Habs

HABERDASHERS'
ELSTREE SCHOOLS

E-safety Policy

Policy Type	Statutory
Regulation	ISSR: 7
Reviewed by	Deputy Head Pastoral
Last Review	Autumn 2024
Next Review	Autumn 2025

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:

Safeguarding Policy
Anti-bullying Policy
Data Protection Policy
Behaviour Policy
Equality Act 2010
Acceptable Use Policy – Students
Preventing and tackling bullying (July 2017)
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.

The member of staff with responsibility for Individual Needs in the Boys' School is the Head of Academic Support.

The member of staff with responsibility for Individual Needs in the Girls' School is the Head of Individual Needs.

4 Background

The Schools embrace the advantages of modern technology. However, the Schools are mindful of the negative impact of the misuse of technology, such as cyberbullying, child-on-child abuse or exposure to inappropriate content. 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 e-

safety policy is to outline what measures the Schools take to ensure that students work in an e-safe environment and that issues are detected and dealt with appropriately. This policy applies to matters arising at School and using School systems.

The policy pays regard to:

- KCSIE September 2024
- 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

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
- 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 E-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, CICT 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-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 Anti-Bullying 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 schools have put in place through the infrastructure and technical provision safeguards to filter and monitor inappropriate content in line with the updates to KCSIE 2023 and still very relevant in KCSIE 2024 This also fulfils our responsibilities under the PREVENT strategy. A web filter (Smoothwall) monitors and reports to the pastoral department for all students. An additional monitoring system (Senso) monitors key strokes or words that students may be inputting on a Windows device (applies to all Senior School students Years 7-12 Boys and Girls), which also reports to the Pastoral Leadership Team. The latter 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.

A core team including the DSLs in senior school and prep/junior schools, and IT leads, meet half-termly to review our filtering and monitoring provision and to ensure that we are complying or putting provision in place to comply with KCSIE.

6 Roles and Responsibilities

In line with *Keeping Children Safe in Education (2024), 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 manage any disciplinary procedures for pupils which arise as a result of them not following the E-safety Policy or AUP
- To work with the Heads of CICT/PSHE to ensure that the e-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 e-safety to pupils to ensure they know how to stay safe online.

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 e-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 e-safety breach.
  - Reports any e-safety related issues that arise to the DSL and Head of CICT.
- IT Support Team:
  - Assists in the resolution of e-safety issues with the DH Pastoral, Head of CICT 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 via OnlineSCR.

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 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 youth produced sexual imagery, 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

Personal Mobile Phone / Device Guidance

At Habs Senior Schools, we believe that our focus should be on responsible use and knowing how to keep safe and healthy. We are aware that technology has many benefits, but it can also play a significant part in many safeguarding and wellbeing issues, including poor concentration, decreased social interaction, or harmful behaviours towards others, such as cyberbullying or child on child abuse. As a result, we operate a no-phone policy from Years 7-11. This includes in the library or after-school clubs.

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 I line with our Behaviour Policy.

Students in Reception – Year 2

Must not bring personal devices into school.

Years 3-6

In the Junior School (Habs' Girls') students are only allowed a phone for use on the coaches and must hand personal devices into the office, collecting them at the end of the day. They should only have a mobile phone in school if they use the coach service. Smart watches such as Apple watches may not be worn in school.

In the Prep School (Habs Boys) students are only allowed a mobile phone for use on the coaches. All devices should be switched off upon arrival and handed into Form Tutors at the start of the school day. Form Captains will then hand all phones into the office where they will be kept for the duration of the school day. Phones should be collected, by individual pupils at the end of the school day from the school office.

Years 7-11

Students should put their mobile phones away **in their locker** on entry to the school site. Headphones, airpods and other listening devices must not be worn at any time on School premises and mobile phones must not be seen or used during the day for any purpose, unless with permission from a teacher. 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. Smart watches such as Apple watches may not be worn in School. There is a sanction ladder in place for any students who do not adhere to the policy.

Sixth Form

Students must put their mobile phones away in their bags, suit pockets or locker on entry to the school site. The Sixth Form should act as role models to younger years so mobile phones may only be used in Sixth Form areas such as the Sixth Form Common Room or designated

study rooms in the old English Block (Boys' School) / Sixth Form Spaces: Common Room and Mezz (Girls' School). They may not be used in areas where other year groups are present. Mobile phones should not be seen or used in lessons unless the teacher gives permission. Smart watches such as Apple watches may not be worn in school.

Accessing School Systems

If you need 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 Y7-11, mobile phones may not be used in the library for any purpose, except for in exceptional circumstances with permission from the Head of Library.

Sanctions

Where a mobile phone is used in contravention of any of the above rules it will be confiscated and handed in to Mrs Wheeler in the pastoral office (Boys' School) or the School office (Girls' School). The Student will be allowed to collect the mobile phone at the end of the day. A log will be kept of those Students whose phones have been confiscated.

First offence: If a phone is found in the hands of a student once they are on school properly (this includes walking from the coach or car into the school building), phones will be confiscated until the end of the day. A first offence will also result in a lunchtime detention at the Boy's School or a L1 at the Girls' School.

Second offence: If a phone is found in the hands of the student again, within the half term, it will result in an After School Detention at the Boys' School or an L2 at the Girls' School.

Third offence: This will result in the phone being confiscated and parents being asked to collect it in person and meet with the Head of House (Boys' School) or Head of Year (Girls' School).

In the exceptional case that a child may need their phone (e.g. for medical reasons) this should be agreed with the Head of House (Boys' School) or Head of Year (Girls' School).

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.

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.

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) 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.