FHS
Francis Holland Schools

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.

Policy owner	RP: Assistant Head Pastoral & Designated Safeguarding Lead SSq: Senior Deputy Head Pastoral Prep: Senior Deputy Head & Designated Safeguarding Lead
Type of policy	Statutory
Last reviewed / approved by / date	Safeguarding Sub-Committee – 31st January 2023
Next school review due	Autumn 2024
Next council review due	Spring 2025
This version published	29th August 2024
Circulation	☐ Trust Website ✓ Schools' Websites ✓ Schools' Sharepoints ☐ FHS People All policies are available from the Trust Office, Francis Holland Schools Trust, 35 Bourne Street, London, SW1W 8JA
Linked Policies	Safeguarding & Child Protection Policy Anti-Bullying Policy Data Protection Policy Student Acceptable Use Agreement Staff Acceptable Use Agreement Microsoft Surface Acceptable Use Agreement Digital Learning Device Policy

Revision History This section should be completed by the reviewer each time this policy is reviewed	
Changes made [Brief description of edits]	Date
Refers to online as opposed to digital safety	Spring 2024
Appendix added for Francis Holland Prep	August 2024

ONLINE SAFETY POLICY

SCOPE

This policy applies to all members of the Francis Holland Schools 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 regarding 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 Schools 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.

AIMS

The Schools aim 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, 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.

ROLES AND RESPONSIBILITIES

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	

EVERYONE

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

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.

HEADS AND SENIOR LEADERSHIP TEAMS (SLTs)

- 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 LEADS (DSLs)

- 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.

DIRECTORS 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 in the Aims section above.
- There is a procedurefor blocking and unblocking sites/YouTube videos which can be found in the appendix.

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

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 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.

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 register 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)

If the primary purpose for the use of 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 of access.

MOBILE PHONES AND SMART WATCHES

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

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;[1]
- 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 devices 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;

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

- 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 can report to any member of staff. In addition, provide a range of other reporting channels at the senior schools:
    - Sloane Square
        - Online safety email (digitalsafety@fhs-sw1.org.uk)
        - Whisper Anonymous Reporting
    - Regents' Park
        - Whisper Anonymous Reporting

- 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;
- 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 on social networks, messaging or other digital platforms.

SCHOOL WEBSITE AND OFFICIAL PLATFORMS

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

ONLINE SAFETY INCIDENTS

RESPONDING TO

- The Schools manage 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

- 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 will be logged by the DSL as part of the school's pastoral records.

REVIEWING

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

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

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.

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**.

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 ELECTRICAL 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:

- Assess 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 Schools' 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 PREP SCHOOL

Particular care shall be given to ensuring the digital safety of the students in the Prep 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 Prep 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 PREP 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. Prep School Microsoft surfaces can also be used for this purpose. Staff do/must not take photographs on personal devices.

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 students 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 students 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 students 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

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.

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.

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 you need to use your phone, please 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.

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.

Template mobile phone information for visitors:

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
- 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 3

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 you may wish your 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 lock their phones in Yondr pouches* 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 Students 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 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/students 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 you need to use your phone, please 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, 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.

Template mobile phone information for visitors.

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: 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 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.
- 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 iPad is used for taking photographs of the pupils, as well as for maintaining assessment records through the Tapestry EYFS Profiles software.