FHS

Francis Holland Schools

Online Safety Policy

Table of Contents

Online Safety Policy

This policy applies to:
Francis Holland Regent's Park **Francis Holland Sloane Square** **Francis Holland Prep**
Where there are differences between the schools these have been clearly highlighted.

Related Policies:
Safeguarding & Child Protection Policy
Anti-Bullying Policy
Data Protection Policy
Privacy Notices
Pupil Digital Code of Conduct
Staff Digital Technology Acceptable Use Agreement
Microsoft Surface Acceptable Use Agreement
Digital Learning Device Policy
Artificial Intelligence (AI) Policy

1. Scope

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

2. Aims

The Schools aim to support the well-being and progress of each pupil while using technology and the internet both in and out of school, and to provide appropriate systems and procedures for the safer use of technology.

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories;
- **Contact** – being subjected to harmful online interaction with other users, such as child-to-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

To meet our aims, the Schools will:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- Protect and educate the whole school community in its safe and responsible use of technology;
- Set clear guidelines for the use of devices for the whole school community;
- Establish clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate.

3. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Filtering and monitoring standards
- Generative AI: product safety expectations

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

4. Roles and Responsibilities

4.1 Key People

Sloane Square	**Regent's Park**	**Prep School**
DSL	DSL	DSL
Deputy DSLs	Deputy DSLs	Deputy DSLs
Director of Digital Learning	Director of Digital Learning	

4.2 Everyone

Everyone who comes into contact with children has a role to play in identifying concerns, sharing information and taking prompt action.

4.3 The School Council (Governing Body)

The governing board has overall responsibility for monitoring this policy and holding the Heads to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Governor who oversees online safety is Simon Hay.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

4.4 Heads and Senior Leadership Teams (SLTs)

Heads and Senior Leadership Teams will:

- Have a duty of care for ensuring the safety (including online) of members of the school community;
- Ensure that staff understand this policy, and that it is being implemented consistently throughout the schools.

Designated Safeguarding Leads (DSLs)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Heads in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

- Working with the Director of Technology to make sure the appropriate systems and processes are in place
- Working with the Heads, Director of Technology and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Heads and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- This list is not intended to be exhaustive.

4.5 Director of Digital Learning (SSQ and RP)

- *Support the DSL and DDSLs with staff training on online safety matters;*
- *Promote awareness of online safety matters throughout the school community;*
- *Promote the online safety curriculum.*

4.6 Online Safety Group

- Annually review the school's approach to online safety;
- Consult on other online safety matters.

4.7 Director of Technology

- Responsible for trust-wide IT strategy.
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

4.8 IT Systems Manager

- Responsible for technical matters pertaining to online safety;
- Ensures the security of digital systems;
- Ensure provision of appropriate monitoring and filtering systems.

4.9 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by logging the incident on CPOMS and emailing the IT team
- Following the correct procedures by emailing the IT team if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

4.10 Pupils

- Use technology responsibly and abide by the school's rules on its appropriate use;
- Report online safety concerns to any member of staff, use the online safety email address or the anonymous reporting tool.

4.11 Parents and Carers

- Support their children in learning to use technology responsibly.
- Notify the DSL or the Head of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

4.12 Visitors and Members of the Community

- Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use
- Where access to the school's internet is offered to visitors, this is monitored, subject to appropriate limits and at the absolute discretion of the school.

5. Curriculum and Training

5.1 Staff Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection policy.

5.2 Pupil Curriculum

Francis Holland Prep

Pupils will be taught to:

- Use technology safely, responsibly and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- By the **end of Year 6**, pupils will know:
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Francis Holland Regent's Park and Francis Holland Sloane Square

Pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- How to report a range of concerns
- Online safety content is taught in Wellbeing / PSHE and Computer Science.
- By the **end of Year 11** pupils will know:
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- The safe use of social media and the internet will also be covered in PSHE and other subjects where relevant.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.
- Online Safety is also a regular subject of form periods and assemblies.
- Online Safety topics are addressed in a range of curriculum subjects where relevant, for example reflecting on bias and reliability of online sources when doing online research or discussing online communications before using a new online platform.

Under the DfE's Relationships Education, Relationships and Sex Education and Health Education guidance, from September 2025, schools have an extended remit regarding teaching pupils about online harms and pornography within the RSE/PSHE curriculum. This will include:

- Pornography's negative influence on sexual attitudes and behaviours
- Deepfakes and AI-generated imagery

- Sextortion and online scams
- Harmful online content
- The serious legal consequences of sharing indecent images of under-18s

6. Educating Parents/Carers about Online Safety

The schools will raise parents/carers' awareness of online safety in letters or other communications home, and in information via MSP. This policy will also be shared with parents/carers on our website. Online safety will also be covered during parent talks.

The schools will let parents/carers know:

- What systems the schools use to filter and monitor online use
- How to help support their children's use of digital technologies

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the Heads.

7. Filtering and Monitoring of IT (including AI usage)

The Trust's filtering and monitoring tools will ensure that harmful and inappropriate content is reliably filtered and prevented throughout all user interactions, including across languages, images and abbreviations. The filtering adapts dynamically based on user age, risk level, context and specific needs, including users with SEN/D. Filtering and monitoring is applied consistently across all devices, including BYOD and smartphones, when they are accessed via the school network.

7.1 Filtering

- Internet access is filtered for all users using an appropriate tool and best practice should be followed. Lists of blocked sites are regularly updated.
- Filtering should address the four areas of risk identified in the Aims section above.
- There is a procedure for blocking and unblocking sites/YouTube videos which can be found in the appendix.

	Sloane Square	Regent's Park	Prep School
Filtering/Firewall	Sophos / Lightspeed		
Monitoring	Lightspeed		
Other	Darktrace Email/Network, Sophos Antivirus	Darktrace Email/Network, Sophos Antivirus	Darktrace Email, Sophos Antivirus

7.2 Monitoring

- The schools monitor the use of its devices, systems, communication services and digital platforms;
- The schools monitor the use of other devices (i.e. those not owned by the school) using its systems with due regard to users' privacy.
- The DSLs log behaviour and safeguarding issues related to online safety.

- This policy will be reviewed every year by the DSLs. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

7.3 Digital Platforms

- The IT Systems Manager and Directors of Digital Learning will, to the best of their ability, keep records of the digital platforms used by the Schools. These are available on request.
- Where staff wish to use a new digital platform, they should inform the Director of Digital Learning (**Sloane Square**) /IT Systems Manager (**Regent's Park**) / IT Systems Manager (**Francis Holland Prep**)
- Where the School assesses that a digital platform presents an elevated online safety risk, the School will conduct a risk assessment for the platform and implement any additional controls.

7.4 Software and Platforms

- Appropriate records of software, platforms and licenses are kept.
- Where pupils are asked to register online accounts to access digital platforms, the minimum of identifiable personal information will be disclosed and only school email addresses will be used.

7.5 Acceptable Use Agreements

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate

Pupils are expected to read through the Pupil Digital Code of Conduct at the start of every academic year which makes pupils aware that their use of school platforms is monitored. The code of conduct is reviewed every year and outlines how every pupil is expected to be a responsible user of the internet and other digital technologies and stay safe while employing them for educational, personal and recreational use.

8. Protecting Data

Personal data should be handled in accordance with the Data Protection Policy.

- Secure access to personal data is provided on and offsite using school approved platforms;
- Personal data should only be stored using school systems and should not be saved on personal devices;
- Pupils' images, video, and work may be made available to parents on appropriate platforms;
- Removable media should not normally be used for the storage or movement of personal data. Where their use is unavoidable, appropriate encryption must be used. School-managed mobile and portable devices are encrypted.

9. Online Safety Incidents

9.1 Responding to Online Safety Incidents

- The Schools manage online safety incidents within the context of the Safeguarding and Child Protection and Behaviour and Sanctions policies;
- The DSL will work with the DDSLs, Director of Digital Learning, and other staff, as necessary, to address any online safety issues or incidents.

9.2 Reporting

- Staff should report online safety incidents on CPOMS;
- Pupils should report all online safety incidents or concerns. They can report to any member of staff, use the online safety email address (Sloane Square) or the anonymous reporting tool ('Whisper')

9.3 Recording

Online safety incidents will be logged by the DSL as part of the school's pastoral records.

9.4 Reviewing

The DSL and relevant members of the safeguarding team will review online safety incidents regularly and make recommendations for changes to policies, staff training, the online safety curriculum and other elements of practice.

9.5 Managing

Once an online safety incident is reported, it will be assessed, and a response determined by the DSL and pastoral team.

10. Cyber-Bullying

10.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the Behaviour and Sanctions policy.)

10.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff and governors receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Behaviour and Sanctions policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

10.3 Examining Electronic Devices

The Heads, and any member of staff authorised to do so by the Heads as set out in our Searches of Pupils policy, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Staff may confiscate any electronic device which, in their view, is being or may be used inappropriately. When a member of staff confiscates an electronic device, it should be:

- Turned off;
- Handed to a relevant member of the safeguarding or pastoral team or the school office at the first available opportunity.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL/DDSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL /DDSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Searches of Pupils Guidance

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

11. Artificial Intelligence (AI)

The Trust recognises the potential of AI, including generative AI (Gen AI) and large language models (LLMs), to transform leadership, teaching, learning, and administration.

Gen AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The Artificial Intelligence (AI) Policy sets out how we use AI to improve educational outcomes, reduce staff workload, and prepare pupils for the future. Our approach ensures safe, fair, and inclusive implementation of AI in line with UK regulations, including UK data protection legislation UK GDPR (DPA) and The Children's Code.

FHS recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

FHS will treat any use of AI to bully pupils in line with our Anti-bullying, and Behaviour and Sanctions policies.

Staff must only use approved AI platforms and must inform their school's Senior Leadership Team and Digital Leads if they wish to trial or adopt new AI tools. If the tool is then approved via the AI Tool Evaluation Checklist (Appendix D), staff may proceed with their trial. The Director of Technology will perform a DPIA if deemed necessary.

For full details, please see the Trust's Artificial Intelligence (AI) Policy, which applies to all staff, pupils and third parties, and the DfE's Generative AI: Product Safety Expectations guidance which covers how to use generative AI safely, and how filtering and monitoring requirements apply to the use of generative AI in education (Generative AI: product safety expectations - GOV.UK).

12. Mobile Technologies (Including BYOD/BYOT)

If the primary purpose for the use of mobile/personal devices in the school context is educational. The school permits staff and pupils to connect personal devices to the school networks and will provide appropriate levels of access.

12.1 Mobile Phones and Smart Watches

Rules are published concerning appropriate use and will be regularly updated, these documents can be found in the appendix.

12.2 Devices For Learning

- Pupils have an approved digital learning device to use in lessons. Other devices should not be used during lesson time;
- The use of devices in lessons is decided by the classroom teacher and sanctions may be applied where the school becomes aware of their misuse;
- The school sets appropriate rules for the use of devices at other times;
- The school may manage some features of learning devices.

13. Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software (this is installed on all Trust devices by IT).
- Keeping operating systems up to date by always installing the latest updates
- Never leaving their device unattended in a vehicle, even in the boot out of sight.

Staff members must not use the device in any way that would violate the school's terms of acceptable use. If staff have any concerns over the security of their device, they must seek advice from the IT Help Desk in SSq and RP, and the DSL in FH Prep.

14. General Guidance: Good Practice and the Use of IT

14.1 Personal Devices

- Pupils and staff may make reasonable use of personal devices in school for personal, educational and professional purposes, provided that relevant rules, guidelines and professional standards are followed, including the provisions of the acceptable use agreements/Pupil Digital Code of Conduct;
- Before using a personal device in school, staff/pupils should seek approval from the Network Manager.
- Staff should not download staff or pupil data directly to their own device.
- If their personal device is compromised and it has been used to access school data/information, it should be reported as a potential breach.

14.2 Communications

When using communication technologies, the school considers the following as good practice:

- Digital communication between staff and pupils must take place using school email, Microsoft Teams and other approved platforms;
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content;
- Communication between staff and pupils must not be made using personal email, social networks or messaging platforms. Pupils should not use personal accounts to communicate with staff. **Where this occurs, staff should self-report to the DSL at once. Further guidelines apply where a member of staff is related to a pupil or a family friend, these are detailed in the Staff Code of Conduct;**
- Staff should not email pupils outside of reasonable school hours (approx. between 7.30am – 5.30pm). Where this is unavoidable, staff should copy an appropriate member of staff such as a Head of Year or Head of Department;
- Telephone communication should take place using the school phone system or a school-owned mobile. Where this is not possible and communication is essential, staff should withhold their personal mobile number and remove any pupil or parent/carer numbers from their phone;
- Users must immediately report, any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should not respond to any such communication;
- Pupils can report to any member of staff. In addition, we provide a range of other reporting channels at the senior schools:
  - **FH Sloane Square**
    - Online safety email (digitalsafety@fhs-sw1.org.uk)
    - Whisper Anonymous Reporting
  - **FH Regent's Park**
    - Whisper Anonymous Reporting
- Staff should report to the DSL, IT Systems Manager or Director of Digital Learning.

14.3 Social Media

When using personal social media, school staff must:

- Not refer to members of the school community by name or publish their personal details;
- Not communicate or connect with pupils;
- Not engage in online discussion on personal matters relating to members of the school community;
- Ensure that all content is legal, appropriate and in keeping with professional standards, making use of appropriate privacy settings;
- Make clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer;
- Further guidelines apply where a pupil is related to or a family friend of a member of staff, **these are detailed in the Staff Code of Conduct.**

14.4 Photographs and Personal Details

- Staff must not take or store photographs, recordings or video of members of the school community on personal devices;
- Pupils must not take or store photographs, recordings or video of staff on personal devices, without the permission of the relevant staff member;
- Pupils and parents should not share photographs, recordings or video of members of the school community on social networks or messaging platforms without consent;

- Pupils must not share photographs or video of the school buildings or people wearing school uniform on social networks, messaging or other digital platforms;
- The personal details of staff, including their names, must not be shared on social networks, messaging or other digital platforms.

14.5 School Website and Official Platforms

The Schools may publish appropriate details about staff and pupils on its website and other official communications channels.

The following types of incident have features particularly relevant to online safety:

- Child abuse imagery
- Youth-produced sexual imagery
- Cyber-bullying
- Grooming and child exploitation (including by extremists and criminals)

Incidents will be handled in accordance with the Safeguarding & Child Protection, Anti-Bullying and Behaviour policies with a view to the pastoral well-being of those involved.

15. How The School Will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and Sanctions. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

16. Review

Policy author/s	RP: Deputy Head Pastoral and DSL SSq: Senior Deputy Head Pastoral and DSL Prep: Senior Deputy Head and DSL Trust: Director of Technology
This review	Summer 2025
Approved by	Safeguarding Committee, Autumn 2025
This policy published	1st September 2025
Next review	Summer 2026

Appendix 1: Procedure for Blocking and Unblocking Websites/YouTube Videos

Overview

This document outlines the steps to block and unblock websites for the school network, in order to ensure the safety and security of the pupils and staff. The procedure involves a request from a teacher or staff member, the verification and approval of the request by the IT team and a DSL or DDSL, and the update of the documentation on Confluence by the IT team.

Procedure

- A teacher or staff member who wants to block or unblock a website/YouTube video for the school network should submit the request to the IT helpdesk.
- The IT team should review the request and check the following criteria:
    - The website is relevant and appropriate for the educational or operational purposes of the school.
    - The website does not contain any harmful, illegal, or inappropriate content that may pose a risk to the pupils or staff.
    - The website does not interfere with the network performance or security of the school.
- The IT team should forward the request to a DSL or DDSL for approval. The DSL or DDSL should review the request and check the following criteria:
    - The website is consistent with the school's safeguarding policy and procedures.
    - The website does not expose the pupils or staff to any online threats, such as cyberbullying, grooming, radicalisation, or exploitation.
    - The website does not violate any ethical, legal, or professional standards.
- If the DSL or DDSL approves the request, they should notify the IT team.
- The IT team should then proceed to block or unblock the website for the school network, following the technical guidelines and protocols.
    - Once the website is blocked or unblocked, the IT team should update the documentation on Confluence, including the following information:
    - The name and URL of the website.
    - The date and time of the blocking or unblocking.
    - The name and role of the approver (DSL or DDSL).
    - The reason for the blocking or unblocking.
- The IT team should also inform the requester and the approver via email that the website has been blocked or unblocked, and provide them with the link to the documentation on Confluence.

Appendix 2 – Use of Mobile Phones: Francis Holland Sloane Square

Use of mobile phones **by pupils**

We believe that it is really healthy for children to enjoy time away from mobile phones and while we understand that our pupils may have a mobile phone at school if they are travelling to and from school independently, they must not be used in school.

Specifically, pupils in Years 7-11 must not use their mobile phones during the school day, including during lessons, in the time between lessons, at breaktimes and at lunchtimes. Sixth formers may only use mobile phones in designated areas of the OSH, and not during lessons.

- **On arrival to school, pupils are required to do the following:**

  Year 7 to Year 11

  Pupils will turn their phones off and lock their phones in Yondr pouches* for the entirety of the school day. There will be unlocking stations in the pupil entrance and in the school office. If a pupil needs to leave during the school day, they will go to the office to unlock their phone.

  Sixth Form

  Pupils may use mobile phones in designated areas of the OSH. This is to reflect their increased independence and responsibility but must not compromise our policy on the use of mobile phones for other pupils.

  **Yondr pouches are purchased by the school and loaned to pupils. Lost pouches cost £30 to replace and this charge will be added to the end of term bill.*

- **On leaving the school:**

  All pupils are advised to put their mobile phones in a zipped pocket before leaving the school premises to minimise the risk of phone snatching and to ensure they are fully alert when crossing roads**.**

Sanctions

So that the school can be a mobile free school, sanctions will be used in the following ways to ensure fairness.

If a pupil fails to secure their mobile phone in the Yondr pouch, they will receive a level 2 detention and their phone confiscated for the remainder of the day. Using the phone during the day or deliberately deceiving staff could incur a higher sanction.

Any use of mobile devices in school by pupils must be in line with the Pupil Digital Code of Conduct.

Any breach of the Pupil Digital Code of Conduct by a pupil may trigger disciplinary action in line with the Behaviour and Sanctions policy, which may result in the confiscation of their device.

Use of mobile phones **by staff**

Staff are permitted to use their mobile phones in staff common areas but are asked to refrain from using them when pupils may be present. This includes (but is not limited to) corridors, the dining room and classrooms. Staff may use their phone to take the register but should then keep it out of sight for the rest of the lesson.

Use of mobile phones by **parents/carers, volunteers and visitors**

Parents/carers, visitors and volunteers (including governors and contractors) must adhere to the school's online safety policy as it relates to staff if they are on the school site during the school day.

This means:

- Not taking pictures or recordings of pupils.
- Not using phones for personal use in lessons, or when working with pupils.

Parents/carers, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school. These rules are:

Use of mobile phones and similar devices in our school

- Please keep your mobile phone on silent/vibrate while on the school grounds
- Please do not use phones where pupils are present. If you must use your phone, you may go to the school office
- Do not take photos or recordings of pupils or staff. This applies to all school events unless otherwise instructed by a member of staff.
- Do not use your phone in lessons, or when working with pupils

The school accepts no responsibility for phones that are lost, damaged or stolen while you are on the school grounds.

Parents/carers must use the school office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on their personal mobile during the school day.

Appendix 3 - Use of Mobile Phones: Francis Holland Regent's Park

Use of mobile phones **by pupils**

Pupils should not use their mobile phones during the school day, including during lessons, in the time between lessons, at breaktimes and at lunchtimes. Sixth formers may only use mobile phones in designated areas of Linhope House, and not during lessons.

Due to travelling to and from school parents may wish their child to have a phone. However, upon arrival to school, pupils are required to do the following:

IIIs/LIV Pupils will turn their phones off and secure their phones in their Yondr pouches*, before locking them in their locker for the entirety of the school day. There will be unlocking stations in the basement, school exits and in the school office. If a pupil must leave during the school day, they will go to the office to unlock their phone.

UIV/LV Pupils will turn their phones off and hand their phones to staff on duty in the Hall and collect them at the end of the school day.

UV Pupils will turn their phones off and keep them in their school bag or locker for the entire school day. This is to reflect their increased independence and responsibility but must not compromise our policy on the use of mobile phones for other pupils.

VI Pupils will turn their phones off and not use their phones during lessons but may use them in designated areas of Linhope House. This is to reflect their increased independence and responsibility but must not compromise our policy on the use of mobile phones for other pupils.

*Yondr pouches are purchased by each pupil via the school, and parents will be billed a one-off fee of £30 in their first school bill. Lost pouches must be purchased at an additional (£30) cost. Each new intake of IIIs will purchase Yondr pouches, until all pupils up to the UV will be using them.

The school may permit pupils to use a mobile phone in school, due to exceptional circumstances. This will be considered on a case-by-case basis. To request such permission, pupils or parents/carers should contact their Head of Year. Otherwise, if parents need to get a message to their daughters, they may contact the school office.
Any pupils who are given permission must then adhere to the school's online acceptable use agreement for mobile phones.

All pupils/pupils are advised to put their mobile phones in a zipped pocket before leaving the school premises to minimize the risk of phone snatching and be more alert when crossing roads.

Sanctions

So that the school can be a mobile free school, sanctions are used to ensure fairness.
Minor infringements such as not turning off a mobile phone may result in a blue slip, contributing to the school's wider behaviour policy. Not locking a phone away or being found to have another hidden phone and then using the mobile phone during the school day may result in more serious sanctions, depending on the severity of the breach of the pupil IT acceptable use agreement.

Use of mobile phones **by staff**

Staff are permitted to use their mobile phones in staff common areas but are asked to refrain from using them when pupils may be present. This includes (but is not limited to) corridors, the dining room and

classrooms. Ideally, staff would use their laptops to take registers, but if they need to use their phone, it should be kept out of sight for the rest of the lesson.

Use of mobile phones **by parents/carers, volunteers and visitors**

Parents/carers, visitors and volunteers (including governors and contractors) must adhere to the school's online safety policy as it relates to staff if they are on the school site during the school day.
This means:

- Not taking pictures or recordings of pupils, unless it's at a public event (such as a school fair), or of their own child.
- Using any photographs or recordings for personal use only, and not posting on social media without consent.
- Not using phones in lessons, or when working with pupils.

Parents/guardians, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.

Parents/guardians must use the school office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on their personal mobile during the school day.

Use of mobile phones and similar devices in our school

- Please keep your mobile phone on silent/vibrate while on the school grounds
- Please do not use phones where pupils are present. If you must use your phone, you may go to the school office
- Do not take photos or recordings of pupils (unless it is your own child), or staff
- Do not use your phone in lessons, or when working with pupils

The school accepts no responsibility for phones that are lost, damaged or stolen while you are on the school grounds.

A full copy of our Online Safety Policy is available from the school office.

Appendix 4: Use of Mobile Phones: Francis Holland Prep

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 Pupil 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.

The Curriculum

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. We do this by:

- Having a clear, progressive online safety education programme as part of the Computing curriculum and PSHE curriculum.
- Regularly reminding pupils about their responsibilities through the Pupil Acceptable Use Policy
- Being aware of what devices are being used by pupils, at school and at home, including the most popular games and apps.
- Ensuring pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Using support from external visitors and speakers, 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 what they see online and shown how to validate information before accepting its accuracy.
- Supporting pupils 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.
- Ensuring that the needs of pupils considered to be more vulnerable online, such as those with SEND or mental health needs, are met appropriately.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.

Parents and carers

The Prep School understands that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents. We do this by:

- Providing information and guidance on online safety in a variety of formats, this will include parent talks and newsletter items
- Drawing parents' attention to the school online safety policy and expectations
- Requiring parents to read the Pupil Acceptable Use Agreement and discuss its implications with their children.

Mobile Phones

- With the exception of Year 6 pupils who have been given permission to walk to school without an adult, mobile phones are NOT permitted in school. If they did so they would be confiscated on sight and returned to parents.
- If a Year 6 pupil has permission to walk to school, she may bring a mobile phone to school but this must be handed in to the front desk as soon as they arrive at school. It is collected at the end of the school day or after clubs.
- Staff are permitted to use their mobile phones in staff common areas but are asked to refrain from using them when pupils may be present. This includes (but is not limited to) corridors, the dining room, the playground and classrooms.
- Parents/carers, visitors and volunteers (including governors and contractors) must adhere to the school's online safety policy as it relates to staff if they are on the school site during the school day.
- Parents/carers, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.
- Parents/carers will be given clear instructions not to take photographs or recordings of pupils during events or school trips.

Devices

- The Prep School has laptops located in charging banks in the Year 5 and 6 classrooms.
- These devices are used by Year 3 to 6 in Computing and Reasoning lessons. These devices may also be used in other lessons where digital learning may complement the curriculum.
- All pupils log in using their usernames and a generic password
- No pupil is left unattended with a device

EYFS

- EYFS staff do not take mobile phones into the classrooms.
- The EYFS mobiles devices are used for taking photographs of the pupils, as well as for maintaining assessment records through the Tapestry EYFS Profiles software.

Photographs in the Prep School

- The school has two trip phones that are taken out by the Trip Leaders. Photographs of the pupils are taken using these phones and then uploaded

- The school has a number of iPods, linked to a school iCloud account. These can also be used to take photographs of the pupils in lessons and on school trips. Prep School Microsoft surfaces can also be used for this purpose. Staff must not take photographs on personal devices.