



FELIXSTOWE
INTERNATIONAL COLLEGE

FRIENDSHIP THROUGH EDUCATION

Online Safety Policy

Version Date:	July 2026
Signed:	Principal
Signed:	
Review cycle:	1 year (usually)
Date of next review:	September 2026 (due to filtering and monitoring changes)

This policy is a working document. It should be read alongside the Safeguarding and Child Protection Policy, which takes precedence in the event of any conflict.

Contents

1. Purpose and scope
 2. Legislation and statutory guidance
 3. Understanding the risks
 4. Roles and responsibilities
 5. Filtering and monitoring
 6. Devices
 7. Online safety in boarding
 8. Generative artificial intelligence
 9. Educating pupils
 10. Responding to incidents
 11. Cyber security
 12. Staff conduct online
 13. Training
 14. Equality
 15. Monitoring and review of this policy
 16. Linked policies and documents
- Appendix A: Named roles
- Appendix B: Annual filtering and monitoring review record
- Appendix C: Matters for the Governing Board to resolve

1. Purpose and scope

Felixstowe International College is committed to safeguarding and promoting the welfare of every pupil in its care. Online safety is not a separate activity: it is part of safeguarding, and it is treated as such throughout this policy.

As a boarding college, our pupils live as well as learn here. For many, particularly those whose families are overseas, a personal device is their main means of staying in touch with home, of accessing pastoral support, and of relaxing. Our approach to online safety therefore has to do two things at once: protect pupils from harm, and protect the things that keep boarders well. This policy sets out how we balance the two.

1.1 Who this policy applies to

This policy applies to:

- all pupils, boarding and day
- all staff, including teaching staff, boarding and pastoral staff, support staff, agency and supply staff
- governors, volunteers, contractors and visitors
- educational guardians and host families acting on behalf of a pupil
- the school's external IT service provider and any other third party processing pupil data or providing filtering or monitoring services

1.2 What this policy covers

This policy covers:

- the school network, wi-fi and internet connection, including in boarding accommodation
- personal devices used for school purposes under our Bring Your Own Device arrangements — every pupil, day and boarding, provides their own device and the school supplies none
- school platforms and accounts, including Google Workspace for Education (Google Classroom, school email and cloud storage), Zoom for live lessons and online meetings, and any generative AI tools approved for school use
- online conduct outside school hours or off site, where it affects the safety or wellbeing of a member of the school community, or the reputation of the school

1.3 Aims

- To safeguard and promote the welfare of all pupils by creating a safe online environment.
- To meet in full the requirements of Keeping Children Safe in Education 2026 and the DfE filtering and monitoring standards.
- To ensure filtering and monitoring are effective, proportionate, regularly reviewed and properly recorded.
- To ensure that measures taken to keep pupils safe online do not unnecessarily restrict education, access to support, or boarders' contact with their families.
- To equip pupils with the knowledge, resilience and confidence to keep themselves safe online, now and after they leave.
- To ensure every adult in the school knows what to do when something goes wrong.

2. Legislation and statutory guidance

2.1 Statutory guidance

- Keeping Children Safe in Education 2026 (DfE), in force from 1 September 2026
- Working Together to Safeguard Children 2023 (HM Government)
- National Minimum Standards for boarding schools (DfE)
- The Education (Independent School Standards) Regulations 2014
- Revised Prevent duty guidance for England and Wales (Home Office, 2023)
- Relationships and Sex Education (RSE) and Health Education statutory guidance (DfE)

2.2 Departmental standards and non-statutory guidance

- Filtering and monitoring standards for schools and colleges (DfE, updated October 2024)
- Cyber security standards for schools and colleges (DfE)
- Meeting digital and technology standards in schools and colleges (DfE)
- Teaching online safety in schools (DfE)
- Generative artificial intelligence in education (DfE)
- Mobile phones in schools (DfE)
- Searching, screening and confiscation: advice for schools (DfE)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
- Appropriate filtering and monitoring definitions (UK Safer Internet Centre)

2.3 Primary legislation

- Education Act 2002, section 157 and the Independent School Standards
- Children Act 1989 and Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Data Protection Act 2018 and UK GDPR, as amended by the Data (Use and Access) Act 2025
- Human Rights Act 1998, in particular Article 8 (right to respect for private and family life)
- Equality Act 2010
- Online Safety Act 2023
- Protection of Children Act 1978 and Criminal Justice Act 1988
- Sexual Offences Act 2003 and Voyeurism (Offences) Act 2019
- Computer Misuse Act 1990
- Malicious Communications Act 1988 and Communications Act 2003
- Obscene Publications Act 1959
- Counter-Terrorism and Security Act 2015
- Protection of Freedoms Act 2012 (biometric data)
- Investigatory Powers Act 2016 and the Telecommunications (Lawful Business Practice) Regulations 2000, so far as they apply to the monitoring of communications

3. Understanding the risks

Keeping Children Safe in Education groups online safeguarding risks into four areas. We use these categories to structure our risk assessment, our curriculum and our monitoring.

Area of risk	What this includes
Content	Exposure to illegal, inappropriate or harmful material: pornography; violent or graphic material; content promoting self-harm, suicide or eating disorders; racism, misogyny, antisemitism and other hate material; terrorist and extremist content; misinformation and disinformation, including AI-generated fakes; content encouraging dangerous challenges.
Contact	Harmful interaction with others: adults seeking to groom or exploit children for sexual, criminal or financial purposes; peer pressure and coercion; contact through gaming, live streaming and messaging platforms; harmful interactions with AI chatbots and companion apps, including simulated relationships and manipulation.
Conduct	A pupil's own behaviour causing or increasing the risk of harm: making, sending or requesting nudes or semi-nudes; creating or sharing AI-generated or digitally manipulated intimate images of another person; online bullying and harassment; misogynistic or discriminatory behaviour online; sharing others' personal information; unauthorised access to systems.
Commerce	Online gambling and gambling-style mechanics in games; in-game purchasing; inappropriate advertising; phishing; financial scams and fraud, including scams targeting international pupils and their families; financially motivated sextortion.

Some pupils are more vulnerable online than others. When assessing risk we give particular thought to pupils with special educational needs or disabilities, pupils with mental health needs, pupils who are looked after or previously looked after, and boarders who are far from home, new to the UK, or experiencing homesickness or isolation.

3.1 Artificial intelligence

Generative AI is now a routine part of pupils' online lives and creates risks across all four areas above. We recognise in particular:

- AI-generated intimate imagery, including “deepfakes” and “nudification” apps used against peers or staff. Creating or sharing such an image of a child is a child protection matter and may be a criminal offence, and is handled under our child protection procedures in the same way as any other nude or semi-nude image.
- AI chatbots and companion apps, which can give harmful advice, simulate intimate relationships, and be used to groom or manipulate.
- AI-generated misinformation, including material designed to radicalise or to defraud.
- The use of AI to produce convincing scam and phishing messages, including messages appearing to come from a pupil's family.

4. Roles and responsibilities

The DfE filtering and monitoring standards require the school to identify and assign clear roles. Named postholders are listed at Appendix A.

4.1 The Governing Board

The Governing Board holds overall strategic responsibility for online safety, including for filtering and monitoring. It will:

- approve this policy and review it annually
- appoint a named governor with responsibility for online safety, filtering and monitoring
- ensure a named member of the senior leadership team is responsible for filtering and monitoring, working with the DSL and the IT Manager
- receive assurance, at least annually and in writing, that filtering and monitoring systems are effective and that the DfE standards are met
- review the record of the annual filtering and monitoring check, including what was tested, what was found and what action was taken
- ensure funding is in place to meet the standards, including the cost of any devices the school provides to pupils who need them
- ensure all governors receive online safeguarding training on induction and refresher training thereafter
- satisfy itself that decisions affecting pupils' personal devices and personal data are lawful, proportionate and properly assessed before they are implemented
- ensure this policy does not disadvantage any pupil or family, in line with the Equality Act 2010

Where practicable, the online safety governor role should be held by a governor other than the Chair, so that the Board retains independent challenge on this area. Where the same governor holds both roles, the Board should record how independent scrutiny is maintained.

4.2 The Head of School

The Head of School will:

- establish a culture in which online safety is fully integrated into safeguarding, and in which pupils and staff feel able to report concerns
- ensure this policy is implemented, understood and applied consistently
- ensure the DSL has the time, training, authority and technical support to carry out the online safety role
- ensure that risk assessments covering online safety, including boarding-specific risks, are in place, suitable and reviewed at least annually
- ensure staff, pupils, parents, carers and educational guardians know what to do if an online safeguarding incident occurs
- ensure the Governing Board is informed promptly of any significant online safety incident
- report annually to the Governing Board on the effectiveness of this policy

4.3 Senior leader responsible for filtering and monitoring

This is a role required by the DfE standards. The named senior leader will:

- own the operational delivery of filtering and monitoring, working with the DSL, the IT Manager and the external provider
- procure, or advise on the procurement of, filtering and monitoring systems and document the reasons for the choice made

- document decisions about what is blocked and what is monitored, and why
- ensure the annual review takes place, is recorded, and is reported to the Governing Board
- ensure that any change to devices, network configuration, providers or major software triggers a fresh check
- ensure staff receive training on their filtering and monitoring responsibilities

4.4 Designated Safeguarding Lead / Designated Online Safeguarding Lead

The DSL holds lead responsibility for online safety as part of the wider safeguarding role. The DSL will:

- take day-to-day responsibility for online safeguarding, including the response to filtering and monitoring alerts
- maintain the online safety incident log and ensure incidents are recorded, classified and tracked
- ensure there is a clear, documented route from alert to action, understood by SLT and by boarding staff, including out of hours
- liaise with children's social care, the police, the local authority designated officer and the Prevent team as appropriate
- meet at least termly with the online safety governor and the IT Manager to review incidents, alerts, filtering change logs and blocked-site requests
- ensure online safety education is embedded across the curriculum and the boarding programme
- provide guidance, support and training to staff, and ensure staff know how to recognise and report online concerns
- keep up to date with developments in online harms, including AI-enabled harms
- report annually to the Governing Board

4.5 Deputy DSL

The Deputy DSL is trained to the same standard as the DSL and will deputise in full, including for out-of-hours boarding incidents. The school will ensure a trained safeguarding lead is contactable at all times that boarders are on site.

4.6 Head of Boarding

The Head of Boarding will:

- ensure boarding staff understand their online safety responsibilities, including overnight and at weekends
- ensure boarders can contact their parents, carers and educational guardians in private, at times that work across time zones
- ensure boarders can access confidential helplines and advocacy services in private, and that these are never blocked by filtering
- ensure the boarding routine sets reasonable expectations about device use, including at night, and that these are applied consistently and kindly
- bring any pattern of concern arising in boarding time to the DSL

Where the Head of Boarding and the DSL are the same person, the Governing Board will ensure workload is realistic and that a trained deputy provides genuine cover.

4.7 IT Manager and external IT service provider

The school employs an external IT service provider to deliver technical online safety measures. Using a provider does not transfer accountability: responsibility for meeting the standards remains with the school. The IT Manager will:

- ensure filtering and monitoring systems are correctly configured, active on all relevant devices and connections, and cannot be circumvented, including by VPN, proxy or DNS change
- ensure filtering blocks illegal content, including by subscribing to the Internet Watch Foundation child abuse image list and the police-assessed list of unlawful terrorist content
- maintain a change log recording every change to filtering, who requested it, who approved it and when
- test the systems as part of the annual review and after any significant change, and record the results
- ensure monitoring alerts reach the DSL promptly, including out of hours
- maintain an accurate inventory of devices in use, including personal devices enrolled under the BYOD arrangements
- ensure the school's written agreement with the provider sets out clearly what the provider does, what the school does, response times, and data protection responsibilities
- report technical limitations honestly and promptly to the senior leader responsible for filtering and monitoring

4.8 Data Protection Officer

The Data Protection Officer will:

- advise the school on its obligations under the Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025
- ensure a Data Protection Impact Assessment is completed and signed off before any new monitoring system, or any material change to monitoring, is introduced, and before any software is installed on pupils' personal devices
- advise on the lawful basis for monitoring, on transparency, and on retention of monitoring records
- ensure privacy information is provided in a form children and families can understand, including for families whose first language is not English
- respond to subject access requests within one month, as required by UK GDPR, extendable by up to two further months for complex requests
- report personal data breaches to the Information Commissioner's Office within 72 hours where the breach meets the reporting threshold, and advise on notification to those affected
- ensure contracts with processors, including the IT service provider and any filtering or monitoring vendor, are compliant
- advise on international transfers of personal data, which is particularly relevant given our pupil population
- report periodically to the Head of School and the Governing Board

Child protection always comes first. Data protection law does not prevent the sharing of information for the purposes of keeping children safe.

4.9 Curriculum leadership

The curriculum leader will ensure that online safety is taught explicitly and revisited across subjects, that it is age-appropriate and relevant to pupils' actual online lives, and that it is planned rather than incidental. Online safety education will be reviewed annually against the risks identified in our incident log and monitoring reports.

4.10 All staff

All staff will:

- read and follow this policy, the Safeguarding and Child Protection Policy and the Staff Acceptable Use Agreement
- read Part One of Keeping Children Safe in Education in full and confirm they have done so
- report any online safeguarding concern to the DSL immediately, and never assume someone else will
- supervise pupils appropriately during online activity and be alert to what pupils are actually doing
- report any filtering failure, over-blocking, or monitoring system fault to the IT Manager and the DSL
- model safe and respectful online behaviour, and maintain professional boundaries in all communication with pupils
- never attempt to investigate a device or an image themselves where a child protection concern arises — this is for the DSL

4.11 Pupils

Pupils are expected to:

- follow the Pupil Acceptable Use Agreement, which is explained and signed on entry and revisited each year
- treat others online with the same respect they would show in person
- tell a trusted adult if they see or receive something that worries them, or if a friend is at risk
- not attempt to bypass filtering or monitoring, or share login details
- not photograph, film or record staff or other pupils without permission

Pupils will never be punished for reporting a concern in good faith, including where they have broken a rule themselves. We would far rather know.

4.12 Parents, carers and educational guardians

We ask parents, carers and educational guardians to:

- read this policy and sign the relevant acceptable use agreements
- talk to their child about online safety and keep the conversation going
- contact the DSL promptly with any concern about a pupil's online life, whether it arises at school or at home
- follow school guidance on device use during exeats and holidays
- model safe and respectful behaviour online, including in parent group chats and on social media

We will provide information and, where there is demand, sessions for parents and guardians, and will make key information available in translation where needed.

5. Filtering and monitoring

This section sets out how the school meets the four DfE filtering and monitoring standards. Filtering is preventative: it blocks access to harmful material. Monitoring is reactive: it identifies concerning activity so that the school can respond. Neither replaces good teaching, good supervision or good pastoral care.

5.1 Standard 1: roles and responsibilities

The named postholders required by the standards are recorded at Appendix A and their duties are set out in section 4. Responsibilities are reviewed whenever a postholder changes, and at least annually.

5.2 Standard 2: review at least annually

The school reviews its filtering and monitoring provision at least once every academic year. The review is led by the senior leader responsible for filtering and monitoring, with the DSL, the IT Manager and the online safety governor, and is recorded using the template at Appendix B.

The review considers:

- the risk profile of our pupils, including boarders, international pupils and pupils with additional vulnerabilities
- what is blocked and whether it is still the right list — both under-blocking and over-blocking
- how effective monitoring has been in practice, judged against the incidents we actually had
- the volume, type and outcome of alerts, and whether the response was timely
- coverage: whether every device and connection in use is actually covered, including personal devices and boarding wi-fi
- any technical limitations reported by the IT Manager or provider
- whether staff know how to report a problem, and whether they have

An additional check is carried out, outside the annual cycle, whenever:

- new devices or device types are introduced, including any new class of personal device
- the filtering or monitoring provider changes, or a system is reconfigured
- the technical configuration of the network or of devices changes
- a major software or operating system update occurs
- a safeguarding incident suggests the systems did not work as intended
- the school introduces a new platform or generative AI tool

5.3 Standard 3: blocking harmful and inappropriate content

Our filtering system blocks, as a minimum:

- child sexual abuse material, using the Internet Watch Foundation URL list
- unlawful terrorist content, using the list assessed by the police
- adult and pornographic content, including nudification and “undress” tools
- content promoting self-harm, suicide or eating disorders
- extremist and radicalising content, and hate material targeting people on the basis of any protected characteristic
- graphic violence and gore

- content relating to illegal drugs or the misuse of prescription drugs
- gambling and gambling-style sites
- sites facilitating the circumvention of filtering, including anonymising proxies and unapproved VPNs
- malware, phishing and known fraudulent sites

Filtering must not be so blunt that it damages education or cuts pupils off from help. In particular, filtering will not block:

- helplines and support services, including Childline, Samaritans, Papyrus, Shout, the NSPCC and the IWF Report Remove service
- reputable health information, including sexual health, mental health and substance misuse support
- support and information resources for LGBT+ young people
- legitimate news, and material needed for the study of difficult topics such as extremism, genocide or war, where access is supervised and educationally justified

Over-blocking is a safeguarding risk in its own right and is treated as a fault to be reported and fixed, not an inconvenience to be tolerated. Any member of staff or pupil may request a review of a blocked site. Requests are logged, decided by the senior leader responsible for filtering and monitoring in consultation with the DSL, and the decision recorded.

Filtering is applied to all school devices and to all traffic on the school network, including in boarding accommodation. Where a filtering category is relaxed for an individual or group, for example for a member of staff undertaking Prevent-related research, the decision, its scope and its duration are recorded and reviewed.

5.4 Standard 4: effective monitoring

Monitoring is targeted at safeguarding. Its purpose is to identify pupils who may be at risk, not to police pupils generally, and not to gather information about pupils' private lives for any other purpose.

Our monitoring strategy records, in a separate operational document reviewed annually:

- which devices and accounts are monitored, and which are not
- when monitoring is active, including whether it operates outside teaching hours
- what triggers an alert, and how alerts are prioritised
- who receives alerts, within what timescale, and who covers evenings, weekends and holidays while boarders are on site
- how alerts are triaged, escalated, recorded and closed
- how long monitoring records are kept, and who can access them

Every alert is reviewed by a person. Automated systems flag; they do not decide. The DSL determines the safeguarding response, which may include no action beyond recording the alert.

Because every pupil uses their own device, and because that device goes home with a day pupil and into a boarding house with a boarder, the scope of monitoring is not the same for both groups. This is set out at 6.5. Any monitoring that extends into pupils' personal time will be justified in the Data Protection Impact Assessment, limited to what is necessary for safeguarding, and clearly explained in advance.

5.5 Privacy, proportionality and data protection

Filtering and monitoring involve processing children's personal data, some of it sensitive. The school will:

- complete a Data Protection Impact Assessment before introducing or materially changing any monitoring system, and keep it under review
- identify and record the lawful basis for the processing, and not rely on consent where consent could not be freely given
- tell pupils and families clearly, in advance and in plain language, what is monitored, when, by whom, and what happens to the information
- collect no more than is necessary, and retain monitoring records no longer than necessary
- restrict access to monitoring data to named individuals with a safeguarding reason to see it
- not use monitoring data for performance management, behaviour policing unrelated to safeguarding, or any purpose not set out here
- respect boarders' right to private contact with their families and with confidential support services

Pupils have rights under Article 8 of the Human Rights Act 1998. Interference with those rights must be lawful, necessary and proportionate to the safeguarding aim. Where a less intrusive measure would achieve the same protection, we will use it.

6. Devices

6.1 Our device model

As an independent school, we require every pupil to arrive with a device for school work. The school does not supply devices. This requirement is a condition of enrolment, set out in the parent contract and the Bring Your Own Device Policy, and the specification is given to families before they accept a place.

Three consequences follow, and this policy addresses each of them:

- the school's filtering and monitoring duties apply in full to any device used for school work, regardless of who owns it
- the device remains the property of the family, so the school's reach over it is defined by what the school has required, published and agreed — not by ownership
- the device goes home with a day pupil and into a boarding house with a boarder, so anything installed on it operates in pupils' and families' own time unless it is configured not to

The school will publish device requirements clearly and in advance, assess any change to those requirements for proportionality and cost before announcing it, and configure filtering and monitoring so that they apply to school use rather than to a pupil's whole life.

6.2 What is required of a personal device used for school work

Where a personal device is used for school work, the school requires that it can be filtered and monitored to the standard set out in section 5 while it is being used for school purposes. Where that is not technically possible on a particular device, the device may not be used for school work.

Device requirements, including minimum specification and compatibility with the school's filtering and monitoring software, are set out in the parent contract and the Bring Your Own Device Policy

and given to families before they commit to a purchase. Where the requirement changes, families are given notice in line with 6.6.

6.3 Conditions before any software is installed on a personal device

No filtering or monitoring software will be installed on a pupil's personal device unless all of the following are in place:

1. A Data Protection Impact Assessment covering the installation and the resulting monitoring has been completed by the DPO and approved by the Governing Board.
2. Written information has been given to parents, carers and pupils setting out, specifically: what the software does; what data it collects; who can see it; when it is active; what will be removed from the device; and what will happen to the software when the pupil leaves.
3. Where installation will remove personal data, apps or settings, this has been stated explicitly and in advance, and families have been given a reasonable period, and practical guidance, to back up data first.
4. A parent or carer, and the pupil, have signed an agreement acknowledging the change to the device. For pupils under 18 whose families are overseas, the school will satisfy itself that the family, not only the educational guardian, has understood and agreed.
5. A route has been identified for any pupil whose family cannot meet the cost, or does not wish to alter a device they own — see 6.6.
6. The IT Manager has verified, and recorded, that the software works as intended on that device type.

6.4 What the school will not do

The school will not:

- install software that resets or wipes a pupil's personal device without prior written agreement from the family and a documented opportunity to back up data
- monitor a pupil's private communications with their family, or with a confidential helpline or advocacy service
- impose a device requirement that leaves a family with no realistic option other than buying a second device, without first considering the alternatives at 6.6 and recording why they were rejected
- apply a requirement retrospectively to a family who has already purchased a device to the school's published specification, without notice and without considering the cost to them
- retain access to a personal device, or to data from it, after a pupil leaves; software will be removed and access revoked as part of the leaving process

6.5 Scope of monitoring: day pupils and boarders

Devices are personally owned and go home, so the school is explicit about when monitoring is active. Our monitoring software supports scheduling, and we use it. Monitoring is switched on and off by time rather than left running continuously, and the schedule differs for day pupils and boarders because the school's duty of care differs.

The schedule below is published to pupils and families, recorded in the monitoring strategy, and reflected in the Data Protection Impact Assessment. Any change to it is a change requiring review under 5.2.

Day pupils

- Monitoring is active during the school day only, from [insert start time] to [insert end time] on school days.
- Monitoring is switched off outside those hours and on weekends, in the school holidays and on days the school is closed. The school does not monitor a day pupil's use of their own device at home, in the evenings or during holidays.
- Supervision of a child's device outside school hours is a matter for their parents or carers. The school supports families with guidance rather than surveillance, and will provide advice on home filtering on request.
- Where a safeguarding concern arises from a day pupil's activity on a school account outside school hours, the school acts on it in the ordinary way.

Boarders

- Boarders are in the school's care outside teaching hours, so monitoring operates across the school day and boarding time while boarders are on site.
- Monitoring is switched off during exeats, half terms and holidays, when a boarder is at home and in their family's care rather than the school's.
- Monitoring during boarding time is limited to what is necessary for safeguarding. It is not used for general behaviour management, and it does not extend to private contact with family, educational guardians, confidential helplines or advocacy services.
- Boarders are told clearly, in a language they understand and before they arrive where possible, what is monitored and when.

Filtering is a separate matter from monitoring. Filtering applies to all traffic on the school network at all times, including in boarding accommodation overnight, because its purpose is to block harmful content rather than to observe pupils.

The IT Manager verifies the schedule as part of the annual review at 5.2, and after any software update, to confirm that monitoring is genuinely inactive outside the published hours. The result is recorded.

6.6 Fairness and cost

Where a school supplies devices, a family who declines a configuration can be given a school one. We have no such stock, so a device requirement falls directly on families, and unevenly. Before adopting any requirement that removes personal use of a pupil's existing device, the school will consider and record the alternatives, which may include:

- a managed profile, container or supervised school account that applies filtering and monitoring to school use without resetting the device or removing personal apps and data
- network-level filtering combined with a managed browser or a managed set of school applications
- limiting the requirement to the device types where enrolment can be achieved without a reset, and adjusting the published device specification accordingly for future joiners
- phasing the requirement so it applies to new pupils from a stated date, rather than to families who have already bought to the previous specification

If, after that assessment, a second device remains the only workable option for some families, the school will:

- establish a hardship route — a small pool of loan devices, a bursary contribution, or an equivalent — funded by the Governing Board, so that no pupil is disadvantaged by their family's ability to pay

- publicise that route to all families at the same time as the requirement itself, not only to those who ask
- handle requests confidentially, with no disadvantage to the pupil
- complete an equality impact assessment before the requirement takes effect
- give families as much notice as possible, and at least a full term where a purchase is involved

6.7 Boarders' personal devices

For a boarder, a personal device is not only a school tool. It is how they speak to their family, keep up with home, and unwind. This is recognised in the National Minimum Standards for boarding schools, which require that boarders can contact their parents and carers in private and can access confidential help.

Accordingly, where a pupil boards:

- the school will not require that a pupil's only personal device be configured for school use exclusively, unless the school has first provided an alternative means of private personal and family contact
- any restriction on personal use will be limited to what is necessary, and will not extend to contact with family, guardians or helplines
- boarders will be able to make and receive private calls at times that work across time zones, including outside the UK working day
- boarders will be told, clearly and in a language they understand, what is and is not monitored during boarding time

6.8 Devices used for remote lessons

Live lessons are delivered through Zoom, and work through Google Classroom and school email. A pupil learning remotely is off the school network, so filtering on the school connection does not reach them: the protection in those lessons comes from how the sessions are set up and supervised. The platform configuration required for this — unique meeting IDs, passcodes, waiting rooms, host-only screen sharing, and ending sessions for all participants — is set out in the Remote Learning Provision Policy and enforced centrally by the IT Manager.

Staff must not use any platform other than those approved above for teaching or for contact with pupils. Where a new platform is proposed, it goes through SLT approval and a data protection assessment, and its introduction triggers a filtering and monitoring check under 5.2.

6.9 Mobile phones

Keeping Children Safe in Education 2026 expects schools to be mobile phone-free environments during the school day by default, with exceptions made deliberately rather than by drift. The school's arrangements for phones during the teaching day, during boarding time and overnight are set out in the Mobile Phone Safety and Acceptable Use Policy. Those arrangements will:

- be clear, consistently applied and explained to pupils and families
- take account of boarders' need to contact home, and of day pupils' need to contact parents about journeys home
- make reasonable adjustments for pupils who need a phone for medical or accessibility reasons

- be enforced through the behaviour policy and searching guidance, not through informal or ad hoc confiscation

6.10 Circumvention

Attempts to bypass filtering or monitoring — through VPNs, proxies, tethering to mobile data to avoid the school network, altering DNS settings or removing management software — are treated as a safeguarding matter as well as a behaviour matter. The response will consider why the pupil did it: sometimes circumvention is a sign of risk rather than defiance.

7. Online safety in boarding

Boarders are online in their own time, in their own space, often late in the evening, and often talking to people thousands of miles away. Our approach reflects that.

- Boarding staff receive online safety training specific to boarding, including the risks that surface at night and at weekends.
- Boarders can contact parents, carers and educational guardians in private, at reasonable times taking account of time differences.
- Boarders are given, in writing and in a form they understand, the contact details for confidential helplines and for the school's independent listener, and can use them privately.
- Expectations about device use overnight are set out in the boarding handbook, applied consistently, and designed to protect sleep rather than to punish.
- Staff are alert to the online risks that particularly affect international boarders: scams and fraud targeting pupils and families, coercion in relation to money, financially motivated sextortion, gambling, and contact from adults met through gaming or social platforms.
- Homesickness and isolation increase online vulnerability. Pastoral staff treat withdrawal into online life as a wellbeing indicator, not simply a screen-time problem.
- Monitoring alerts arising outside the teaching day reach a trained safeguarding lead the same day, and immediately where a pupil may be at risk of harm.

8. Generative artificial intelligence

The school permits the use of approved generative AI tools where there is a clear educational purpose and appropriate oversight. Before any tool is approved for pupil use, the school will assess its age suitability, its data protection implications and its content safeguards, and will record the decision.

- Pupils are taught how generative AI works, what it gets wrong, and why its output cannot be trusted uncritically.
- Personal data, and in particular safeguarding information, must never be entered into a generative AI tool that has not been approved by the school.
- Staff may use approved AI tools to support their work, but remain professionally responsible for anything produced. AI must not be used to write safeguarding records, child protection referrals or reports about individual pupils.
- Creating or sharing sexual images of a child using AI is a child protection matter and may be a criminal offence. It is handled under the procedure at 10.3, exactly as any other nude or semi-nude image would be.

- Use of AI to bully, harass, impersonate or humiliate a pupil or member of staff, including through manipulated images or voice, is a serious disciplinary and safeguarding matter.
- Pupils are taught about AI companions and chatbots, including that these systems can give harmful advice and can be used by others to manipulate them.

9. Educating pupils

Filtering and monitoring keep pupils safer while they are with us. Education is what keeps them safer afterwards. Online safety is taught through RSHE, computing and citizenship, reinforced across the curriculum, and revisited in the boarding programme.

The programme covers, at an age-appropriate level:

- evaluating information online, including recognising misinformation, disinformation and AI-generated content
- privacy, data and digital footprint
- healthy relationships online, consent, and the law relating to images
- recognising grooming, exploitation and coercion, including financially motivated sextortion
- online bullying, misogyny and harmful sexual behaviour online
- extremism, radicalisation and building resilience to it
- gambling, in-game spending, scams and fraud
- the impact of online life on sleep, mood and mental health
- how and where to get help, in school and independently

We take part in Safer Internet Day each February, but treat it as a punctuation mark rather than the programme itself. The programme is reviewed annually against what our incident log and monitoring reports actually show.

10. Responding to incidents

10.1 Reporting

Any concern about a pupil's safety online is reported to the DSL immediately, using the school's usual safeguarding reporting route. Staff do not need to be certain, and do not need to investigate first. If a child is at immediate risk, staff call 999.

All online safety incidents are recorded, classified and tracked on the safeguarding recording system. The DSL reviews patterns termly and reports to the Governing Board annually.

10.2 Filtering and monitoring alerts

Alerts are triaged by the DSL or a trained deputy. The response is proportionate and, wherever possible, supportive: a pupil searching for information about self-harm needs help, not sanction. Every alert results in a recorded decision, even where the decision is that no further action is needed.

10.3 Nudes, semi-nudes and AI-generated intimate images

The school follows the UKCIS guidance *Sharing nudes and semi-nudes: advice for education settings*. Staff must:

- report to the DSL immediately

- never view, copy, print, share, store or forward the image
- never delete the image or ask the pupil to delete it before the DSL has decided on the response
- never ask the pupil to disclose details of the image, and never share information with other staff or pupils beyond what is necessary
- explain to the pupil that this has to be passed on, and that they are not in trouble for telling

This applies equally to images that have been digitally created or manipulated, including AI-generated images. The DSL will decide, with reference to the guidance, whether a referral to children's social care or the police is required, and will consider support for both the child depicted and the child who shared or created the image. Pupils will be told about the IWF Report Remove service, which can help get images taken down.

10.4 Online child sexual exploitation, criminal exploitation and sextortion

Where a pupil may be being groomed, exploited or blackmailed online, the DSL will follow child protection procedures and refer to children's social care and the police as appropriate. In cases of financially motivated sextortion, pupils are advised not to pay, to keep evidence, to stop contact and to tell an adult immediately. The response focuses on support: pupils in this situation are victims of crime and frequently feel unable to tell anyone.

10.5 Radicalisation and extremism

Concerns that a pupil is being drawn into terrorism are reported to the DSL, who will consider a Prevent referral and liaise with the local authority Prevent lead. Staff should be alert to online radicalisation and to the role of algorithmic content in it.

10.6 Online bullying and harassment

Online bullying, including sexual harassment, misogyny and image-based abuse, is dealt with under the Anti-Bullying Policy and, where relevant, as a child protection matter. It is never dismissed as "banter" or as something that happened outside school.

10.7 Illegal content

Suspected child sexual abuse material is reported to the police and to the Internet Watch Foundation. Staff must not attempt to verify, copy or preserve such material themselves. Suspected terrorist content is reported to the police.

10.8 Concerns about a member of staff

Any concern about the online conduct of a member of staff, governor, volunteer or contractor is reported to the Head of School, or to the Chair of Governors where the concern relates to the Head. The school follows the low-level concerns and allegations procedures in Part Four of Keeping Children Safe in Education and consults the local authority designated officer where the harm threshold may be met.

11. Cyber security

A cyber incident is a safeguarding risk: pupil records, safeguarding files and images are exactly what attackers want. In line with the DfE cyber security standards, the school will:

- require multi-factor authentication on all school accounts, including staff email and administrative systems
- maintain offline, tested backups of critical data
- apply security updates promptly and keep supported software in use
- operate least-privilege access, reviewed when staff change role or leave
- train staff to recognise phishing, including AI-generated phishing
- maintain and test an incident response plan, including who reports a breach and to whom
- assess the security and data protection posture of suppliers before contracting

12. Staff conduct online

- All communication with pupils takes place through school systems and accounts. Staff do not contact pupils through personal accounts, personal phone numbers or personal social media.
- Staff do not accept or initiate social media connections with current pupils.
- Staff manage their own privacy settings and are mindful that material they post publicly may be seen by pupils and families.
- Staff use school devices for school work wherever possible, and never store pupil personal data on unencrypted personal devices or personal cloud accounts.
- Boarding staff take particular care over the boundary between pastoral availability and personal contact, especially in the evenings.
- Breaches of the Staff Acceptable Use Agreement are dealt with under the disciplinary procedure and, where a child may be at risk, under safeguarding procedures.

13. Training

Training is only useful if people remember it and act on it. We therefore check understanding rather than only attendance.

- All staff receive online safeguarding training on induction and as part of regular safeguarding updates, at least annually.
- All staff read Part One of Keeping Children Safe in Education in full, and this is recorded.
- The DSL and deputies receive enhanced training covering online harms, filtering and monitoring, AI-enabled harms and the response to image-based abuse.
- Boarding staff receive training covering out-of-hours online risk.
- The IT Manager and relevant staff are trained on their filtering and monitoring responsibilities, including how to report a fault.
- Governors receive online safeguarding training on induction and refresher training thereafter; the online safety governor receives training specific to the filtering and monitoring standards.
- Understanding is checked through short assessments; gaps identified are recorded and addressed, and the record retained.

14. Equality

This policy has been equality impact assessed under the Equality Act 2010. We have given particular attention to:

- the cost of device requirements and their potential to disadvantage pupils from lower-income families
- pupils with special educational needs or disabilities, who may need assistive technology, adjusted arrangements, or additional teaching about online risk
- pupils for whom English is an additional language, and their families, who must receive information in a form they can understand
- the risk that filtering blocks legitimate support resources for pupils with protected characteristics, including LGBT+ pupils
- the disproportionate impact of online sexual harassment and image-based abuse on girls

Where a potential disadvantage is identified, the school will mitigate it, and record what it has done.

15. Monitoring and review of this policy

This policy is reviewed annually by the DSL, the senior leader responsible for filtering and monitoring, the Head of School and the online safety governor, and approved by the Governing Board. It will also be reviewed:

- after any significant online safety incident
- when statutory guidance changes
- when filtering, monitoring or device arrangements change materially

Effectiveness is judged against: the incident log and what it shows about recurring risks; the outcome of the annual filtering and monitoring check; alert response times; the results of pupil, parent and staff surveys; and training records. A statement of effectiveness, with recommendations, is presented to the Governing Board annually.

16. Linked policies and documents

- Safeguarding and Child Protection Policy
- Pupil Acceptable Use Agreement
- Staff Acceptable Use Agreement
- Bring Your Own Device Policy
- Mobile Phone Safety and Acceptable Use Policy
- Filtering and Monitoring Strategy (operational document)
- Data Protection Policy, Privacy Notices and Data Protection Impact Assessments
- Behaviour and Discipline Policy
- Anti-Bullying Policy
- Prevent Duty Policy
- Policy on Sexual Harassment and Sexual Violence
- Boarding Handbook and boarding policies
- Remote Learning Provision Policy
- Complaints Policy
- Cyber Security and Business Continuity Plan

Appendix A: Named roles

These roles are required or expected by Keeping Children Safe in Education and the DfE filtering and monitoring standards. This table is reviewed whenever a postholder changes.

Role	Name	Notes
Head of School	Rebecca Mainprice	
Chair of Governors	Robert Noakes	
Designated Safeguarding Lead and Designated Online Safeguarding Lead	Chaerin Lee	Also Head of Boarding
Deputy Designated Safeguarding Lead	Joyce Jennings Katherine Murphy	Provides cover including out of hours
Governor responsible for online safety, filtering and monitoring	Robert Noakes	Currently also Chair of Governors — see 4.1
Senior leader responsible for filtering and monitoring	Chaerin Lee	Required by the DfE standards; must be an SLT member
IT Manager	Cerys Parker	
External IT service provider	TBC Sep 26	Contract and responsibilities to be recorded
Data Protection Officer	Andy Crow	
Independent listener for boarders	Andy Byford	Required by the boarding standards

Appendix B: Annual filtering and monitoring review record

Completed at least once each academic year, and after any of the trigger events at 5.2. Retained as evidence for the Governing Board and for inspection.

Item	Record
Date of review	
Present	
Systems in scope (filtering, monitoring, devices, connections)	
Reason for review (annual / trigger event)	
Risk profile considered (including boarders and international pupils)	
Testing carried out and by whom	
Blocked categories reviewed — changes made	
Over-blocking identified and resolved	
Coverage gaps identified (devices or connections not covered)	
Alert volumes, response times and outcomes since last review	
Technical limitations reported by provider	
Staff awareness checked	
Data Protection Impact Assessment reviewed and still valid	
Actions agreed, owner and deadline	
Reported to Governing Board on	