FHS
Francis Holland Schools

Name of Policy	Online Safety
Author	Director of Digital Learning Responsible Staff DSLs
Committee for Review & Approval	Safeguarding Sub-Committee
Date of Last SLT Revision	February 2024
Date of Committee Approval	January 2023
Date of Next SLT Review	Autumn 2024
Date of Next Committee Review & Approval	Spring 2025
Regulation Number	n/a
Regulation Description	n/a

Revision History This section should be completed by the reviewer each time this policy is reviewed	
Changes made [brief description of edits]	Date [Term and Year]
Reviewed and adopted by the Trust – names changes and input from Regent's Park	Spring Term 2023
Refers to online as opposed to digital safety	Spring 2024

Availability of this document:

Copies of this document are available digitally at francisholland.org.uk/policies or printed on request from the school office:

- Regent's Park - Ivor Place, London, NW1 6XR
- Sloane Square - 39 Graham Terrace, London, SW1W 8JF

Application of this document:

This policy applies to all FHS Trust Schools. Where there are differences in procedures between the schools this has been clearly highlighted in the appendices

Contents

Contents 2

Scope 3

Related Policies & Documents 3

Aims 4

Roles and Responsibilities 4

- Key People 4
- Everyone 4
- The School Council (Governing Body) 5
- Head and Senior Leadership Team (SLT) 5
- Designated Safeguarding Lead(s) (DSL) 5
- Director of Digital Learning 5
- Online Safety Group 5
- Director of Information Systems 5
- IT Systems Manager 5
- All Staff and Volunteers 5
- Students 5
- Parents and Carers 6

Curriculum and Training 6

- Student Curriculum 6
- Educating Parents and Carers 6
- Staff Training 6

Technical Provision 6

- General 6
- Security 6
- Filtering 6
- Monitoring 6

Digital Platforms 7

- Health and Safety 7
- Visitor Access 7
- Software and Platforms 7
- Acceptable Use Agreements 7

Protecting Data 7

Mobile Technologies (including BYOD/BYOT) 7

- Mobile Phones and Smart Watches 8
- Devices for Learning 8
- Personal devices 8

Communications 8

Social Media 8
Photographs and Personal Details 9
School Website and Official Platforms 9
Responding to Online safety Incidents 9
Reporting Online safety Incidents 9
Recording Online safety Incidents 9
Reviewing Online safety Incidents 9
Managing Online safety Incidents 9
Investigating Incidents 10
Investigating Incidents Involving Youth Produced Sexual Content (nudes and semi-nudes) 10
Searches for and of Electronic Devices 10
Confiscating an Electronic Device 12
Francis Holland Junior School 12
Photographs in the Junior School 12

Scope

This policy applies to all members of the Francis Holland School Regent's Park, Francis Holland Sloane Square and Francis Holland Junior School community (including staff, students, 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.

The Education and Inspections Act 2006 empowers Heads to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated safeguarding, behaviour and anti-bullying policies. Where known, the school will inform parents/carers of incidents of inappropriate online behaviour that take place out of school, except where to do so would not be in the best interests of the student.

Related Policies & Documents

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Information Systems Policy
- Data Protection Policy
- Student Acceptable Use Agreement
- Staff Acceptable Use Agreement
- Microsoft Surface Acceptable Use Agreement
- Digital Learning Device Policy

- Online Safety Procedures and Implementation[1]

Aims

The school aims to support the well-being and progress of each student 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, anti-Semitism, radicalisation and extremism
- **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, we 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

Roles and Responsibilities

Key People

	Sloane Square	Regent's Park	Junior School
DSL	Sarah Pittaway	Nick Gridelli	Suzy Dixon
Deputy DSLs	Clare Stansfield	Loretta Herrera	
Director of Digital Learning	Thomas Hayward	Maria Merrigan	

Everyone

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

[1] Maintained by the Online safety Lead, this document gives additional detail and context to the policy, as well setting out fuller procedures.

The School Council (Governing Body)

Council Members are responsible for the approval of the Online Safety policy and for reviewing the effectiveness of the policy. They receive regular updates on online safety. They will ensure that online safety is a running and interrelated theme while devising and implementing the school’s approach to safeguarding and related policies and procedures.

Head and Senior Leadership Team (SLT)

- Duty of care for ensuring the safety (including online) of members of the school community
- Aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- Oversee the staff acceptable use arrangements and take appropriate action over staff who breach them.

Designated Safeguarding Lead(s) (DSL)

- Overall responsibility for online safety issues and handling these according to the school’s Safeguarding and Child Protection, Behaviour and Anti-Bullying policies
- Ensure all staff receive appropriate training and advice on online safety matters and are aware of the procedures that need to be followed in the event of an online safety incident
- Lead an annual review of the school’s approach to online safety , the risks faced by the school community and oversee the implementation of any resulting recommendations.

Director of Digital Learning

- Lead staff training on online safety matters
- Promote awareness of online safety matters throughout the school community
- Oversee the online safety curriculum.

Online Safety Group

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

Director of Information Systems

- Responsible for trust-wide IT strategy.

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.

All Staff and Volunteers

- Be aware of online safety matters and the school’s policies and procedures
- Report online safety incidents according to the school’s policies
- Model responsible use of technology
- Supervise the use of technology during school activities onsite and offsite
- Deliver the online safety curriculum.

Students

- 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.

Parents and Carers

- Support their children in learning to use technology responsibly.

Curriculum and Training

Student Curriculum

Online safety should be addressed throughout the curriculum. Staff regularly reinforce online safety messages in academic lessons, tutor time and assemblies, and the school provides a varied and appropriate online safety curriculum which:

- is structured to ensure key topics are covered and revisited at various stages in a form appropriate to that age group
- is embedded in lessons and reinforced through tutor time activities and assemblies
- is reviewed regularly for relevance and effectiveness

Educating Parents and Carers

The school offers a range of relevant support to parents/carers to inform them of online safety issues and help them support their children's use of digital technologies.

Staff Training

All staff will receive appropriate online safety training, which will be regularly updated and reinforced. Records of staff training will be kept, and provision made for staff to receive specialist training. Governors should be aware of online safety issues and all Governors should receive appropriate training.

Technical Provision

General

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- Full details of technical measures are kept by the IT Systems Manager.

Security

- IT Systems Manager will ensure appropriate security measures are in place to protect the school's digital infrastructure from damage, loss of data and other risks.

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 above.
- There is a policy for blocking and unblocking sites.

	Sloane Square	Regent's Park	Junior School
Filtering	Sophos		
Monitoring	senso.cloud	senso.cloud	senso.cloud
Other	LibraESVA and Lightspeed		

Monitoring

- The school may monitor the use of its devices, systems, communication services and digital platforms.

- The school may monitor the use of other devices (i.e. those not owned by the school) using its systems with due regard to users' privacy.

Digital Platforms

- The IT Systems Manager and Director of Digital Learning will, to the best of their ability, keep records of the digital platforms used by the school. 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).
- 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.

Health and Safety

- Staff using IT equipment will mainly be covered by the provisions of the Display Screen Equipment (DSE, Health and Safety) Regulations 1992.

Visitor Access

- 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.

Software and Platforms

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

Acceptable Use Agreements

- Students and parents/carers co-sign the Student Acceptable Use Agreement at the start of each academic year. This agreement makes students aware that their use school platforms may be monitored. The acceptable use agreement is referred to throughout the school to ensure students are aware of its provisions and how it aims to protect them.
- Staff sign a Staff Acceptable Use Agreement and other agreements as relevant. This forms part of the contract of employment which outlines rules for them regarding online safety .

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.
- Students' 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-owned mobile and portable devices are encrypted.

Mobile Technologies (including BYOD/BYOT)

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

Mobile Phones and Smart Watches

- Rules will be published concerning appropriate use and regularly updated.

Devices for Learning

- Students 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.[2]
- The school sets appropriate rules for the use of devices at other times.
- The school may manage some features of learning devices.

Personal devices

- Students 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.
- Certain types of device are not permitted, which are listed in the procedures and implementation document.

Communications

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

- Digital communication between staff and students 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 students must not be made using personal email, social networks or messaging platforms. Students 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 student or a family friend.
- Staff should not email students 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 student 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.
  - Students should report to any member of staff, use the online safety email address (Sloane Square) or the anonymous reporting tool (‘Whisper’)
  - Staff should report to the DSL, IT Systems Manager or Director of Digital Learning

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 students

[2] Further rules are in posters and in the Student Acceptable Use Agreement.

- 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 student is related to or a family friend of a member of staff.

Photographs and Personal Details

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

School Website and Official Platforms

- The school may publish appropriate details about staff and students on its website and other official communications channels.

Responding to Online safety Incidents

- The school manages online safety incidents within the context of its safe-guarding and behaviour 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.
- The DSL will manage all online safety issues and incidents in line with the school’s child protection policy

Reporting Online safety Incidents

- Staff should report online safety incidents through the pastoral reporting system, ensuring that the Director of Digital Learning is copied in.

Students 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’)

Recording Online safety Incidents

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

Reviewing Online safety Incidents

- The DSL, Director of Digital Learning and relevant members of the pastoral 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.

Managing Online safety Incidents

- Once an online safety incident is reported, it will be assessed, and a response determined by the DSL and pastoral team in consultation with the Director of Digital Learning.

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, Anti-Bullying and Behaviour policies and with a view to the pastoral well-being of those involved.

Investigating Incidents

Investigating Incidents Involving Actual or Suspected Illegal Content

If there is any suspicion that any web site or device being investigated may contain child abuse images, or if there is any other suspected illegal activity, all the steps below must be followed.

- Report to the police and report under local safeguarding arrangements.
- Secure and preserve evidence.
- Report to the DSL.
- Await police response.

The school will work in accordance with the Safeguarding policy and the advice of the police and other relevant agencies when taking further action.

Staff must never:

- Investigate themselves
- View, copy, print, share, store or save such content– this is illegal.

Investigating Incidents Involving Youth Produced Sexual Content (nudes and semi-nudes)

Where a disclosure is made concerning youth-produced sexual imagery, the school will follow the safeguarding policy and other relevant guidance. Staff should take the following action:

- Secure and preserve evidence
- Report to the DSL

Staff must never:

- Investigate themselves
- View, copy, print, share, store or save, or ask a child to share or download such material – this is illegal.

Where a member of staff has been unable to avoid viewing images or video containing youth produced sexual content or child abuse (such as if a child shows the imagery before explaining its nature), they should report this to the DSL and seek support.

Searches for and of Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher, 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

The DSLs shall always be considered authorised members of staff in this regard. In the context of a school trip, the trip leader shall be considered an authorised member of staff in this regard.

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- 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 cooperation

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 Head, DSLs and other relevant members of the pastoral team 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 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 behaviour and safe-guarding policies

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

In the course of their duties, a member of staff may always ask a student to show them content on an electronic device. Where a student refuses, the device may be confiscated and the matter referred to the student’s head of year, who will decide on further actions with the pastoral team. Staff should not examine a device without consent or when the student is not present, except where the correct procedure is being followed for a search without consent.

Confiscating an Electronic Device

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 pastoral team or the school office at the first available opportunity.

Francis Holland Junior School

Particular care shall be given to ensuring the digital safety of the students in the Junior School. Where digital platforms are used, attention must be given to ensuring that the content and tools are age appropriate. This includes incidental online content such as advertising. Students in the Junior School should not be given unsupervised access to digital devices or platforms. Appropriate supervision will depend on the age of the students, the platforms used and the nature of the task.

Online safety is taught through the PSHE curriculum with a specific focus given to this in Online safety Week. Further guidance is given in the Online safety Procedures and Implementation Document.

Photographs in the Junior School

The EYFS iPad is used for taking photographs of the pupils, as well as for maintaining assessment records through the Teachermate EYFS Profiles software. EYFS staff do not take mobile phones into the classrooms.

Years 1 – 6 teachers have been provided with iPods, linked to a school iCloud account. These are used to take photographs of the pupils in lessons and on school trips. Junior School Microsoft surfaces can also be used for this purpose. Staff do not take photographs on personal devices.