



Online Safety & Mobile Phone Policy

Policy Type	Statutory
Regulation	ISSR: 7
Reviewed by	Deputy Head Pastoral
Last Review	Autumn 2026
Next Review	Autumn 2027

1	Introduction.....	2
2	Related Policies	2
3	Terminology	3
4	Background	3
5	Communicating about Online safety with Staff, Pupils and Parents	4
5.1	Further Information and Support for Parents and Pupils	4
5.2	Identifying and Reporting Incidents.....	5
5.3	Filtering and Monitoring Inappropriate Content	5
6	Roles and Responsibilities	6
7	Staff	7
7.1	Duty to Report Online Safety Breaches and Safeguarding Concerns	7
8	Online Safety in the Curriculum	7
9	Guidance for Parents	8
10	The Management of Personal Data	8
	Appendix 1.....	9
	Mobile Phones, Smartphones and Personal Devices	9
	Students in Reception – Year 2	9
	Years 3-6	9
	Years 8-11.....	10
	Sixth Form	11
6.	Sanctions	12
	Viewing Youth Produced Sexual Imagery (Nudes and Semi-Nudes)	13
	Deletion of images	14

1 Introduction

This policy has been reviewed in accordance with the statutory guidance set out in Part 3 – Paragraph 7, Safeguarding: Standards and Regulations, Handbook for the Inspection of Association Independent Schools, Including Residential (Boarding) Schools and Registered Early Years Setting Documents, effective September 2023. In particular, the requirements set out from page 46, Evaluating Safeguarding.

2 Related Policies

This policy should be read in conjunction with the following other policies:

Acceptable Use Policy – Students
AI Policy

Anti-bullying Policy
Behaviour Rewards and Sanctions Policy
Data Protection Policy
Equality Act 2010
Preventing and tackling bullying (July 2017)
PSHE Policy
Safeguarding Policy
School's code of conduct for using IT

3 Terminology

Head where not explicitly defined, means either the Headmaster of the Boys' School or/and the Headmistress of the Girls' School.

Parents includes one or both parents, a legal guardian, or education guardian.

School means Haberdashers' Boys' School and/or Haberdashers' Girls' School which are operated by the Haberdashers' Aske's Elstree Schools Limited, the Schools Trustee of Haberdashers' Aske's Charity.

Student or **Students** means any student or students in the School at any age.

4 Background

The Schools embrace the advantages of modern technology, including the substantial educational benefits. However, the Schools also recognise that technology is a significant component in many safeguarding, wellbeing and behavioural issues affecting children and young people, presenting risks, such as cyberbullying, online abuse, child-on-child abuse or exposure to harmful content, misinformation, disinformation, the sharing of inappropriate imagery, online exploitation, deepfakes, AI generated or enabled imagery or bullying, harmful online influences, extreme content, misogynistic content, and excessive or problematic device use. The School is therefore committed to helping students develop healthy, balanced and age-appropriate relationships with technology. It is the duty of everyone; staff, parents and students to work together to ensure that every child in our care is safe. The purpose of this online safety policy is to outline what measures the Schools take to ensure that students work in a safe environment, develop healthy technology habits, balance online and offline activity and that issues arising from device use are detected and dealt with appropriately. This policy applies to matters arising at School and/or using School systems.

The policy pays regard to:

- KCSIE September 2026
- UKCIS Guidance on Nudes and Semi-Nudes
- Department for Education document on Sharing Nudes and Semi-Nudes December 2020
- Teaching Online Safety in Schools June 2019

- Education for a Connected World 2020 edition
- Online Safety Act October 2023
- Generative AI in Education 2025

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning, there are still dangers related to their use, especially in relation to young pupils and their personal safety. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material, including misinformation, disinformation and conspiracy theories
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
- Commerce: including online gambling and financial scams

This policy acknowledges that the use of technology must be in line with fundamental British values.

5 Communicating about Online safety with Staff, Pupils and Parents

We recognise that the active management of hardware, software and connectivity is vitally important, and that teachers and parents have a part to play in the safeguarding and protection of pupils. Staff undergo regular safeguarding training which is integrated, aligned and considered as part of the overarching safeguarding approach. This training may be through the School Staff Development Programme, INSET programme or safeguarding bulletins.

We hold at least one annual event for parents on online safety. We also post, via our parent portal and letters home, up-to-date advice on current trends and tips for parents.

We have AUPs for Staff, Pupils and Parents. These give clear guidance on the use of technology in the classroom and beyond for all users. They also make clear reference to permissions/restrictions and agreed sanctions. Staff, pupils and parents and visitors have to agree to the relevant AUP as part of their access process.

Pupils are taught, via the assembly programme, Form Times, ICT or Computing lessons and PSHE lessons about internet safety and digital wellbeing. The aim is to build resilience in the pupils to protect themselves and their peers through education and information. For example, they are made aware of the dangers of using certain forms of social media and how to protect themselves online. The Schools work with a number of agencies to develop the best programme of study including Tooled Up, Alan McKenzie, the Think U Know programme developed by the Child Exploitation and Online Protection (CEOP) and the Parent Zone.

5.1 Further Information and Support for Parents and Pupils

The following is not exhaustive but should provide a useful starting point:

- Tooled Up
- www.thinkuknow.co.uk

- www.disrespectnobody.co.uk
- www.saferinternet.org.uk
- www.internetmatters.org
- www.childnet.com/cyberbullying-guidance
- www.pshe-association.org.uk
- www.gov.uk/government/publications/the-use-of-social-media-for-online
<http://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation> [Report Remove | Childline](#) (report a nude image shared online)

NCMECs take it down tool – anonymously take down nudes that are yet to be shared online but you think might be shared at some point in the future.

5.2 Identifying and Reporting Incidents

Reporting of incidents is actively encouraged and support is provided through the pastoral system. Incidents are dealt with immediately and parents are usually informed. The AntiBullying Policy, Behaviour Policy and AUPs are very clear about what is not acceptable. Trends in incidents are also discussed and recorded at Pastoral meetings.

5.3 Filtering and Monitoring Inappropriate Content

The School uses 'Lightspeed' as part of its filtering and monitoring strategy. These systems assist the School in identifying and responding to potential safeguarding concerns, including searches, content, communications or behaviours that may indicate a risk of harm. This includes concerns relating to bullying, cyberbullying, self-harm, suicide, exploitation, violence, extremism, inappropriate sexual behaviour, child-on-child abuse and other safeguarding risks. Monitoring also assists the School in identifying attempts to access inappropriate or harmful online content.

~~Senso software can give teachers access to students' screens during lessons as a classroom management and active monitoring tool. We also keep a log of incidents which are regularly checked, and issues reported to Pastoral Leaders.~~

Filtering and monitoring arrangements apply to School-managed devices and networks and are designed to balance safeguarding requirements with the educational needs of students. The School recognises that filtering and monitoring are important safeguarding tools but form only one part of a wider safeguarding approach that includes staff vigilance, education, pastoral support and effective reporting procedures.

The School maintains records of significant alerts and incidents and ensures that concerns are reviewed by appropriate staff, including safeguarding and pastoral leaders where necessary. Designated Safeguarding Leads, pastoral leaders and IT staff meet regularly to review the effectiveness of filtering and monitoring arrangements, identify emerging risks and ensure continued compliance with statutory guidance. This review includes consideration of developments in technology, online trends, social media platforms, artificial intelligence and other digital tools used by children and young people.

The School also recognises the increasing use of generative artificial intelligence and reviews its filtering and monitoring arrangements regularly to ensure that AI-enabled

technologies are used safely, responsibly and in accordance with School expectations. The DfE has published Generative AI: product safety expectations to support schools to use generative artificial intelligence safely, and explains how filtering and monitoring requirements apply to the use of generative AI in education

6 Roles and Responsibilities

In line with *Keeping Children Safe in Education (2026)*, Annex C, the Designated Safeguarding Lead (DSL) has overall responsibility for online safety, including filtering and monitoring.

The DSL will ensure that this policy is understood and upheld by all members of the School and to help the Schools keep up-to-date with current online safety issues and guidance issued by relevant organisations such as the Independent Schools Inspectorate, the DfE and CEOP (Child Exploitation and Online Protection). All safeguarding issues must be raised with the DSL.

The DSLs' responsibilities are as follows:

- To monitor trends relating to mobile phone misuse, online harms and technology-related safeguarding concerns
- To oversee implementation of the School's smartphone-free strategy and ensure that mobile device procedures continue to support safeguarding, wellbeing and educational outcomes
- To manage any disciplinary procedures for pupils which arise as a result of them not following the Online safety Policy or AUP
- To work with the Heads of ICT/Computing/PSHE to ensure that the Online Safety Policy is kept up to date and that it is implemented
- To understand and hold responsibility for the Filtering and Monitoring systems put in place

The responsibility of the Head of PSHE is:

- To provide an education programme about online safety to pupils to ensure they know how to stay safe online as outlined in the PSHE policy

The IT Department has a key role in maintaining a safe technical infrastructure at the Foundation and in keeping abreast with technical developments. They are responsible for the security of the Foundation's hardware system. The responsibilities of the IT department are as follows:

- Director of IT, in conjunction with IT Infrastructure and Operations Manager:
 - Ensures that the best technological solutions are in place to ensure online safety whilst still enabling pupils to use the system effectively in their learning, particularly in relation to filtering and monitoring
 - Ensures that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition, securing and preserving evidence of any online safety breach
 - Reports any online safety related issues that arise to the DSL and Head of ICT
- IT Support Team:
 - Assists in the resolution of online safety issues with the DH Pastoral, Head of ICT and other members of staff.

All staff working with students are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's online safety procedures and Staff Code of Conduct. Staff must communicate on a professional level and only through School based systems, never through personal mechanisms such as email, text, mobile phones. Any suspected misuse or problems are to be monitored and reported immediately.

7 Staff

As part of the induction process, all staff are required to have read and accepted the Acceptable Use Policy.

All staff receive regular information and training on online safety issues in the form of INSET training or bulletins and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All staff are required to read and acknowledge that they have read the Acceptable Use Policy every year.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise.

Staff are to implement mobile phone expectations consistently and fairly, and to challenge inappropriate device use and report concerns in accordance with this policy. Staff should actively monitor students' online activity in school.

7.1 Duty to Report Online Safety Breaches and Safeguarding Concerns

Staff should promptly inform the Director of IT, Compliance Manager and IT Infrastructure and Operations Manager if they suspect or become aware of an online safety breach, except where the case involves safeguarding concerns, in which case the matter should be reported as set out below:

Staff must promptly inform the Designated Safeguarding Lead if they have any safeguarding concerns about a student related to online activity (including making, possessing or sharing nudes and semi nudes, including where self-generated or generated by AI, deepfakes, or those digitally altered, cyberbullying and inappropriate or illegal content).

8 Online Safety in the Curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to students on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our students' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas. Educating pupils on the dangers of technologies that may be encountered outside

school will also be carried out via PSHE by presentations in assemblies, as well as informally when opportunities arise.

9 Guidance for Parents

The school seeks to work closely with parents in promoting a culture of online safety. The respective schools will always contact parents if it has any concerns about students' behaviour in this area and encourages parents to share any concerns with the school.

The school will provide information and guidance on online safety by a variety of means (including offering specific online safety guidance at parent forums and other events).

10 The Management of Personal Data

Please refer to the Data Protection Policy and the Acceptable Use Policy for Students for further details.

Staff may only take information off site when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, Staff should securely use remote access tools (such as Office 365 and iSAMS) in lieu of memory sticks. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must immediately be reported to the Director of Computing and ICT.

Appendix 1

Mobile Phones, Smartphones and Personal Devices

1. Purpose

Safeguarding and promoting the welfare of children is everyone's responsibility. The School recognises that online safety is an integral part of safeguarding and that technology is a significant component in many safeguarding and wellbeing issues affecting children and young people. Mobile phones and connected devices can provide benefits in communication and safety, but may also contribute to distraction, reduced social interaction, cyberbullying, child-on-child abuse and exposure to harmful content.

Haberdashers' Schools are committed to providing a calm, focused and purposeful learning environment. As part of this commitment, the School aims to maintain mobile phone-free environments during the school day, enabling students to focus fully on learning, participate positively in school life and develop healthy, age-appropriate relationships with technology. Through a phased smartphone-free strategy the School intends to become smartphone-free from Reception to Year 11 by 2030. This approach supports student wellbeing, strengthens safeguarding, encourages positive social interaction and aligns with the School's wider approach to online safety and digital wellbeing.

It is a requirement of the School that all passengers on our Coach Service have a charged mobile with them, but this must be used in a sensible manner when on the coaches. Mobile phones must not be used to take photos, take videos or access explicit content or any content which is not age-appropriate. Failure to adhere to this will result in a sanction in line with our Behaviour Policy. Where a phone has been confiscated, the school will liaise with parents about transport arrangements.

2. Year Group Expectations

Students in Reception – Year 2

Must not bring personal devices into school. Smart watches and internet-enabled wearable devices are not permitted.

Years 3-6

The Prep and Junior Schools are smartphone-free. Students requiring a device for coach travel should use a basic mobile phone intended solely for communication and safety purposes. Smartphones are not permitted. Devices must be switched off throughout the school day and handed to the designated member of staff on arrival (School Office). Smart watches, smart glasses and other internet-enabled wearable devices are not permitted.

Year 7

Year 7 is smart-phone free. Students travelling independently may bring a basic mobile phone without internet access. Smartphones are not permitted. Devices must be switched off and secured in a Yondr pouch on arrival and remain inaccessible throughout the school day, including educational visits, residential trips, sports fixtures and co-curricular activities. Mobile phones may only be accessed with the explicit permission of a member of staff. Smart watches, smart glasses and other internet-enabled wearable devices are not permitted.

If a Student needs to call home, then arrangements will be made for this via the Head of Section, Head of House, Head of Year or the School Office. There is a sanction ladder in place for any students who do not adhere to the policy.

Years 8-11

Students may bring a smartphone to school if needed. Upon arrival on site, devices must be switched off and secured in a School-issued Yondr pouch. Devices must remain inaccessible throughout the school day, including educational visits, residential trips, sports fixtures and co-curricular activities. Mobile phones may only be accessed with the explicit permission of a member of staff. Smart watches, smart glasses and other internet-enabled wearable devices are not permitted.

If a Student needs to call home, then arrangements will be made for this via the Head of Section, Head of House, Head of Year or the School Office. There is a sanction ladder in place for any students who do not adhere to the policy.

Sixth Form

Sixth Form students may use mobile phones only in designated Sixth Form areas such as the Sixth Form Common Room or designated study rooms in the Sixth Form block/Study spaces (Boys School) or Common Room and Mezz (Girl's School). Phones must not be used in shared spaces used by younger pupils or where visible to younger pupils. Sixth Form students are expected to model responsible and appropriate technology use. Mobile Phones are not to be used in lessons. Smart watches, smart glasses and other internet-enabled wearable devices are not permitted.

3. Yondr Procedures

Daily Procedure

- Switch off device before entering school grounds.
- Place device into pouch.
- Lock pouch in front of staff member (likely form tutor during AM reg).
- Store pouch in school bag or locker.

Late Arrival

Students arriving late must secure devices at Reception.

Early Departure

Students leaving site early may unlock devices through Reception when signing out.

Forgotten Pouches

Students who forget their pouch must hand their device to Reception at the start of the school day. The device will be stored securely and returned at the end of the day. Repeated failure to bring a pouch to school may be treated as a breach of this policy.

Tampering or Damaged Pouches

Any accidental damage should be reported immediately. Where damage appears deliberate, this will normally be treated as a serious breach of this policy and may result in disciplinary sanctions in addition to the cost of replacement. Possession of magnets or attempts to bypass the system will normally be treated as a serious breach of School rules.

Lost and Replacement Pouches

Lost pouches should be reported immediately and a replacement charge of £20 will apply.

4. Communication During the School Day & Accessing School Systems

Parents should contact the School Office if they need to communicate with their child during the school day. Students wishing to contact home should speak to an appropriate member of staff. Mobile phones should not be used for communication during the school day without specific staff authorisation.

If a student needs to access School systems e.g. Onenote / SOCS / emails during the day, these should only be accessed in the library using school devices, and not from mobiles. In Y7-13, mobile phones may not be used in the library for any purpose, except for in exceptional circumstances with permission from the Head of Library. If Sixth Form students wish to listen to music through headphones in the library, they may do so by connecting to their laptop or school device.

5. Medical or Exceptional Circumstances

Alternative arrangements may be agreed where a student requires access to a mobile device for medical reasons. Examples may include diabetes monitoring and other clinically evidenced conditions. Such arrangements must be approved by the Head of Section and reviewed periodically.

6. Sanctions

The School expects our students, with the full support of parents and carers, to comply with the expectations outlined in this policy. Where students fail to comply with the Mobile Phone and Personal Devices section of this policy, including tampering with the Yondr system, parents or guardians will be contacted and the following sanctions will apply in accordance with the Behaviour, Rewards and Sanctions Policy.

- First offence: It will be confiscated until the end of the day and the student will receive an After School Detention / L2.
- Second offence: The phone will be confiscated for a week.
- Third offence: The phone will be confiscated until the next school holiday break.

Confiscated mobile phones will be handed in to the Pastoral Office (Boys' School) or the School Office (Girls' School). A log will be kept of those Students whose phones have been confiscated.

The School does not accept any responsibility for the theft, loss of or damage to mobile devices brought onto School premises, including devices that have been confiscated.

7. Serious breaches

Should the Student use the mobile phone in any way which breaks the Student Code of Conduct or the Acceptable Use Policy, or in a way which causes harm to another student, then more serious sanctions will be applied which may include searching or confiscating the phone,

coach bans, exclusions, and in the case of criminal activity, reporting to the police or other external agencies where appropriate.

The following examples will normally be regarded as a serious breach of this policy:

- deliberately damaging a Yondr pouch
- possession or use of magnets or other devices intended to bypass the Yondr system
- accessing a phone through unauthorised means during the school day
- assisting another student to access a device in breach of this policy
- recording, photographing or filming others without permission
- sharing inappropriate images, videos or content
- behaviour involving cyberbullying, child-on-child abuse or any safeguarding concern facilitated through technology

Viewing Youth Produced Sexual Imagery (Nudes and Semi-Nudes)

Adults should not view youth-produced sexual imagery unless there is good and clear reason to do so. Wherever possible, responses to incidents should be based on what DSLs have been told about the content of the imagery. The decision to view imagery should be based on the professional judgment of the DSL and should always comply with the child protection policy and procedures of the school.

If a decision is made to view imagery the DSL would need to be satisfied that viewing:

- is the only way to make a decision about whether to involve other agencies (i.e. it is not possible to establish the facts from the young people involved)
- is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the pupil or parent

A report may be unavoidable because a pupil has presented an image directly to a staff member or the imagery has been found on a school device or network.

If it is necessary to view the imagery, then the DSL should:

- Never copy, print or share the imagery; this is illegal
- Discuss the decision with the Headmaster or Headmistress
- Ensure viewing is undertaken by the DSL or another member of the safeguarding team with delegated authority from the Headmaster or Headmistress
- Ensure viewing takes place with another member of staff present in the room, ideally the Headmaster/Headmistress or a member of the senior leadership team. This staff member does not need to view the images
- Wherever possible ensure viewing takes place on School or college premises, ideally in the Headmaster's/Headmistress's or a member of the Senior Leadership Team's office

- Ensure wherever possible that images are viewed by a staff member of the same sex as the pupil in the imagery
- Record the viewing of the imagery in the school's safeguarding records including who was present, why the image was viewed and any subsequent actions

Further details on searching, deleting and confiscating devices can be found in the Department for Education Searching, Screening and Confiscation advice.

If youth-produced sexual imagery has been unavoidably viewed by a member of staff either following a disclosure from a pupil or as a result of a member of staff undertaking their daily role (such as IT staff monitoring School systems) then DSLs should be informed.

Viewing youth-produced sexual imagery can be distressing for both young people and adults and appropriate emotional support may be required.

Deletion of images

If the School has decided that other agencies do not need to be involved, then consideration should be given to deleting imagery from devices and online services to limit any further sharing of the imagery. The government's Searching, Screening and Confiscation advice ([Searching, screening and confiscation at school - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/612212/Searching_screening_and_confiscation_at_school_-_GOV.UK.pdf)) highlights that schools have the power to search pupils for devices, search data on devices and delete pupil produced sexual imagery.

However, just as in most circumstances it is not recommended that school staff view imagery, it is recommended that schools should not search through devices and delete imagery unless there is good and clear reason to do so. It is recommended that in most cases young people are asked to delete imagery and to confirm that they have deleted the imagery. Young people should be given a deadline for deletion across all devices, online storage or social media sites.

Pupils are reminded that possession of youth-produced sexual imagery is illegal, even when the imagery is of the pupil who possesses it. They should be informed that if they refuse or it is later discovered they did not delete the image they are committing a criminal offence and the police may become involved. All of these decisions need to be recorded; including times, dates and reasons for decisions made and logged in the safeguarding records. Parents and carers should also be informed unless this presents a further risk to the pupil.