The King's (The Cathedral) School

Online Safety Policy (formerly E-Safety Policy)

Responsibility:	Mr J Pinguenet
Ratified By:	Governing Body
Date Reviewed:	March 2026
Next Review Date:	March 2027

Contents

Online Safety Policy

1. AIMS

The King's (The Cathedral) 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.

The 4 Key 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, 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;
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. LEGISLATION AND GUIDANCE

This policy is 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.

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects 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, 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. This policy also reflects the Online Safety Act 2023, which places duties on online service providers to reduce illegal and harmful content and improve user safety.

This policy also takes into account the National Curriculum Computing programmes of study.

3. ROLES AND RESPONSIBILITIES

3.1 The Governing Body

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

The governing body will hold regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy;
- Agree and adhere to the terms stated in the Staff ICT Acceptable Use Policy and Agreement;
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures;
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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 THE HEADTEACHER

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

3.3 THE DESIGNATED SAFEGUARDING LEAD AND DEPUTIES

Details of the school's designated safeguarding lead (DSL) and Deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The Deputy Designated Safeguarding Lead (DDSL) with responsibility for online safety will take 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;
- Working with the Headteacher, ICT 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 child protection policy;
- Ensuring that any online safety incidents are logged on MyConcern (the school's safeguarding recording system) 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;
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the headteacher and/or governing body.

This list is not intended to be exhaustive.

3.4 INFORMATION AND COMMUNICATIONS MANAGER

The ICT Manager 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 and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including

terrorist and extremist material - the recommended health check of IT systems is annually, but ours reviewed/updated constantly;
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly - AV software is dynamically updated 24/7;
- Conducting a full security check and monitoring the school's ICT system: our system is actively scanning 24/7 with a full scan per computer each day. All files opened on a computer from CDs & USB sticks are actively scanned on detection. Likewise so are emails. Files already on the network (located on the servers, are scanned daily);
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files - Smoothwall (school's firewall & web filter hardware/software) fulfils this and is dynamically updated.

This list is not intended to be exhaustive.

3.5 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 ICT Policy (by reading, adhering to and signing the policy) see Staff ICT Acceptable Use Policy and Agreement;
- Working with the DSL to ensure that any online safety incidents are logged on My Concern 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, including grooming, coercion, exploitation, sextortion and image-based abuse, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.6 PARENTS

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 acceptable use of the school's ICT systems and internet see STUDENTS' ACCEPTABLE USE OF ICT FOR THE KING'S SCHOOL NETWORK AND THE WORLD-WIDE WEB.

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

- What are the issues? - UK Safer Internet Centre;
- Hot topics - Childnet International;
- Parent resource sheet - Childnet International.
- NSPCC – Keeping Children Safe Online

3.7 VISITORS AND MEMBERS OF THE COMMUNITY

Visitors 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 the Staff ICT Acceptable Use Policy and Agreement.

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of either the Computing or Learning for Life (LfL) curriculum:

All schools have to teach:

- Relationships education and health education in primary schools;
- Relationships and sex education and health education in secondary schools.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly;
- Recognise acceptable and unacceptable behaviour;
- Identify a range of ways to report concerns about content and contact.

By the **end of Year 6**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not;
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous;
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;
- How information and data is shared and used online;
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy;
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
- How to report a range of concerns.

By the **end of Year 11**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online;

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online;
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them;
- What to do and where to get support to report material or manage issues online;
- The impact of viewing harmful content;
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners;
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail;
- How information and data is generated, collected, shared and used online;
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours;
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

The safe use of social media and the internet will also be covered in other subjects where relevant.

Emerging technologies and artificial intelligence (AI): The school recognises the increasing role of artificial intelligence (AI), live streaming and emerging technologies in pupils' online experiences. Staff will support pupils to understand both the opportunities and risks associated with these technologies, including misinformation, deepfakes and privacy risks. Teaching and acceptable use in relation to AI will be delivered in line with the school's Artificial Intelligence (AI) Policy.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. EDUCATING PARENTS ABOUT ONLINE SAFETY

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

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

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

6. ARTIFICIAL-INTELLIGENCE

Refer to 'AI Acceptable Use Policy' which has more detail about the risks associated with the use of AI and a statement for students to confirm they understand its acceptable use.

7. CYBER-BULLYING

7.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and Anti Bullying policy.)

7.2 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 are actively encouraged to discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Learning for Life (LfL), and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets 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 behaviour 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.

The DSL or DDSLs will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

8. EXAMINING ELECTRONIC DEVICES

Any searching or examination of electronic devices should be conducted according to our Behaviour Policy, referring to section 9 - The Right to Search

If inappropriate material is found on the device, it is up to DSL/DDSLs or Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person; and/or
- The pupil and/or the parent refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not view the image;**
- Confiscate the device and report the incident to the DSL (or DDSL) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation;
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people;
- Our Behaviour Policy;
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

9. 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 on the Students' Acceptable Use of ICT for the King's School Network and the Internet document.t. 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 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 Care Code of Conduct Policy. The 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.

10. 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 up the risks;
- 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 DDSLs 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 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 child protection and safeguarding policy.

11. MONITORING ARRANGEMENTS

- The school will review filtering and monitoring provisions at least annually, ensuring they are effective and up to date.
- The IT network manager is responsible for managing filtering and monitoring systems, with a daily report from Smoothwall sent to the DDSL responsible for online safety
- Smoothwall software ensures that systems block harmful and inappropriate content without unreasonably impacting teaching and learning.
- All incidents in relation to risks with online safety will be logged on MyConcern (the school's safeguarding recording system).

This policy will be reviewed every year by the DDSL responsible for online safety. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

12. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy;
- Behaviour policy;
- Staff Code of Conduct Policy;
- Complaints Policy;
- AI Acceptable Use Policy
- Staff ICT Acceptable Use Policy and Agreement and STUDENTS' ACCEPTABLE USE OF ICT FOR THE KING'S SCHOOL NETWORK AND THE WORLD-WIDE WEB.