Upton Hall School

ONLINE SAFETY POLICY

'This policy will be implemented in a way which honours the vision that every FCJ school is a community of persons - students, staff, governors - bound together in mutual respect and ready to rely on each other in fulfilling their privileged task as educators in a Catholic school.'

Contents

1. Aims

Upton Hall School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- 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.

1.1 The Four 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, anti-Semitism, 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.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2025, 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.

It reflects existing legislation, including but not limited to the Education Act 2002, the Education (Independent School Standards) Regulations 2014 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 considers the national curriculum computing programmes of study and complies with our funding agreement and articles of association.

3. Roles and Responsibilities

3.1 Governing Body

The governing body has overall responsibility for monitoring this policy and holding the headmistress to account for its implementation.

The governing body 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).

The governor who oversees online safety is Mrs Micha Woodworth, safeguarding link governor.

All governors 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 (Appendix 2).
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for

vulnerable children, victims of abuse and some pupils with SEND 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.

3.2 Headmistress

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

3.3 Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our Safeguarding and Child Protection Policy, as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headmistress in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headmistress, 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 safeguarding and child protection policy.
- Ensuring that any online safety incidents are logged 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 3 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 Headmistress and/or Governing Body.

This list is not intended to be exhaustive.

3.4 Deputy Headteacher (Ethos and Personal Development)

The Deputy Headteacher takes lead responsibility for

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Ensuring that pupils are taught about the safe use of social media and the internet as part of the Flourish programme, particularly in relation to Relationships and Sex Education.

3.5 Director of Business

The Director of Business is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness (based on DfE filtering and monitoring standards) 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 school's ICT 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 school's ICT 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 5) 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 school's ICT systems and the internet (Appendix 2), and ensuring that pupils follow the school's terms on acceptable use (Appendix 1).
- Working with the DSL to ensure that any online safety incidents are logged 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

Parents are expected to:

- Notify a member of staff or the Headmistress of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendices 1 and 2).
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    - What are the issues? - UK Safer Internet Centre
    - Parent and carer support - Childnet International
    - Parents are encouraged to download the National Online Safety app, which aims to educate adults in online safety, so that they can help their child make informed decisions and stay safe online. Parents should enrol to Upton Hall using this link.

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT 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 (Appendix 3).

4. Educating Pupils About Online Safety

Online safety education at Upton Hall School FCJ is embedded across the curriculum and delivered through Computing and the Flourish Programme (our whole-school approach to PSHE and RSE). Our approach is proactive, age-appropriate, and responsive to emerging risks, ensuring pupils are equipped to navigate the digital world safely, confidently and in keeping with our Catholic values.

4.1 Curriculum Integration

Online safety is explicitly taught through:

- Computing lessons, which focus on safe use of networks, managing digital identity and passwords, online research skills and awareness of phishing and malware.
- The Flourish Programme, which addresses safe and respectful online relationships, digital consent, the impact of pornography, harmful content, online bullying and image-sharing.
- Religious Education, where themes of human dignity, ethical use of technology and responsible communication are reinforced.

In Key Stage 3, pupils are taught to:

- Use technology safely, respectfully, responsibly and securely, including how to protect their identity and privacy online.
- Recognise harmful content, contact and conduct and understand how to report concerns.
- Reflect on how faith, dignity and respect shape their online interactions.

In Key Stage 4, pupils build on this by:

- Understanding the changing nature of online risks and how to respond appropriately.
- Exploring the consequences of sharing and receiving explicit content (nudes and semi-nudes), online coercion, and digital reputation. **M**isogynistic or misandrist content, upskirting or coercive control online **are also explored.**
- Recognising the signs of online grooming, abuse and manipulation.

In Key Stage 5, the Flourish curriculum prepares students for adult life by covering:

- Digital literacy and managing digital footprints.
- Healthy online relationships, consent and boundaries.
- Understanding data usage, scams, online fraud and personal security.

By the end of secondary school, pupils will understand:

- That online behaviour should reflect the same high standards expected offline, rooted in respect and responsibility.
- The risks associated with harmful online content and the difficulty of removing material once shared.
- That it is a criminal offence to share, possess or view indecent images of children, even if created by children themselves.
- How personal data is collected, shared, and used**,** and how to manage privacy settings and report misuse.
- How to identify, avoid, and report online bullying, exploitation, abuse and harassment.
- That they are entitled to support and protection, and that speaking up is a strength.

4.2 Whole-School Reinforcement

Online safety is regularly revisited through assemblies, form time, themed weeks such as Safer Internet Day and sessions with external speakers, including police and safeguarding professionals.

Our Flourish curriculum includes up-to-date case studies, real-world scenarios and links to national guidance, supporting understanding across all key stages.

Pupil voice contributes to curriculum planning and helps identify emerging concerns.

4.3 Reporting and Support

Pupils are actively encouraged to speak up if they are worried about anything they encounter online. They can:

- Report concerns via the SpeakUp section of the Thrive Hub VLE.
- Speak to any trusted adult in school, including the Designated Safeguarding Lead or a Deputy DSL.
- Access signposted links for reporting online sexual exploitation and contacting the Police, clearly displayed in form rooms and on the school VLE.

We are committed to ensuring that every pupil knows how to report concerns safely, feels confident they will be taken seriously, and trusts that appropriate support will follow.

5. Educating Parents About Online Safety

The school will raise parents' awareness of internet safety in information evenings, letters or other communications, and in information via our website and social media accounts. This policy will also be shared with parents and they are able to create a National Online Safety account which provides many resources to help parents understand the risks that young people face online.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headmistress.

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Behaviour for Learning 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. Form tutors will discuss cyber-bullying with their form groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

All staff, governors 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 provides information on cyber-bullying to parents so that 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's Behaviour for Learning 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, including utilising the Safer Schools Police Officer.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will

be dealt with through the school complaints procedure.

7. Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the 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 and sixth form students on a daily basis. Internet use by staff, volunteers, governors and visitors (where relevant) will be monitored if there are low-level concerns, and through spot checks once per month to ensure they comply with the above. The school uses Impero software to monitor staff and pupils' use of the Internet.

More information is set out in the acceptable use agreements in Appendices 1 and 2.

8. Pupils Using Mobile Devices in School

Pupils may bring mobile devices into school, but are not permitted (with the exception of permission by staff) to use them during:

- Lessons
- Form time
- Clubs before or after school, or any other activities organised by the school.

During these periods phones must be turned off. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Behaviour for Learning policy, which will result in the confiscation of their device. See also Mobile Phone policy.

9. Staff Using Work Devices Outside School

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT Manager. Work devices must be used solely for work activities.

10. How the School Will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour for Learning policy. 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 school's ICT 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The DSL and Headmistress will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police or LADO.

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 the risks up.
- 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 deputies will undertake specific DSL training, which will include online safety, at least every two years. They will also update their knowledge and skills about 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 Safeguarding and Child Protection Policy.

12.Monitoring Arrangements

The DSL will log safeguarding incidents related to online safety in CPOMS.

The Deputy Headteacher will ensure behavioural incidents, including bullying, related to online safety are logged on SIMS.

This policy will be reviewed annually and in response to significant updates to KCSIE or emerging risks.

13.Links with Other Policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour for Learning Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT policy
- Social media policy

Appendix 1: KS3-5 Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a staff member • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teacher's first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. I have read and understand the sections around social media use etc. in the staff Code of Conduct. I understand there if low-level concerns arise from my use of technology, then this will be investigated.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Online Safety Training Needs – Self Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer: **Date**:	
Question	**Yes/No (add comments if necessary)**
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?	
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?	