

# North London Collegiate School



Founded 1850

## DIGITAL SAFETY POLICY FOR PUPILS

Category / Review period	B / 1 year
Policy Lead	Deputy Head (Pastoral)
Reviewed By	Deputy Head (Pastoral), Head of Junior School & Director of Innovation
Review Completed	June 2025 (revised February 2026)
Authorised By	Deputy Head (Pastoral)
Date of Authorisation	June 2025
Date of Next Review	June 2026

### Contents

1.	Introduction.....	2
2.	Aims and objectives.....	3
3.	Statutory and regulatory framework.....	3
4.	Scope and responsibilities.....	3
5.	Risk management.....	4
6.	Pupils.....	5
7.	Inappropriate use by pupils.....	6
8.	Accidental use.....	6
9.	Deliberate misuse.....	6
10.	Parents and visitors.....	7
11.	All staff.....	7

12.	The use of technology.....	7
13.	Use of mobile electronic devices .....	8
14.	Video and photography.....	9
15.	Social media .....	10
16.	Curriculum and tools for learning.....	10
17.	Monitoring and review .....	11
Appendix 1 - Senior School Pupil Digital Safety Agreement & Guidelines for Use of 1:1 (iPad) devices .....		12
Appendix 2 - Lower School Pupil Digital Safety Agreement .....		14
Appendix 3 - First School Pupil Digital Safety Agreement .....		16

## **1. Introduction**

- 1.1 North London Collegiate School (the School) expects pupils to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour.
- 1.2 The Digital Safety Policy for Pupils sets out the roles, responsibilities and procedures for the acceptable, safe, and responsible use of all digital and electronic communication technologies. This includes the use of School based devices as well as personal mobile devices, digital content on the internet, collaboration tools such as email and instant messaging, as well as other social networking platforms and technologies.
- 1.3 The relevant Digital Safety Agreement will be circulated to parents and pupils prior to the start of every academic year for pupils and parents to read, sign and return to the School.
- 1.4 This policy should be read in conjunction with the following which are available on the School website:
- Anti-bullying Strategy
  - Behaviour Policy
  - Data Protection Policy
  - PSHE Policy
  - Privacy Notices
  - Safeguarding & Child Protection Policy
  - Terms & Conditions
  - Use of Pupils' Images and Names Policy
- 1.5 This policy applies to the whole School from Early Years Foundation Stage (EYFS) to sixth form.

1.6 This policy is available on the School website.

1.7 Copies of the above are held at the Senior School Office for consultation by parents. You may also email the School at [Office@nlcs.org.uk](mailto:Office@nlcs.org.uk) to request hard copies which can be made available in large print or other accessible format if required.

## **2. Aims and objectives**

2.1 The aims and objectives of this policy are to:

- ensure the safeguarding of all pupils within the School by detailing appropriate and acceptable use of all online and digital technologies
- help pupils take responsibility for their own Digital Safety, and to help staff guide and teach them appropriately
- ensure that pupils use technology safely and securely and are aware of both external, and peer to peer risks when using technology
- outline the roles and responsibilities of all pupils, staff and parents
- ensure all pupils and parents are clear about procedures for misuse of any online technologies
- develop links with parents and the wider School community to ensure continued awareness of online technologies
- encourage pupils to make safe, secure and effective use of technology
- minimise the risk of harm to the assets and reputation of the pupils and / or the School

## **3. Statutory and regulatory framework**

3.1 This policy complies with the following:

- [The Education \(Independent School Standards\) Regulations \(2014\)](#)
- The latest version of Keeping Children Safe in Education

## **4. Scope and responsibilities**

4.1 This policy relates to safety and the acceptable use of the following technologies, both inside and outside of the School, whether on School devices or on devices which are privately owned by pupils and/or parents.

- Collaboration platforms including the internet, email, and Virtual Learning Environments
- Fixed desktops, laptops, mobile devices and tablets
- Instant messaging and presence awareness and all other social networking platforms (including but not limited to WhatsApp, TikTok, Snapchat, Facebook, Instagram, LinkedIn, Twitter and other technologies which enable the sharing of information, images, and conversation)

- Mobile phones and smartphones/watches, and apps including games
  - Cameras, webcams, and other photographic and video equipment
- 4.2 Parents are encouraged to read this policy with their child and discuss the topics and implications it addresses in an age appropriate way. Parents are encouraged to attend any digital safety talks held at the School.
- 4.3 The Governing Body has overall responsibility for the safeguarding procedures within the School, the day to day responsibilities for which are delegated to the Head. The Designated Safeguarding Governor takes leadership of the School's safeguarding arrangements, including the School's online safety procedures, on behalf of the Governing Body, including an annual review of the procedures.
- 4.4 The Head has overall responsibility for the safety and welfare of members of the School community. The Head delegates day to day responsibility for the online safety of pupils to the Designated Safeguarding Lead (DSL) as the person with responsibility for safeguarding and child protection throughout the whole School.
- 4.5 The Deputy Head (Pastoral) and the Head of the Junior School are responsible for the implementation and annual review of this policy and will review the record of Digital Safety incidents and new technologies where appropriate, to consider whether existing security and Digital Safety practices and procedures are adequate.
- 4.6 The Director of IT is responsible for the operation of the security of the School's systems, including the filtering system to ensure that pupils are unable to access any material online that poses a safeguarding risk, including terrorist and extremist material, while using the School network.

## **5. Risk management**

- 5.1 Whilst the School endeavours to safeguard and mitigate against all risks with regards to Digital Safety, it will never be able to eliminate them all. Any incidents that come to our notice will be dealt with quickly and appropriately, according to this policy, to ensure the School continues to protect pupils.
- 5.2 To safeguard and promote the welfare of pupils both inside and outside of the School, it is important to anticipate and prevent the risks arising from:
- Inappropriate contact from users online, including strangers
  - Cyber-bullying and similar forms of online abuse or harassment
  - Illegal activities of downloading or copying of copyright materials and file-sharing via the internet or mobile devices
  - Issues with inappropriate email
  - Exposure to inappropriate online content and material

- The sharing of personal data, including images and the use of social media
- 5.3 Pupils should be mindful of their use of social media platforms and the digital footprints created.

## **6. Pupils**

6.1 Pupils are responsible for their actions, conduct and behaviour on the internet and with technology. Their use of technology should be safe, secure, responsible and legal. If a pupil is aware of misuse by other pupils they should talk to a teacher or member of staff about it as soon as possible.

6.2 In lessons and during School related activities, pupils will use School devices to access content and resources. All pupils will receive guidance on the use of the School's internet and digital systems.

6.3 Our pupils:

- are responsible for following the Digital Safety Agreement whilst within School and at home, as agreed each academic year or whenever a new pupil starts at the School for the first time, and are required to sign that they have read and understood this policy. Pupils are asked to review the Digital Safety Agreement annually with their form tutor.
- are taught about Digital Safety in a safe, responsible and age – appropriate manner
- should immediately tell an adult about any inappropriate materials or contact from someone they do not know
- are reminded that the consensual and non-consensual sharing of nude and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery), is strictly prohibited by the School and may constitute a criminal offence
- are made aware of the potential use of online digital technologies
- are taught and encouraged to consider the implications for misusing the internet and, for example, posting inappropriate materials to websites or on social media applications
- are taught that the downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose', and be copyright free
- are taught that sending malicious or hurtful messages, either inside School or outside of School can become a matter whereby the School may set sanctions or involve outside agencies such as the police
- are taught not to put themselves at risk online and taught what to do if they are concerned they have put themselves at risk
- are taught what to do if they are concerned that other children are at risk
- are given explicit guidelines and procedures for using mobile phones and other personal

devices in School and are expected to abide by this policy

- 6.4 The School reserves the right to monitor the use of the digital communications and technology in the School, including the use of the internet, email and social media. Pupils should remember that even when an email or something that has been downloaded, has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private. If a pupil is unsure about whether they are doing the right thing, they must seek assistance from a member of staff.
- 6.5 If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures as set out in the School's Safeguarding & Child Protection Policy. If a pupil is worried about something that they have seen on the internet, they should talk to a teacher or member of staff about it as soon as possible.
- 6.6 In a case where the pupil is considered to be vulnerable to radicalisation as a result of their on-line activity they will be referred to the Channel programme, this should be in consultation with the DSL.

## **7. Inappropriate use by pupils**

- 7.1 Where a pupil breaches any of the rules, practices or procedures set out in this policy, the Head will apply sanctions that are appropriate and proportionate to the breach including, in the most serious cases, in line with the School's Behaviour Policy.
- 7.2 Unacceptable use of electronic equipment or the discovery of inappropriate data or files on School devices, or inappropriate posts online, could lead to confiscation of any relevant School device or deletion of the material in accordance with the practices and procedures in this policy and the School's Behaviour Policy.

## **8. Accidental use**

- 8.1 If a pupil accidentally accesses inappropriate materials, the pupil is expected to take action to minimise the screen or close the window and immediately report this to an appropriate member of staff. All Digital Safety incidents should be reported to the Deputy Head (Pastoral) or the Head of the Junior School, and will be recorded in the appropriate way.

## **9. Deliberate misuse**

- 9.1 Should a pupil be found to deliberately misuse digital or online facilities whilst at School, appropriate actions will be taken. Please refer to the School's Behaviour Policy for further details. Deliberate abuse or damage of School equipment will result in parents being informed, and where appropriate, billed for the replacement costs of the equipment.
- 9.2 Should a pupil use the internet - whilst not in School time and/or not on the School premises, whether on a School or personal device, in such a way as to cause hurt or harm to a member of the School community, the School will act quickly and in accordance with its Behaviour Policy.

## **10. Parents and visitors**

- 10.1 All parents have access to a copy of this policy on the School website. Parents are asked to explain and discuss the policy with their child, where appropriate, so that they are clearly understood and accepted.
- 10.2 As part of the approach to developing Digital Safety awareness with pupils, the School may offer parents the opportunity to find out more about how they can support the School to keep their child safe whilst using online technologies beyond School; this may be by offering parent education talks or by providing advice and links to useful websites. The School wishes to promote a positive attitude to using the internet and digital and social technologies, and therefore asks parents to support their child's learning and understanding of how to use online technologies safely and responsibly. In line with this, parents are encouraged to use their own filtering and monitoring technology at home.

## **11. All staff**

- 11.1 Digital Safety is the responsibility of every member of the School community. All staff at the School have a responsibility to promote, observe, and respond to events surrounding Digital Safety. Staff are encouraged to act as good role models in their use of technologies, the internet and mobile electronic devices, and report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding & Child Protection Policy and procedures.

## **12. The use of technology**

- 12.1 The School will do all it reasonably can to limit exposure to the above risks when using the School's network. This is achieved by putting safety and security at the heart of the IT strategy and embedding it by default in the design of all systems. The School secures inbound and outbound traffic, has in place filtering systems to safeguard pupils from potentially harmful and inappropriate material online, and scans all incoming email. The filtering can be configured such that pupils in the Junior School will receive different filtering rules than those in the Senior School.
- 12.2 Secure Wi-Fi access is provided in and around the School grounds. Pupils must connect to the internet whilst on premises owned by the School using the 'Student' wireless network.
- 12.3 Visitors to the School are expected to connect to the School's wireless network and will be issued with an account and code personal to them by reception staff.
- 12.4 The School is aware that many pupils have unlimited and unrestricted access to the internet via mobile phone networks (i.e., 3G, 4G and 5G), and that this access means some pupils may use this technology inappropriately to bully or harass other pupils, or to view or share inappropriate material, whilst at School. Pupils must connect to the School's wireless network whilst on the premises, and abide by the School's Behaviour Policy and Anti-bullying Strategy.
- 12.5 The School provides accounts and email addresses for all pupils to promote safe and efficient

communication inside and outside of the School. Office 365 is the School's main collaboration platform, and all staff and pupils use Teams for sharing information and communicating. Pupils in the Junior School are taught about internet and email access and begin to use these accounts from Year 2 onwards, before which they may use a generic account to log in with.

### **13. Use of mobile electronic devices**

- 13.1 The School operates a mobile phone-free approach throughout the school day, including lessons, movement between lessons, breaktimes and lunchtime. Pupils in Reception to Year 11 must not access or use mobile phones or smart devices at any point during the school day unless explicitly authorised by a member of staff for a specific and supervised purpose.
- 13.2 "Mobile electronic device" includes without limitation mobile phones, smartphones / watches, tablets, laptops, including those which have been issued by the School to pupils. Pupils are permitted to bring in their own mobile electronic devices for use in the School, as long as they are connected to the School wireless network.
- 13.3 Mobile electronic devices must be placed on silent.
- 13.4 In the Junior School all mobile phones must be handed in to the form teacher at the start of each day.
- 13.5 Pupils in Years 7 to 11 (inclusive) must lock their mobile phones in their Yondr pouches for the duration of the school day and must not bring other smart devices with similar functionality (including smart watches) into school. It is the responsibility of all pupils to put their phone into the pouch on arrival at school. Unlocking stations are at school entrance and exits for use only at the end of the school day. Spot checks will be carried out at regular intervals. Any pupil found with their mobile phone during the day will have it confiscated and returned at the end of the school day. Pupils in Years 7 to 11 (inclusive) may not switch on or use their mobile phones during any part of the school day without the permission of a member of staff. Pupils in the Sixth Form must keep their mobile phones out of sight and must not use them in public areas. Limited mobile phone access for Sixth Form pupils reflects their increased independence and is carefully managed so as not to undermine the School's whole-school mobile phone-free approach. Mobile phone use by Sixth Form pupils must not be visible to younger pupils, remains prohibited in all teaching and public areas, and any misuse will be subject to sanctions in line with this policy and the Behaviour Policy.
- 13.6 Any student in Year 7-11 not using their Yondr pouch will be issued with a flag. Any Sixth Form student seen using their phone outside of the Sixth Form Common Room will be issued with a flag. Two flags in Year 7-11 will result in contact home and the student to bring her phone to the Deputy Head Pastoral's Office for 5 school days. Three flags will result in Sixth Form students being required to use a Yondr pouch for a period of 2 weeks and contact with home.
- 13.7 Students in Year 7 and below (inclusive) are not permitted to bring smart phones to school or travel to school with a smart phone. Students in Year 7 may bring a brick phone to school and put their phone into their Yondr pouch. Any Junior School student bringing a smart phone to school should hand it into the Junior School Office staff.

- 13.8 Students needing a replacement Yondr pouch should email [mypass@nlcs.org.uk](mailto:mypass@nlcs.org.uk) and collect their new pouch from the Transport Office at an agreed time. Replacement pouches are £20 and can be paid for via Evolve. Faulty pouches will be replaced free of charge.
- 13.9 Pupils may not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed with the Head and the Examinations Office.
- 13.10 Use of electronic devices and/ or digital technology of any kind, including but not limited to mobile phones and other smart devices with similar functionality (including smart watches), to abuse, bully, harass or upset or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- 13.11 The School reserves the right to confiscate and search, in appropriate circumstances, a pupil's mobile phone, mobile electronic device, and other smart devices with similar functionality (including smart watches) for a specified period of time if the pupil is reasonably suspected or found to be in breach of these rules. The pupil may also be prevented from bringing a mobile electronic device into the School temporarily or permanently.
- 13.12 The School is supported by Department for Education guidance to confiscate mobile phones and smart devices as a proportionate sanction. Staff acting lawfully and reasonably are protected from liability for loss or damage to confiscated items.
- 13.13 The School recognises that some pupils may require access to a mobile phone or smart device for disability-related needs, medical conditions, or other individual circumstances. Any such access will be agreed in advance, be purpose-specific, time-limited and supervised, and will not constitute a blanket exemption from the School's mobile phone-free policy. Where appropriate students in Year 7-11 will be issued with a Velcro Yondr pouch. These arrangements will be reviewed regularly.
- 13.14 The School will determine clear expectations regarding the use of mobile phones and other smart devices on educational visits, trips and residential. Depending on the nature and purpose of the activity, mobile phone use may be restricted or prohibited entirely. Students in Year 7-11 should take their Yondr pouch on all trips and will be advised by staff when it should be operational. Any permitted use will be clearly communicated to pupils and parents in advance and will reflect safeguarding, welfare and behavioural considerations.
- 13.15 Parents and carers should contact the School Office as the primary point of contact during the school day. Pupils should not use mobile phones or smart devices to communicate directly with parents during the school day, except where explicitly authorised by a member of staff for safeguarding or welfare reasons.

#### **14. Video and photography**

- 14.1 The School adheres to the UK General Data Protection Regulation and understands that an image or video is considered personal data. The School's Use of Pupils' Images and Names Policy, Parent and Pupils' privacy notices explains how and why the School collects photographs

and videos and what the School does with this type of personal data. Parents may choose to opt out of having their image used by the School at any time, by informing the School's Marketing team in writing. Any use of information before consent is withdrawn remains valid.

- 14.2 Parents are asked to be considerate when taking videos or photographs at School events and are requested not to publish materials such as images or recordings of other children in any public forum, or to 'tag' children from other families in images already published, without the permission of the relevant family. It is illegal to sell or distribute recordings from events without permission.
- 14.3 Using photographic material of any kind to abuse, bully, harass or upset or intimidate others will not be tolerated and will constitute a serious breach of discipline.

## **15. Social media**

- 15.1 Social media is a broad term for any kind of online platform which enables people to directly interact with each other. The School recognises the numerous benefits and opportunities which social media offers. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. The School encourages the safe and responsible use of social media by its staff, parents, and pupils. It must be noted that in most cases, children under the age of 13 are not permitted to create or use personal social media accounts.

## **16. Curriculum and tools for learning**

- 16.1 The School teaches pupils how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning through PSHE lessons and form time discussions. The following concepts, skills and competencies are taught through the School in an age-appropriate manner:
- Digital citizenship
  - Future work skills
  - Internet literacy
  - Making good judgments about websites and emails received
  - Knowledge of risks such as viruses, and opening mail from a stranger
  - Access to resources that outline how to be safe and responsible when using any online technologies
  - Knowledge of copyright and plagiarism issues
  - File-sharing and downloading illegal content
  - Uploading information – knowing what is safe to upload, and not to upload personal information

- Where to go for advice and how to report abuse

16.2 These skills are taught explicitly within the curriculum throughout a range of subjects. Pupils are taught skills to explore how online technologies can be used effectively, in a safe and responsible manner. Further details about the content of the curriculum related to IT can be found in the IT and PHSE curriculum documentation.

## **17. Monitoring and review**

17.1 The Head and Senior Team will regularly monitor and evaluate the effectiveness of this policy.

17.2 This policy will be subject to review by the Deputy Head (Pastoral), Head of Junior School and the Director of IT at least annually (or more frequently if changes to legislation, regulation or statutory guidance require).

17.3 This policy will be subject to review by the relevant committee of the Governing Body every year.

17.4 Consideration of the efficiency of the School's Digital Safety procedures will be included in the Governors' annual review of safeguarding.

17.5 The date of the next review is shown on the front page.

## **Appendix 1 - Senior School Pupil Digital Safety Agreement & Guidelines for Use of 1:1 (iPad) devices**

This agreement sets out the responsibilities associated with using a 1-to-1 iPad device, which is loaned to pupils by North London Collegiate School. It includes expectations around care, usage, and online behaviour. It should be read alongside the school's full **Digital Safety Policy for Pupils**.

By providing consent on SchoolBase, pupils and their parent(s) confirm that they have read and understood the following terms and agree to abide by them at all times.

---

### **School's approach to electronic devices**

- Students in Year 7-11 should not bring in any electronic device into school for academic purposes, for example their own iPad or laptop.
  - Full details about the School's approach to electronic devices can be found within the School's Safeguarding and Child Protection Policy on our [website](#).
- 

### **Care, Responsibility and Damage/Loss**

- The pupil is responsible for the iPad and accessories (keyboard case, charger) at all times, whether at school, at home, or in transit.
- Any damage, loss or theft must be reported immediately to the pupil's guardians and Head of Section.
- The school may require payment for any repair or replacement. Current costs (subject to change) are:
  - Apple iPad 10.2 – £279.60
  - Logitech Rugged Combo 3 Case – £79.20
  - Charger & Cable – £38.00
- Parents are advised to check whether the device is covered by their personal insurance. Leaving the device unattended or unsecured (e.g., in a vehicle) may invalidate claims.
- The school is not liable for costs associated with home use, such as electricity, internet, or subscriptions.

### **Care Expectations:**

- Keep the iPad in a secure location when not in use.
  - Use the device on a hard, flat surface.
  - Do not eat or drink near the iPad.
  - Keep the iPad clean and free from decorations or stickers.
  - Do not tamper with serial numbers or identification labels.
- 

### **Acceptable Use**

- The iPad is for **educational use only** and must not be loaned to others.
- Pupils must ensure the device is **fully charged each evening**.
- Only school-approved apps may be installed or used.

- **Social media use** is not permitted on school iPads.
- Usage is restricted to **teacher direction and designated homework areas** during lunch.
- The iPad must **not be used while travelling to or from school** and should be safely stored in a bag.
- Photos/videos may only be taken **with staff instruction and approval**, and the camera sound must remain on.
- iPads may be inspected by staff at any time and remain the property of the school.

---

### **Responsible Behaviour & Online Safety**

Pupils must uphold the highest standards of behaviour online. This includes:

- Never using technology or social media to harass, upset, or intimidate others.
- Not posting offensive, discriminatory, or inappropriate content.
- Not engaging in behaviour that might damage the school's or individuals' reputations.
- Never using the school's logo or branding without permission.
- Not plagiarising material from the internet or sharing platforms.
- Only sharing photos/videos of others with their permission.
- Not sharing personal details (their own or others') online.
- Respecting the privacy of others and using social media responsibly.
- Ensuring social media privacy settings are correctly applied.
- Reporting and blocking any offensive messages received.
- Never contacting staff via personal emails, phone numbers, or social networks.

---

### **Confirmation and Consent**

Parents and pupils confirm their understanding and agreement by completing the consent form on SchoolBase:

**Parent Portal → Pupil Details → Other Consents → iPad Agreement → Consent Given**

## **Appendix 2 - Lower School Pupil Digital Safety Agreement**

These rules will keep me safe and help me to be fair to others when using technology at School.

### **Using the School's IT resources:**

- I will only use the School's technology for schoolwork and homework
- I will use school-approved communication tools e.g. Teams, responsibly and for educational purposes only
- I will take care when handling the School's technology equipment, including mobile devices such as iPads and laptops
- I will not bring files into School without permission or upload inappropriate material to the network

### **Responsible behaviour:**

- I will only edit or delete my own files and not look at or change other people's files without their permission
- I will not share my personal login details with anyone, and I will not use another person's login details.
- I will only visit Internet sites that are appropriate for School work
- The messages I send, or information I upload, will always be polite and sensible
- I will respect copyright rules and give credit to work that is not my own
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it
- I will not take or publish a photograph, video or audio of anyone without receiving their permission first
- I am aware that social media has age restrictions and I should not have accounts on any site or app that I am not old enough for
- I will not use digital technology to exclude other people or talk negatively about them, or in any way which might cause upset, hurt or embarrassment
- I will report any instances of cyberbullying or online harassment immediately to a trusted adult
- I understand that what I publish online might be available to be read by many more people than originally intended and/or that I lose control of information and images as soon as they are published

### **Using my own device in School**

- I will only bring a phone to school if I travel on the coach or have permission to walk.
- If I have permission to bring a phone to school, I will hand it to my form teacher each morning and collect it at the end of the day
- I will not use a mobile phone during the School day
- I understand that having personal devices in School is at my own risk

**Online safety:**

- I will not give my home address, telephone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission
- I will only connect with people I know, or a responsible adult has approved
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it and I will show a teacher/responsible adult

I understand the Digital Safety Agreement for using the internet, email and online tools safely and responsibly.

I am aware that the adults working with me at School will check that I am using technology appropriately.

I understand that my parents or guardians may be informed of my digital activities at School if necessary.

I understand that if I do not follow these rules, there will be consequences according to the School's behaviour policy.

Please complete the form [here](#) to confirm you have read and discussed the digital safety agreement with your child.

### Appendix 3 - First School Pupil Digital Safety Agreement

- 1. I will always ask an adult before going online.**  
It's important to have permission so that I can use the internet safely.
- 2. I will only use apps and websites that are safe and suitable for my age.**  
If I'm not sure, I will ask an adult to check first.
- 3. I will keep my personal information private.**  
This means not sharing my full name, address, school, or phone number online.
- 4. I will be kind and respectful to my teachers, friends and family online.**  
Just like in real life, it's important to be kind online.
- 5. If I see something that makes me feel upset, scared, or confused, I will tell an adult straight away.**  
It's important to ask for help if something doesn't feel right.
- 6. I will only talk to people I know in real life when I'm online.**  
If someone I don't know tries to talk to me, I will let an adult know.
- 7. I will look after the devices I use and use them carefully.**  
I will make sure they are kept safe and used properly.

Please complete the form [here](#) to confirm you have read and discussed the digital safety agreement with your child.