with pupils via personal accounts.
- Pupils must not be added as social media contacts.

8.2 Pupils

- Personal devices are not permitted unless explicitly authorised.
- Smart devices must not be used without permission.
- Any misuse will be addressed under the Behaviour Policy.

9. Safe Use of Email and Online Communication

All users must:

- Communicate professionally.
- Avoid offensive or discriminatory language.
- Report concerning communications immediately.
- Not access inappropriate material.
- Staff must remain vigilant to phishing and cyber fraud attempts.

10. Data Protection and Storage

- The school complies with the Data Protection Act 2018, UK GDPR and the Data Use and Access Act 2025.
- All school-related data must be stored on approved cloud platforms.
- Personal data must not be stored on memory sticks.
- Devices must be encrypted where appropriate.
- Data breaches must be reported immediately.

11. Digital Video and Images

- Images and video must only be taken on school devices.
- Parental consent must be obtained before publication.
- Pupils' full names will not be used alongside images.
- Images must not be shared on personal social media platforms.
- Pupils must not take images of others without permission.

12. Reporting Concerns

Any member of the school community who has a concern about online safety must report it immediately to:

- The DSL
- The IT Coordinator
- The Headteacher (if appropriate)

All concerns are recorded using the school's safeguarding reporting system.

The school will refer to the following agencies where there is risk of significant harm:

- Local Safeguarding Partners
- Police
- National Crime Agency CEOP Command

13. Misuse and Sanctions

The school does not tolerate:

- Illegal activity
- Cyberbullying
- Harassment
- Accessing extremist material
- Sharing indecent images
- Discriminatory conduct

Sanctions will be applied in accordance with the Behaviour Policy.

14. Working with Parents

The school:

- Provides annual online safety information sessions.
- Communicates emerging risks to parents.
- Encourages open dialogue regarding online behaviour.
- Supports parents in implementing safe practices at home.

15. Complaints

Complaints relating to online safety should be addressed to the IT Coordinator or DSL in the first instance and they will undertake an investigation where appropriate.

Serious concerns may be escalated under the Complaints Policy.

Incidents of or concerns around e-safety will be recorded using a “Report of a concern” form, found as Appendix B of the Safeguarding and Child Protection Policy; and reported to the school's IT Coordinator and the Designated Safeguarding Lead in accordance with the school's Safeguarding and Child Protection Policy.

16. Monitoring and Review

This policy is reviewed annually or sooner if:

- There are significant safeguarding incidents.

- Statutory guidance changes.
- Technology developments necessitate updates.
- The Governing Body reviews online safety arrangements annually.