Kimbolton School
Cambridgeshire

ONLINE SAFETY POLICY

Policy owner: This policy is the responsibility of the Designated Safeguarding Lead / Online Safety Lead.
Governor Committee: People & Culture
Policy Summary Statement: The purpose of this online safety policy is to ensure a secure digital environment for students and staff by promoting responsible internet use and protecting against risks like cyberbullying, inappropriate content, and privacy breaches. This policy provides guidelines and tools to help the school community engage safely and ethically online, fostering a safe digital space that supports learning.

Release Date:	Autumn 2024
Review Date:	Autumn 2025

Kimbolton School
Cambridgeshire

Online Safety Policy

CONTENTS

Kimbolton School
Cambridgeshire

Online Safety Policy

INTRODUCTION

This Policy is linked to the

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Anti-Cyber Bullying Policy
- Staff and Pupil AUA
- 'Prevent Duty' Risk Assessment

PRINCIPLES

Kimbolton School is committed to providing a safe and secure environment for children, staff and visitors and promoting a climate where children and adults will feel confident about sharing any concerns which they may have as a result of online safety issues.
We recognise the need to be alert to the risks posed by strangers or others (including the parents or carers of other pupils) who may wish to harm. We will take all reasonable steps to lessen such risks by promotion of online safety and Acceptable Use policies that are clearly understood and respected by all.
The policy is applicable to all onsite and offsite activities undertaken by pupils whilst they are the responsibility of the School.

PURPOSES

- To outline the nature of online safety and how staff and pupils may identify it.
- To identify simple ways in which online safety issues can be reported to responsible adults.
- To provide a clear policy and guidelines to enable online safety to be tackled effectively.

LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2024, and its advice for schools on:

- Teaching online safety in schools. Preventing and tackling bullying and cyberbullying: advice for head teachers and school staff.
- Searching, screening and confiscation, with a particular focus upon filtering and monitoring.
- Harmful online challenges and online hoaxes.

GUIDELINES

Why the internet and digital communications are important

- The internet is an essential element in 21st Century life for education, business and social interaction. The School has a duty to provide pupils with high-quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

Internet use will enhance and extend learning

- Staff will be made aware of, and pupils will be educated in, the safe use of the internet.

- Clear boundaries will be set and discussed with staff and pupils for the appropriate use of the internet and digital communications.
- Staff and pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate internet content

- School should ensure staff and pupils understand that the use of internet-derived materials should comply with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught about how to be safe when online

Online Safety is taught through all years, either through tutor times or embedded into the school PSHE curriculum. The approach is to ensure students know how to keep themselves safe online, inside and outside of school, as strong as possible. The PSHE curriculum includes, but not limited to:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by people they have met online.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyberbullying.
- Access to unsuitable video / internet games.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Harmful online challenges and online hoaxes.

Information system security

- The ICT system security will be reviewed regularly by the Network Manager.
- Virus protection will be installed and updated regularly.

Email

- Pupils and staff should only use approved curriculum email accounts in school and when working on school business. Prep School pupils do not have a school email account.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils must report if they receive an offensive or inappropriate email to a relevant member of staff or the Online Safety Lead; Ms V Garratt, vkg@kimboltonschool.com
- In email communication, pupils must not reveal their personal details, or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated as suspicious, and attachments not opened unless the author is known.

Published content and the School website

- Staff or pupil personal contact information will not be published.
- The contact details of staff given online will be a person's official school email address.
- The School's PR & Communications Manager will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully so that images of individual pupils cannot be misused.
- Written permission from parents or carers, using the approved permission form, will be obtained before photographs of pupils are published on the School website.
- Work can only be published with the permission of the pupil.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be capture using school equipment; the personal equipment of staff should not be used for such purposes. Images once stored on the school network should be deleted from the devices.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- In the Early Years, phones and cameras should not be used unless in an emergency (see Safeguarding and Child Protection Policy).

SOCIAL NETWORKING AND PERSONAL PUBLISHING

The School will educate pupils in the safe use of social networking sites. Pupils will be advised to make their profiles as private and secure as possible. They are taught to consider the appropriate and safe times when they can give out personal details which may identify them, their friends, or their location. The online lessons are focused on the four key areas:
Context – Conduct – Contact – Commerce
Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
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 them 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 nonconsensual 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.

- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now, or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils should only invite known friends and deny access to others.
- Pupils will be taught about being resilient to radicalisation, with an awareness made to the different ways that this may occur, including grooming (see Prevent Duty in the Safeguarding Policy).

Managing monitoring and filtering

- If staff or pupils discover an unsuitable site, it must be reported to the Network Manager or Online Safety Lead.

- ICT Support will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Terminology related to specific forms of radicalisation will be added to the school filtering system in order to protect pupils.
- All staff will follow the School's safeguarding procedures if any changed behaviour is observed.
- The School uses Securus and FastVue software to scan the content of searches/emails connected to the School's Wi-Fi system for any potential emerging concerns for safety. This is also supported via intermittent Boxphish online safety online training courses and TES Develop EduCare training courses.

Managing webchat

- Webchat will only occur under the direct supervision of a teacher who will, as far as reasonably possible, ensure it is appropriate and safe.
- MS Teams and Showbie are the only online virtual learning system that teachers can use. Lessons/communication should be in groups and two members of staff should be invited to attend the session. Only one has to be present, however the other member of staff could pop in if need be. If this is not possible, then the member of staff needs to record the session and store in a department folder.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit before use in school is allowed.
- The School is aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communication.
- Where contact with pupils is required to facilitate their safety (e.g. on school trips), staff will be issued with a school phone.
- The sending of abusive or inappropriate text messages is forbidden.
- It should be noted that games machines, including the Sony Playstation, Microsoft Xbox and others, have internet access which may not include filtering, therefore staff must ensure due care is given when used in school, or particularly in the Boarding Houses.

Managing social media - both Private and for official School use

- This applies to social networking sites (e.g. *Facebook, Instagram, SnapChat, TikTok*), blogs, microblogs such as *X (formerly known as Twitter)*, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia*, and content sharing sites such as *Flickr, YouTube, Twitch and Kick*.
- Users should be conscious at all times of the need to keep personal and professional/school lives separate. They should not put themselves in a position where there is a conflict between the School and their personal interests.
- Users should not engage in activities involving social media which might bring Kimbolton School into disrepute.
- Users should not represent their personal views as those of Kimbolton School on any social medium.
- Users should not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations or Kimbolton School.

Personal use of social media

- Pupils should not have contact through any personal social medium with any member of staff, other than those mediums approved by the Senior Leadership Team, unless the staff concerned are family members. This stipulation remains extant for two years after the pupil has left Kimbolton School. Those pupils departing the School before the end of the Upper Sixth should not be in direct social media contact until the age of 21.

- Photographs, videos or other types of images of pupils and their families, or images depicting staff members, clothing with school logos or images identifying school premises, should not be published on personal, non-private or public web space without prior permission from the School.
- All staff and pupils are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. All staff and pupils should keep their passwords confidential, change them often and be careful about what is posted online.
- We accept that some sites may be used for professional purposes to highlight a personal profile with summarised details, e.g. LinkedIn. We advise that care is taken to maintain an up-to-date profile and a high level of presentation on such sites if Kimbolton School is listed.

Using social media

- The School's PR & Communications team have full responsibility for running the School's official website, Facebook, X (formerly known as Twitter) sites and Instagram.
- Staff wanting to set up departmental Facebook, Instagram or X (formerly known as Twitter) feeds must have permission from the Online Safety Lead and be followed accordingly.
- The School's YouTube channel is the full responsibility of the Head of Digital Learning.
- Whilst pupils and the wider school community are encouraged to interact with these social media sites, they should do so with responsibility and respect.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to GDPR 2018 and the School's Data Protection Policy.

Authorising access

- All staff must read and sign the Staff Acceptable Use Policy before using any school ICT resource, including iPads issued for professional use.
- The School will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- All Senior School pupils must read and sign the Pupil Acceptable Use ICT and iPads Agreement before using any school ICT resource. All iPads will be registered with the School's MDM system.
- Acceptable Use Agreements are reviewed at the end of each school year, in preparation for the new academic year. Pupils will re-sign if the AUA is amended in the light of new developments.
- Prep School pupils should not be left unsupervised when using the internet in lessons.

Assessing risks

- The School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the School network. The School cannot accept liability for any material accessed, or any consequences of internet access.
- Staff should apply due diligence to assess the suitability of online resources, internet sites etc, before sharing/recommending with others.
- Every year, the School will audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective. The School will ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the School.

- Any complaint about staff misuse must be referred to the Headmaster and, if the misuse is by the Headmaster, it must be referred to the Chair of Governors in line with the School's Safeguarding and Child Protection procedures.
- Pupils, parents, and staff will be informed of the Complaints Procedure.

Communicating Online Safety and introducing the Online Safety Policy to pupils

- Online Safety rules will be distributed to all pupils at the start of the academic year, and they are requested to save them on their iPads. All system users are informed that network and internet use will be monitored.
- A programme of Online Safety training and raising of awareness will occur during PSHE lessons.
- A Digital Leaders Programme for Sixth Form students to help communicate Online Safety to the rest of the School. Some of their responsibilities include but not limited to: Producing and delivering assemblies about online safety; Promoting the acceptable use of devices; Demonstrating how to use new apps or programs; Organising Safer Internet Day; Trying out and reviewing new apps, websites and programs which could be used in lessons.

Staff and the Online Safety Policy

- New staff have a session on online safety as part of their induction.
- All staff will be given access to the School's Online Safety Policy and its importance explained. Staff must be informed that network and internet traffic can be monitored and traced to the individual user, including staff laptops and iPads.
- Staff that manage filtering systems, or monitor ICT use, will be supervised by senior leadership and ensure clear procedures for reporting issues.
- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings, or even malicious accusations. Staff must take care to always maintain a professional relationship.

Reporting Online Safety breaches

- All members of the school community should be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless, irresponsible or, very rarely, deliberate misuse.
- No definition of 'indecent' material has been written in law and it is up to interpretation by a jury.

As guidance:
Unsuitable material = any information or images relating to;

- Extreme violence that can cause upset to a child;
- Racist material;
- Pornography
- Radicalisation
- Swearing
- Violence/cruelty
- Bullying
- Gambling
- Sites which encourage vandalism, crime, terrorism, eating disorders or suicide.
- Unmoderated chat

Illegal material = anything illegal in the real world is illegal in the digital world;

- Child exploitation
- Child abuse
- Grooming

Monitoring

- Staff report and log concerns of incidents regarding behaviour and safeguarding issues related to online safety on CPOMS. The Online Safety Lead and the Designated Safeguarding Lead.
- The Online Safety Lead will ensure that full records are kept of incidents.
- These records will be reviewed termly by the Online Safety Lead. The Designated Safeguarding Lead and Senior Deputy Head will review them when a serious incident occurs.

Enlisting parents' and carers' support

The School is committed to raising parents' awareness of internet safety and will provide information and to parents and carers through:

- The attention of parents and carers will be drawn to the School's Online Safety Policy on the school website.
- The School will maintain a list of online safety resources for parents/carers on the school website.
- The School will signpost support and make clear how parents/carers should report any issues or concerns on the school website.