KEW COLLEGE PREP

Online Safety Policy

This policy applies to the whole school including EYFS

This policy is written with due regard to the following:

Keeping Children Safe in Education (KCSIE) (Sep 2025)
Working Together to Safeguard Children (Jul 2023)
Data Protection Act (1998)
ISI Handbook for the Inspection of Schools: Commentary on the Regulatory Requirements (Sep 2023)
The Prevent Duty: Departmental Advice for schools and childminders (Sep 2023)
Prevent Duty guidance: for England and Wales (Sep 2023)
UKCCIS Guidance on Sexting in Schools and College (2016)
Teaching Online Safety in Schools (Jan 2023)
The use of social media for online radicalisation (Jul 2015)
DfE: Relationships Education, Relationships and Sex Education (RSE) & Health Education (Sep 2021)
DfE "Plan technology for your school" service (filtering/monitoring standards, signposted in KCSIE 2025)
DfE Guidance Generative AI: Product Safety Expectations (Jan 2025)

See also the school's policies as follows:
Safeguarding and Child Protection Policy, Staff Guide to School Procedures, Staff Code of Conduct, Anti-Bullying Policy, Anti-Cyber Bullying Policy, Implementing Prevent Policy, Record Retention Policy, Whistleblowing Policy and Procedures

Definitions or abbreviations used in this policy

DFE: Department for Education
DPA: Data Protection Act
DSL: Designated Safeguarding Lead
EYFS: Early Years Foundation Stage
ICT: Information and communication technology
IT: Information Technology
ISP: Internet Service Providers
KCSIE: Keeping Children Safe in Education
PSHEE: Personal, Social, Health and Economic Education
The School: Kew College Prep
UKCCIS: UK Council for Child Internet Safety
URL: Uniform Resource Locator
WSUS: Windows Server Update Service

At Kew College Prep

DSL: Sarah Jones
Deputy DSL and Head: Jane Bond
Deputy DSL Early Years: Lee-Anne Tizard

Latest resources promoted by DfE can be found at:

- www.saferinternet.org.uk
- www.thinkyouknow.co.uk
- www.kidsmart.org.uk
- www.childnet.com
- www.commonsense.org/education/uk/digital-citizenship

https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

1. Introduction

This Online Safety Policy outlines the commitment of Kew College Prep to safeguard members of our school community online in accordance with statutory guidance and best practice.

This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school.

2. Roles and responsibilities

The following is a list of roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our safeguarding policy:

Role:	**Key Responsibilities:**
Head & DSL	• As set out in KCSIE, hold the lead responsibility for online safety, within their safeguarding role • receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety • meet regularly with the governor in charge of Safeguarding to discuss current issues, review (anonymised) incidents and filtering and monitoring logs, ensuring that annual (at least) filtering and monitoring checks are carried out • attend relevant governing body meetings/groups • report regularly to headteacher/senior leadership team • responsible for monitoring, responding and resolving reports of online safety incidents and deciding on the most appropriate course of action which could include a safe space chat, targeted support in school or a referral by liaising with relevant agencies, ensuring that all incidents are recorded on SchoolBase liaise with staff on matters of safety and safeguarding and welfare (including online and digital safety)
Director of Studies	• ensure that the curriculum throughout the school makes the best use of technology and the pupils follow appropriate programmes of study both to develop the necessary technological skills and to keep themselves safe
Privacy Officer (IT) & Deputy Head	• work closely with the DSL • receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments

	• have a leading role in establishing and reviewing the school online safety policies/documents using the DfE's 'Plan technology for your school' service to assess and improve systems against filtering and monitoring standards • promote an awareness of and commitment to online safety education • ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents • provide (or identify sources of) training and advice for staff/governors/parents/ carers/pupils • receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) regarding the areas defined In Keeping Children Safe in Education • Follow government guidance on how filtering and monitoring requirements apply to the use of generative AI in education and supports schools to use generative AI safely
ICT Teacher	• teach all pupils at the beginning of each academic year about appropriate use and ensure throughout the year that safe use of the internet is taught and understood by the pupils • ensure pupils are educated in an age-appropriate manner to keep themselves safe and understand the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults, and to adjust their behaviour as necessary • ensure children are aware of the online safety risks posed by misinformation, disinformation, and conspiracy theories, often presented in convincing ways through AI generated material • discuss the '***Rules for Pupils***' and '***Responsible Internet Use***' documents with pupils, which are located in their school diaries. Any pupil who misses this lesson will meet the ICT teacher separately to discuss these matters
Website & Social Media Contributors	• ensure the safeguarding of any children appearing on our public website by omitting surnames and any details • ensure pupil images on the public part of the website are only used where photographic parental consent has been received
Teachers	• each time a member of staff logs on to their own account, they are shown a reminder of the school rules and regulations which they must agree to before logging into the system • staff have their own school email addresses • staff should adhere to use of computers in line with the ***Staff Guide to School Procedures*** and ***Staff code of conduct*** • staff can only access the school network offsite through a secure log on • any photographs taken for School purposes must only be taken and stored on the school network and not on any personal device
Pupils	• pupils are instructed in acceptable (i.e. responsible and safe) use of the Internet • pupils in Years 3 to 6 are given a copy of the "***Rules for Pupils***" in their diaries and are, along with their parents, required to sign the "***Responsible Internet Use***" form in each year before their children are allowed to use the internet • Pupils from Nursery to Year 2 use a generic User identity monitored by the teacher

	• Pupils from Year 3 upwards have their own school based individual email account • are informed that their Internet use & computer use will be monitored at all times • each time a pupil logs in to their own account, they are shown a reminder of the school rules and regulations which they must agree to before logging into the system • as part of the PSHEE provision at Kew College Prep, the Relationships Education curriculum and the ICT and computing curriculum pupils are taught how to keep themselves safe online and to understand the risks posed by adults or young people • are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement and ***Online Safety Policy*** • should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so • should know what to do if they or someone they know feels vulnerable when using online technology • should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's ***Online Safety Policy*** covers their actions out of school, if related to their membership of the school
All staff, volunteers, and contractors	• new staff are introduced to the school's systems as part of their induction training; should they require further training they should contact the Deputy Head or Privacy Officer (IT) • safe internet use is a regular feature of staff safeguarding training which is compulsory every year • to read, understand, sign and adhere to the ***Staff Guide to School Procedures***, ***Employee Handbook*** and the ***Staff Code of Conduct*** (where relevant) • understand any updates annually • to report any suspected misuse or problem to the Privacy Officer (IT) or Deputy Head • to model safe, responsible, and professional behaviours in their own use of technology • the Prevent Strategy, incorporating online radicalisation, is known to all staff following workshops and online tutorials
Parents & Carers	• understand that they play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way The school will take every opportunity to help parents and carers understand these issues through: • publishing the school ***Online Safety Policy*** on the school website • providing them with a copy of the pupils' acceptable use agreement in their child's diaries • publish information about appropriate use of social media relating to posts concerning the school. • seeking their consent concerning digital images. • parents'/carers' evenings, newsletters and social media.

3. Monitoring and filtering

- Provision of a buffer between Kew College Prep and the Internet which is designed to ensure children are safe and enhance performance.
- The school uses appropriate filtering and monitoring systems to protect pupils from harmful and inappropriate content, including material that can promote extremism, radicalisation or bullying. The school recognises the risks posed by the spread of misinformation, disinformation, conspiracy theories, and AI-generated content.
- Real time monitoring with automated alerts through Netsupport/classroom.cloud DNA monitoring system.
- Filtering is provided by Smoothwall to ensure staff and pupils are protected, content reviewed and sites blocked. The filtering software, used and monitored by the Kew College Prep Network, contains a number of lists or categories of URLs that can be marked as allowed or denied. These lists are updated frequently. Any unsuitable sites that are discovered by pupils or staff are reported to the IT Department; it is then reported to the ISP to add to the block list
- Sites that are within disallowed categories are blocked automatically. This mechanism provides an additional 'safety' check. It also allows for many more sites than would conventionally be available, using the simple 'allowed list' system used by other filtering applications.
- Safe search settings are employed in Microsoft Edge and Google. Bing is not accessible due to its inability to filter correctly under safe searches.
- Monitored and filtered email for pupils.
- Email anti-virus – to scan all unencrypted external and internal email delivered to the Kew College Prep Network, using anti-virus system that are kept constantly up to date
- Microsoft Critical Updates: distribution of Microsoft critical security updates services WSUS (school's responsibility to ensure computers are kept updated).
- The school will make use of the DfE's 'Plan technology for your school' service to assess compliance with filtering and monitoring standards and receive recommendations on strengthening our systems.
- Statutory UK ISP monitoring laws – Records all Internet usage and email. The Head will be informed when grooming or abuse is suspected.

4. Reporting mechanisms

There are various reporting mechanisms in school that should be used as follows:

- Termly risk assessments - these should refer to any technology in the relevant area including electrical hazards, trip hazards.
- An IT Helpdesk for speedy electronic reporting of maintenance issues staff may face.
- Pupil Misuse: any complaints about pupil misuse should be referred to the IT Manager and to the DSL in the first instance, and to the Head if relevant. Pupils misusing or unsafely using any of the school's software will also be taught about why their behaviour was unsafe and any safeguarding concerns followed up by the DSL.
- Smoothwall provides updates on a daily basis of items reported to key staff and for more serious issues to the Deputy Head and the Head for clearance. Any safeguarding issues will

immediately be reported to the DSL, who will deal with the matter in accordance with the schools ***Safeguarding and Child Protection Policy.***

- Concerns over the use of IT, including use of mobile telephones and cameras, sending of images via the internet or by texting, inappropriate material appearing on the screen, inappropriate use of IT by a pupil, parent or staff member, must be reported immediately to the Deputy Head unless this comes under child protection in which case the Head and DSL should be informed immediately. If the concern is about the Head, then the Chair of Governors should be contacted without the Head being informed.
- Children who are working online have clear reporting routes to staff so that they know who they can turn to in the event of online abuse or feeling unsafe online.

5. Use of Mobile Technology by pupils

The use of personal devices, such as mobile phones, iPads, tablets or laptops, by pupils is not allowed in school, unless specific permission has been given i.e. approved laptop use instead of handwriting.

Pupils in Year 6 only, who wish to bring a mobile phone to school as they are travelling to school independently, must hand it in to a member of staff on the gate upon arrival at school and may then collect it at the end of the day. It must be switched off whilst pupils are at school.

No other pupil is permitted to bring a mobile phone to school. No child should have a mobile phone on their person or in their bag during school hours. If a pupil is found to have one, it is removed, held in the office and handed to the parent, guardian or carer the end of the day. The child will be disciplined in accordance with the school ***Good Behaviour and Discipline Policy***.

Certain pupils are allowed to use a laptop in lessons and/or exams because of specific learning difficulties.

The school's supply of ipads, laptops and Surface Go tablets is restricted to lesson time when staff are able to supervise their use.

6. Management of personal data

The school has a need to process personal data and follows the principals of the Data Protection Act (DPA) and General Data Protection Requirements to ensure that personal data:

- Is processed fairly and lawfully
- Is obtained only for lawful purposes and is not further used in any manner incompatible with those original purposes
- Is accurate and, where necessary, kept up to date
- Is adequate, relevant and not excessive in relation to the purposes for which it is processed
- Is not kept for longer than is necessary for those purposes
- Is processed in accordance with the rights of data subjects under the DPA
- Is protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction, or damage; and

- Is not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information
- Is aware that GDPR does not limit sharing of information when required to identify children at risk of harm and to safeguard children from harm

For the purposes of the DPA, Kew College Prep is the "data controller" of personal data about pupils and their parents and/or guardians.

6.1 Personal data processed by the school

Personal data processed by the school includes contact details, national curriculum and other assessment results, attendance information, special educational needs, and images of pupils engaging in school activities and, in relation to parents and/or guardians, may include financial information. The school may also process sensitive personal data such as ethnic group, religious beliefs and relevant medical information. Personal data will usually be collected directly from parents / guardians, but some may be passed to the school by third parties.

6.2 Purposes for which personal data may be processed

Personal data (including sensitive personal data, where appropriate) is processed by the school strictly in accordance with the Data Protection Act in order to:

- Support its pupils' teaching and learning
- Monitor and report on their progress
- Publish examination results (as separately notified to affected pupils and/or their parents and/or guardians)
- Provide appropriate pastoral care
- Assess how well the school as a whole is doing
- Communicate with former pupils
- Monitor pupils' email communications, internet use and telephone calls for the purpose of ensuring compliance with the school's ***Online Safety*** and ***Anti-Cyber Bullying Policies***
- Where appropriate, promote the school to prospective pupils (including through the school's prospectus, School Magazine and website), and
- Other reasonable purposes relating to the operation of the school.

7. Online Safety and Remote Learning

As set out in KCSIE guidance, Kew College Prep online safety is the responsibility of the DSL who works with staff to promote safe practice across the school and with parents and pupils to support safe practice at home.

In line with the DFE's Guidance Teaching online safety in school (June 2019), pupils are taught about online safety and harms in their IT lessons, through their PSHEE lessons and through Relationships Education in an age-appropriate way. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies. They are taught the underpinning knowledge to help them navigate the online world safely and confidently regardless of the device, platform or app. This includes:

- how to help them evaluate what they see online

- how to recognise techniques used for persuasion
- how to identify online risks
- to understand what acceptable and unacceptable behaviour looks like, and
- how and when to seek support.

At induction and through regular annual training, staff are trained in the role of technology in both safeguarding and wellbeing issues, and that online abuse can occur in tandem with face-to-face abuse. Any concerns related to online abuse will be dealt with in line with Kew College Prep's ***Safeguarding and Child Protection Policy***. Referrals will be made to Richmond and Kingston SPA, and the police may also be contacted when deemed necessary and appropriate.

Children who are working online in school or at home, have clear reporting routes to staff so that they know who they can turn to in the event of online abuse or feeling unsafe online. Parents, pupils and staff are aware of the role of the DSL and Deputy DSL in reporting online safety matters.

Child Sexual Exploitation and Child Criminal Exploitation can be facilitated through online platforms such as the Web and Social Media Apps. Child on child abuse and initiation or hazing type of violence and rituals may include an online element. It is important that parents are aware of their child's online activity which extends beyond the school's online learning platform. Parents, carers, teachers and other Kew College Prep staff should immediately draw to the attention of the DSL or Deputy DSL any activity that might be related to CSE and/or CCE. Parents have the option to reach out to a range of support organisations including the Richmond and Kingston SPA. Kew College Prep, via the National Online Safety platform, provides a wide range of informational video clips and courses to support our parent community to recognise, respond to and manage suspected Child Sexual or Child Criminal Exploitation.

7.1 Procedures adopted to safeguard children while learning remotely

At times, it may be necessary for Kew College Prep pupils to receive their lessons via a secure remote learning platform. If this is necessary, Kew College Prep will provide guidance for its parents for keeping our children safe online whilst working at home, together with colourful posters for pupils highlighting key points for keeping them safe online. Parental consent is required for children to participate in online schooling and to submit videos and pictures of themselves; this consent can be changed at any time through Schoolbase.

Information is also provided to parents in the form of lessons to be provided (for example, live stream lessons or pre-recorded lessons) and the conduct expected of staff, pupils and parents. Staff are trained regarding the appropriate use of using pre-recorded videos/Powerpoint presentations, live lessons and/or photographs to support learning.

Remote teaching may include both recorded or live direct teaching time, and time for pupils and students to complete tasks and assignments independently. Microsoft Teams is the learning platform used by the Kew College Prep community for remote learning. It is centrally secured, and safe for children and staff to use.

To safeguard children and staff, live lessons adhere to the following rules which are communicated to staff, parents and pupils:

- use neutral or plain backgrounds
- ensure appropriate privacy settings are in place
- ensure staff understand and know how to set up and apply controls relating to pupil and student interactions, including microphones and cameras
- set up lessons with password protection and ensure passwords are kept securely and not shared
- ensure all staff, pupils, students, parents and carers have a clear understanding of expectations around behaviour and participation.

7.2 Use of Pupil Images for Remote Learning

- ***Pre-recorded videos/PowerPoint presentations and photographs of pupils to support remote learning*** - pre-recorded videos/PowerPoint presentations and photographs of pupils will be kept for the academic year and then securely deleted.
- ***Recording of Remote Lessons to allow pupils to re-work through the lessons in their own time*** – if the lesson is recorded, it will only contain pupil's voices but not images of pupils. Lessons that are recorded are kept for the academic year and then securely deleted.
- ***Livestreaming of PSHEE lessons from the classroom to allow a pupil to join the lesson from home*** - the lesson will contain pupil's voices and images. These lessons are not recorded.

8. On-line communication with parents, carers, and pupils

When communicating online with parents, carers, pupils and students, the following should be adhered to at all times:

- communicate through the school channels approved by the senior leadership team
- use school email accounts (not personal ones)
- use school devices over personal devices wherever possible
- not to share personal information
- ensure parents and carers are clear when and how they can communicate with teachers (resources to support communications are available)
- ensure logins and passwords are secure and pupils and students understand that they should not share this information with others.

8.1 Remote meetings with parents

- ***Remote meetings with parent groups***: if meetings are to be recorded for dissemination to other parents, this will be advised to all parents when the meeting is set up.
- ***Remote online one-on-one parent meetings:*** unless for a specific purpose and agreed by both parties or for safeguarding reasons, parent one -on-one meetings, including Parent's Evenings meetings are not recorded. Parents will be told in advance that the school will not be recording the meeting and that parents do not have the school's permission to record the meeting.

Reviewed by:	Reviewed and Approved by:	Updated by:
The Education and Welfare Committee	Title: Head	Title: Designated Safeguarding Lead / IT Manager
	Date: 3 Sep 2025	Date: 3 Sep 2025
Date: 30 Jan 2024		

KEW COLLEGE PREP

Internet use – Rules for Pupils

These rules will help us to be fair to others and keep everyone safe.

The following rules apply to all children in Reception – Year 6:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use the school computer network and Internet for learning
- I know that the school may check my computer files and the Internet sites that I visit
- I will only use the internet when an adult is with me, and I have permission
- I will always ask if I get lost on the Internet
- I will tell an adult if I see anything I am uncomfortable with or that breaks these rules

The following additional rules apply to children in Years 3 - 6:

- When online, I will act as I expect others to act toward me
- I will not take or share images of anyone without their permission
- I will only use apps that are authorised by a member of staff
- I will immediately close any webpage I am not sure about
- I will not try to alter the settings on any devices or try to install any software or programmes
- I will not bring disks or Memory Sticks into school except with prior permission
- I will not use any personal device to connect to the school internet or network unless it is approved
- I will not use any social media sites
- I will never share personal information or passwords with other people
- I will never arrange to meet anyone I don't know
- I will not look at, or change other people's files without their permission
- I understand that I should hand in to the school Office any personal mobile device which has the capacity to access the internet or take photographs, and that I must not use any such device at school, on school trips or at games, etc
- I understand that if I break these rules, I could expect to be disciplined according to the school's current policies and that my parents will be informed

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of E-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text or imagery.

KEW COLLEGE PREP

Responsible Internet Use Agreement

Dear Parent,

As part of your child's curriculum and the development of ICT skills, the school provides supervised access to the Internet.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to deal with this risk at school. Our filtering system restricts access to inappropriate materials, and we have dedicated monitoring software, that automatically blocks and flags up potential unsuitable content. This may not be the case at home, and we can provide references to information on Safe Internet Access if you wish. We do also send out a monthly Online Safety Newsletter which provides valuable information and guidance into how to protect your children at home.

At school, Net Support DNA safeguarding system is live and monitored daily. Net Support DNA monitors keywords and phrases to alert schools of any online activity, either by staff or pupils that may have online safety or safeguarding issues. The Designated Safeguarding Lead reviews the findings on a regular basis and report to the Head.

Pupils in Years 1-Year 6 have been given a presentation to help them understand the Kew College Prep Online Safety Rules and Agreement at age-appropriate levels.

Both pupils and their parents/carers are asked to read the enclosed Rules for pupils for Responsible Internet Use, and sign to show that the Online-Safety Rules have been understood and agreed. These documents are in each Pupils diary.

Yours sincerely,

Mr Thornton
ICT Teacher

Pupil's Responsible Internet Use Agreement	
Pupil:	Class:
· I have read and I understand the School Rules for Responsible Internet Use · I will use the computer, network, iPads, Internet in a responsible way and obey these rules at all times • I know that the school may check my computer files and the Internet sites that I visit	
Signed	Date: