FIRST BRIDGE SCHOOL

Online safety, mobile use and AI policy

Introduction

The aim of this policy is to outline First Bridge School's safe and effective practice use of the internet, as well as general use of cameras, tablets and computers. The policy pays contextual regard to the latest 'Keeping Children Safe in Education' (September 2025) statutory safeguarding guidance, and the DfE's 'Teaching online safety in schools' guidance (January 2023). It complements the school's safeguarding policy, whistleblowing policy, data protection policy and anti-bullying policy.

First Bridge School's approach to using technology, the internet, and AI

We work with primary aged pupils with complex SEND on a predominantly 1:1 model. This context dictates how we use technology and the internet, and therefore how we interpret and apply the latest safeguarding guidance for schools.

- Use of all technology, predominantly iPads/tablets, are only used when pupils are supervised in person, and only for use of approved applications:
    - Youtube kids
    - Writing wizard
    - Proloquo2go
    - Fruit Ninjas
    - Lucas and friend's app
    - BBC CBeebies app
    - Khan Academy Kids app
    - Famly app
    - HiRasmus

- All devices, including laptops and computers, are stored securely when not in use, within classrooms.

- Staff check any applications/content which the pupils will view, before sharing it with pupils.

- The DNS filtering and monitoring system ensures that any inappropriate content is blocked and activity is monitored. DNS operates on both the schools wifi system and is installed on all school devices. Alerts go directly to the headteacher, who is also the Designated Safeguarding Lead (DSL). However, in the unlikely event

that any staff member should discover any potentially unsafe or inappropriate material, they must immediately remove the content from the pupil's view. All such incidents must be reported to the DSL.

- No school devices are ever used for personal use by staff.

- We teach, wherever possible and age-appropriately, pupils to understand online safety and explain about how and why we use the internet. This is part of the PSHEE curriculum.

- Staff are aware of the need to limit the time pupils spend on devices and develop strategies to ensure that they spend a balance of time engaged in this and other activities.

- Staff use the school's digital cameras and tablets (only; personal devices are never used) to record pupils' learning and achievements. Tablets are password-protected with a pin and stored securely overnight. Photographs and videos are deleted securely once uploaded to the relevant application and/or are no longer required.

- Standard tablets may be used only in open bathroom areas (e.g., handwashing areas) to support toileting independence.

- Pupils who use tablets for communication may keep their devices inside toilet cubicles.

- Communication devices are held by the pupil or stored in the therapist's tote bag — never held by staff.

- If reinforcement is needed inside cubicles, staff use an alternative device with the camera permanently disabled/off. These devices are used only to deliver visual, auditory, or interactive reinforcers during toilet learning.

- Photographs are never taken of pupils in nappies, when asleep or when inappropriately dressed.

- Any photographs or videos taken by staff, other adults (including parents), and the pupils themselves during ANY school activity (including outings and events) are not put on public display or

published anywhere on the internet or social media, unless specific consent is received from the adults and parents of the pupils involved.

- The computer systems, all devices and all data (including for e.g. voicemails, emails and all information transmitted) are the property of First Bridge School and are provided for business purposes only; all information stored on these systems remains the property of First Bridge School.

- To prevent computer viruses from being transmitted there must be no downloading of unauthorised software. Staff must be very careful when opening email attachments; it is safer to delete the email without opening it than if in doubt call the sender and confirm whether the attachment was intended. Use of 'memory sticks' is not permitted.

- All internet activity and history are monitored and can be reviewed by the school's leadership team.

- Staff may use Artificial Intelligence (AI) such as Co-Pilot or ChatGPT to, for example, plan learning activities, but never input personal details of pupils or colleagues of any type, such as reports and images. No data that could identify First Bridge School, its pupils or staff, should ever be uploaded to AI platforms.

- Mobile devices, including phones, are not used by pupil-facing staff, parents or visitors during working hours wherever pupils are present. Mobile phones must be locked in the school's phone lockers during pupil-facing hours.

- During outings, senior members of staff ONLY keep their personal phones with them in case of emergencies.

- Any breaches of this policy are subject to the school's disciplinary procedure.

Appendix 1: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels to share information about the school: • Our official Facebook, Instagram and LinkedIn profiles • Official website and blogs • We use the FAMLY portal as well as email to communicate with parents/carers Parents/carers are free to set up independent groups (e.g. WhatsApp) to communicate with each other, however First Bridge School will not be monitoring these groups. First Bridge School requires that these groups are respectful and factual to all the parties involved and discussed in such groups.	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way. • Use private groups or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident. • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers.	
Signed:	**Date:**

Appendix 2: Acceptable use agreement for staff

Acceptable use of the school's ICT facilities and the internet: agreement for staff	
Name of staff member:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote any private business, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed:	**Date:**