NOTTING HILL & EALING
HIGH SCHOOL

GDST
GIRLS' DAY SCHOOL TRUST

Whole School

Digital and Online Safety Policy

2024-2025

Contents

1.Policy Introduction and Aims

The purpose of this policy is to:

- Safeguard and protect all members of the school's community when using technology online and in school.
- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns.

The issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material; for example pornography, racist or radical and extremist views, and in some respects fake news
- Contact: being subjected to harmful online interaction with other users; for example children can be contacted by bullies or people who groom or seek to abuse them
- Commercial exploitation: for example young people can be unaware of hidden costs and advertising in apps, games and website
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying

2.Policy Scope

This policy applies to all staff including teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers. It applies to the whole school including the Early Years Foundation Stage. It applies to access to school systems, the internet and the use of technology, using devices provided by the school or personal devices.

The policy also applies to online safety behaviour such as cyber-bullying, which may take place outside the school, but is linked to membership of the school. The school will deal with such behaviour within this policy and associated behaviour and discipline policies, and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

2.1 Links with other policies and practices

This policy links with a number of other policies, including:

- The GDST *Information Security Policy*
- The GDST *Data Protection Policy*
- The school's *Safeguarding and Child Protection Policy*
- The GDST *Safeguarding Procedures* (which incorporates the staff *Code of Conduct*)
- *Acceptable Use Agreements* (AUAs) for staff and pupils
- GDST *Social Media Policy*
- The school's *Behaviour and Discipline Policy*
- The *Anti-Bullying Policy*
- Staff handbook sections
- Student Digital Code of Conduct

3. Roles and Responsibilities

The Designated Safeguarding Leads (DSL) are responsible for online safety.

All members of the community have important roles and responsibilities to play with regard to online safety:

3.1 The Headmaster:

- Has overall accountability for online safety provision
- Ensures that online safety is viewed as a safeguarding issue and that practice is in line with GDST and national recommendations and requirements
- Ensures the school follows GDST policies and practices regarding online safety (including the Acceptable Use Agreements), information security and data protection
- Ensures that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety
- Supports the DSL by ensuring they have sufficient training, time, support and resources to fulfil their responsibilities
- Ensures that all staff receive regular, up to date and appropriate online safety training
- Is aware of what to do in the event of a serious online safety incident, and will ensure that there are robust reporting channels for online safety concerns, including internal, GDST and national support
- Receives regular reports from the DSL on online safety
- Ensures that online safety practice is audited and evaluated regularly in order to identify strengths and areas for improvement.

3.2 The Designated Safeguarding Leads (DSLs):

- Takes day to day responsibility for online safety
- Promotes an awareness of and commitment to online safety throughout the school community
- Acts as the named point of contact on all online safety issues, and liaises with other members of staff or other agencies, as appropriate
- Keeps the online safety component of the curriculum under review, in order to ensure that it remains up to date and relevant to pupils
- Facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Monitors pupil internet usage, taking action where required
- Maintains the online safety incident log and record of actions taken, and reviews the log periodically to identify gaps and trends
- Reports regularly to the Head and SLT on the incident log, internet monitoring, current issues, developments in legislation etc.

3.3 The IT department:

- Apply appropriate technical and procedural controls to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- Keep up to date with the school's online safety policy and technical information in order to carry out their online safety role effectively and to inform and update others as relevant
- Provide technical support to the DSL and leadership team in the implementation of online safety procedures
- Ensure that the school's filtering policy is applied and updated on a regular basis, and oversees the school's monitoring system
- Report any filtering breaches or other online safety issues to the DSL, Head, GDST and other bodies, as appropriate
- Ensure that any safeguarding concerns are reported to the DSL, in accordance with the school's safeguarding procedures.

3.4 All school staff:

- Read, adhere to and help promote the Digital policy, Acceptable Use Agreements and other relevant school policies and guidance
- Take responsibility for the security of school systems and the data they use, or have access to
- Model safe, responsible and professional behaviours in their own use of technology
- Supervise, guide and monitor pupils carefully when engaged in activities involving online technology (including extra-curricular and extended school activities if relevant)
- Have an up to date awareness of a range of online safety issues and how they may be experienced by the children in their care
- Identify online safety concerns and take appropriate action by reporting to the DSL
- Take personal responsibility for professional development in this area.

3.5 Pupils (at a level that is appropriate to their individual age, ability and vulnerabilities):

- Engage in age appropriate online safety education opportunities
- Read and adhere to the school Acceptable Use Agreements
- Respect the feelings and rights of others both on and offline, in and out of school
- Take responsibility for keeping themselves and others safe online
- Report to a trusted adult, if there is a concern online.

3.6 Parents and carers:

- Read the school Acceptable Use Agreements and encourage their children to adhere to them
- Support the school in online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home
- Model safe and appropriate use of technology and social media, including seeking permission before taking and sharing digital images of pupils other than their own children
- Identify changes in behaviour that could indicate that their child is at risk of harm online
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online
- Use school systems, such as learning platforms, and other network resources, safely and appropriately
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

3.7 External groups:

- Any external individual/organisation must sign an Acceptable Use Agreement prior to being given individual access to the school network.

4. Safe Use of Technology (Staff and Students)

The school uses a wide range of technology which includes providing student access to:

- Computers, laptops and other digital devices
- Internet and the web, including cloud services and storage
- Learning platforms
- Email and messaging
- Games consoles and other games based technologies
- Digital cameras, webcams and video cameras
- Virtual reality headsets
- Supervision of pupils will be appropriate to their age and ability
- ***Artificial intelligence***

As well as many benefits, there are, of course, also potential dangers in using the internet and other forms of digital technology, for example the presence of offensive material, the ease with which strangers can make contact, exposure to scams, the use of digital technology by bullies, and issues such as harassment and defamation. Therefore, the school has produced a Digital Code of Conduct, which is set out below, that pupils and their parents must return a signed copy of to the school.

4.1.1 School Network

Online Behaviour

While using school IT systems and devices, students agree to:

- Use IT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes.
- Not download or install software on school equipment without permission.
- Only log on to the school network, learning platform and devices using my own username, email and password.
- Ensure that all communications with pupils, teachers, or others are responsible and sensible. Students also agree not to post aggressive or offensive material on the system or web at any time.
- Not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If material is accidentally come across, students report it immediately to my teacher.
- Not attempt to bypass the internet filtering system.
- Ensure that online activity, both in school and outside school, will not cause the school, the staff, pupils or others distress or bring the school into disrepute.
- Pupils must respect copyright and understand that, particularly in respect to coursework, submitting work downloaded directly from the Internet may invalidate their marks.

Online Safety

When students are accessing the internet, NHEHS students must:

- Be very careful about giving out personal information such as name, phone number or addresses online. Students should not post their information in a social space so that anyone can see it.
- Not arrange to meet someone they only know online unless their parent/guardian/ teacher has clearly approved of this.
- Not use chat rooms, newsgroups or instant messaging, other than those provided by the school.
- Not use the internet to cause distress, harass or bully others or to incite others to do these things (this could include posting photographs of fellow pupils and staff).
- Understand that online contacts may lie about their identity. Students should know that information on the web can be unreliable and be very cautious about who and what they believe.
- Understand that images of pupils and/or staff will only be taken, stored and used for school purposes in line with

school policy and with permission. They will not distribute images outside the school network without permission.
- Support the school approach to online safety and not upload any material that could offend a member of the school community.
- Understand that all their use of GDST systems, including Chromebooks is monitored and logged and can be made available to my teachers. The same is true for own devices when connected to the school network.
- Be aware that if anything makes them uncomfortable or worried, they can share this with a teacher or parent without being blamed.

This Code of Conduct applies to the services that the GDST provides which can also be accessed away from school via the internet.

4.1.2 Use of AI

Artificial Intelligence (AI) is a broadly used term to describe machines/programs that are able to simulate human intelligence. Generative AI describes the algorithms that create new content based on human commands, for example Chat GPT. This section of the code of conduct describes how NHEHS students must conduct themselves when using these AI technologies.

NHEHS students must:

- Use AI in a **responsible and ethical manner,** adhering to all school policies, and especially when it comes to **plagiarism**. Use of AI must be **referenced** and **explained** in their work.
- **critically evaluate and verify** AI-generated outputs with trusted sources before accepting it as true as they do not always produce accurate results, and may contain **bias** or create "**fabrications"**.
- safeguard their online safety and privacy by **avoiding sharing personal information** with AI tools
- seek **help and guidance** from their teacher if they encounter any challenges or concerns.

Misconduct in academic work is covered in the **Academic Integrity Policy.**

4.1.3 Chromebooks

All girls in Years 7-11 are issued with a school-managed Chromebook which they are responsible for both in and out of school. These devices are leased by the school and are recalled and replaced every three years. On receiving their Chromebook, girls and their parents agree to the following Acceptable Use Agreement:

- Chromebooks are only to be used for school purposes.
- Chromebooks are to be brought to school everyday with a full charge.
- The Chromebook should be stored in a secure location either locked in a school locker or at home.
- The use of the Chromebook is monitored both at home and in school and the usage logs are checked by the Deputy Head Pastoral and shared with other colleagues as necessary.
- Chromebooks are not to be used at break or lunchtime, unless for completing work silently in the Library.
- The school's Digital Acceptable Use Policy is to be adhered to at all times when online.
- No software must be downloaded or installed onto the Chromebook without permission.
- They must only log on to their Chromebook with their own email address and password.
- Care must be taken not to damage or lose the Chromebook, with parents accepting liability for any repair or maintenance costs. Please see Chromebook Repair and Replacement Policy for more details.
- Replacement chargers and styluses can be purchased from the IT office via ParentPay.
- The external appearance of the Chromebook must not be damaged or defaced in any way. This includes stickers/skins being applied to the device.
- The Chromebook must be returned to school as and when required.
- Girls are also required to be equipped with plug-in headphones (not Bluetooth) in all lessons, for use with the Chromebooks.

Any pupil seen not adhering to this agreement should be reported to their tutor/HoY and the Assistant Head IT. Staff should record any girls who have failed to bring a charged Chromebook and headphones to their lesson using the Behaviour Manager shortcut in the register in SIMS. Girls needing to emergency charge their Chromebook during the school day may do so using one of the charging lockers in school. All staff are encouraged to be vigilant in enforcing the 'no-Chromebook outside of lessons' policy, with the exception of independent work in the library.

Chromebook Repair and Replacement

In the event of a Chromebook being damaged, the school will attempt to repair the device in house. Any cost of replacement parts will be passed on to parents. Where the device cannot be repaired, or is lost, parents will be liable for the full cost of replacement.

As students are responsible for the maintenance of the device, they are encouraged to purchase protective cases for the Chromebook. Students should not apply any stickers/skins to the device.

4.1.4 Use of Personal Devices and Mobile Phones

Pupils are permitted to bring mobile phones and digital devices to school, but their use is subject to the following guidelines:

- Students in **Years 5 to 8** should not have a smartphone in school. If parents want their daughter to have a phone for safety reasons, they will need to purchase a 'brick' phone and it is their choice as to which phone to purchase.
- Girls in the **Junior School** and from **Year 7 to Year 11** in the Senior School may not use mobile phones at any time during the school day, unless permission is given for a specific educational reason.
- In the **Junior School** it must be turned off and handed to their class teacher on arrival, and then collected at the end of the day.
- Students from **Years 7 - 11** must put their phones in their lockers on arrival and they will not be allowed to use their phones once on the school site. The length of time for confiscation if not adhering to this school rule is a week. If a phone is confiscated and parents are concerned that their daughter should have a phone for safety reasons, we suggest she has a 'brick' phone while it is confiscated or another phone of their choice.
- For girls in **Year 12 and Year 13**, mobile phones should be switched off and kept out of sight during lessons, while girls are in the main school buildings and when walking between buildings. **Year 12 and 13** girls may use their phones in the Sixth Form Centre, as long as this is not in a manner or place that is disruptive to others or to the normal routine of the school.

These guidelines also apply to the use of mobile phones during school trips, extra-curricular activities or other off-site supervised activities. Girls should keep their phones switched off and in their bags (Senior School) or with the teacher (Junior School). They may only be used if permission is given by the member of staff in charge of the trip.

Responsibility for the phone rests with the pupil and the school accepts no financial responsibility for damage, loss or theft. (Any mobile phone found 'lost' in school should be handed in to the school office).

Communication with home

If there is an emergency which requires communication with home, pupils should speak to a member of staff who will help them. Pupils will be able to use a phone in the school office to call home if necessary.

If a parent needs to contact their daughter, for instance in an emergency, they should phone the school office for a message to be passed on to the pupil, rather than trying to contact a girl directly on her mobile phone. This ensures that a pupil is given support and privacy in dealing with a potentially difficult situation.

If an after school fixture or club is cancelled on the day, parents will receive a message via Schoolcomms by email or text, as appropriate.

4.3 Use of Personal Devices and Social Media

All members of the school community are expected to engage in social media in a positive, safe and responsible manner, at all times.

Parents, Carers, Visitors and Staff

- Members of staff will ensure that the use of personal phones and devices takes place in accordance with the law, as well as relevant school policy and procedures, such as: Confidentiality, Safeguarding and Child Protection, Data Security and Acceptable use Agreements.
- Images of pupils must not be stored on personal devices.
- Staff should not use their phone when teaching unless it is an emergency or permission has been sought from the Headmaster.Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's policies.
- The school will ensure appropriate signage and information is provided to inform parents, carers and visitors of expectations of use
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches of school policy.

Pupils

- The school is aware that many popular social media sites state that they are not for children under the age of 13. The school will not create accounts specifically for children under this age
- The use of social media during school hours for personal use is not permitted.
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies.

4.4 Legislation

Most electronic information is protected by copyright, similar to books, music, or plays. Staff and students must avoid copyright infringement, particularly by copying material without proper acknowledgment (Copyright, Designs and Patents Act 1988). Misuse of computers, including unauthorised access, file modification, and installing malicious software, is illegal (Computer Misuse Act 1990). Personal data will be handled according to GDPR and GDST's Privacy Notices, detailed in the school's Data Protection Policy.

5.Education and Engagement

5.1 Education and engagement with pupils

The school curriculum includes age-appropriate lessons and activities on online safety for all pupils, intended to raise awareness, build resilience and promote safe and responsible internet use by:

- Ensuring education regarding safe and responsible use precedes internet access
- Including online safety across the curriculum, including the Personal Social and Health Education, Relationships and Sex Education and Computing programmes of study, covering use both at school and home
- Regularly reinforcing online safety messages when technology or the internet is in use
- Ensuring that the needs of pupils considered to be more vulnerable online, such as those with SEND or mental health needs, are met appropriately

- Using support, such as peer education approaches and external visitors, to complement online safety education in the curriculum
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Teaching pupils to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Supporting students in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making

The school will support pupils to read and understand the *Acceptable Use Agreement* in a way which suits their age and ability by:

- Discussing the AUA and its implications, and reinforcing the principles via display, classroom discussion etc.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- Recognising positive use of technology by pupils

6. Reducing and Responding to Risks

6.1 Reducing online risk

The internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The school will:

- Regularly review the methods used to identify, assess and minimise online risks
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material
- Ensure, through online safety education and the school AUAs, that pupils know that the school's expectations regarding safe and appropriate behaviour online apply whether the school's networks are used or not
- The school will monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied in practice

The policy framework will be reviewed by the GDST at least annually, and in response to any new national guidance or legislation, significant developments in the use of technology, emerging threats or incidents that have taken place

6.2 Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns
- Incidents will be managed depending on their nature and severity, according to the relevant school policies
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the ITS or Legal Department at the Trust Office.
- Where there is suspicion that illegal activity has taken place, the school will contact the Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or the Local Authority first, to ensure that potential investigations are not compromised.

6.2.1 Concerns about Pupils' Welfare

- The DSL will be informed immediately of any online safety incident that could be considered a safeguarding or child protection concern
- The DSL will ensure that online safeguarding concerns are escalated and reported to relevant agencies
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

6.2.2 Misuse

- Complaints about IT misuse by pupils will be dealt with by a senior member of staff under the relevant policies and procedures and according to the nature of the complaint
- Any complaint about staff misuse will be referred to the Headmaster
- Pupils and parents are informed of the school's complaints procedure.

7. Useful links and sources of advice

7.1 Guidance and resources

- Teaching Online Safety in School (DfE)
- Education for a Connected World (UKCIS)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
- Harmful online challenges and online hoaxes (DfE)
- Cyberbullying: understand, prevent and respond (Childnet)
- Cyberbullying: advice for headteachers and school staff (DfE)
- Meeting digital and technology standards in schools and colleges March 2022 (DfE)
- Generative artificial intelligence in education (DfE)

7.2 National Organisations

- Action Fraud: www.actionfraud.police.uk
- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
    - ChildLine: www.childline.org.uk
    - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
    - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
    - Telephone helpline: 0844 381 4772

Reviewed July 2024

Next review July 2025