Falkner House School Internet Policy and Procedures

Available for parents to access on the school website and on request. Nursery - Year 6 including EYFS

1. Policy Statement

This policy has regard to the following guidance and advice: KCSIE (2026), DfE Health and Safety: responsibilities and duties for schools (2022), Cyberbullying: Advice for Headteachers and School Staff (2014) , Advice for Parents and Carers on Cyberbullying (2014), Meeting Digital and Technology Standards in Schools and Colleges (2025), Cyber security standards for schools and colleges (2025), Mobile phones in schools (DfE, statutory guidance under section 550C of the Education Act 1996, from 29 June 2026).

Please also see the following Falkner House Policies: Child Protection and Safeguarding (for the definition of Child on Child abuse (including bullying and cyber bullying), Behaviour, PSHE and RSE Policies and syllabus, Pupil iPad policy and Procedures, Staff Code of Conduct, Date Protection

2. Aims

It is the duty of Falkner House to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation.

This policy, supported by the policies set out above, is implemented to protect the interests and safety of the whole school community (staff and pupils alike). It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. The school recognises that technology, and risks and harms related to it, evolve, and change rapidly. As such, our approach to online safety is regularly reviewed by the computing team and as a minimum this occurs on an annual basis.

3. Roles and responsibilities

The School's Head of IT is responsible for day-to-day internet, technology and IT security including cyber security at school (as part of the school's wider safeguarding strategy, with reference to Cyber security standards for schools and colleges (2025)) following the protocols agreed with the headteacher, set out below and the Falkner House Safeguarding and Child Protection policy. The Head of IT would refer any concerns to the Headteacher and/or to the DSL depending on the circumstances.

As with all issues of safety at Falkner House, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

4. Filtering and Monitoring

Filtering and monitoring systems are designed to safeguard pupils and staff online, including in relation to harmful, inappropriate or unsafe content, suspicious searching, concerning online behaviour, and risks arising from emerging technologies including Generative AI. It is essential that pupils are safeguarded from potentially harmful and inappropriate online material. As part of this process the school has appropriate filtering and monitoring systems in place and regularly reviews their effectiveness (at least annually, with documented checks). The school fully complies with the Department for Education's published filtering and monitoring standards which set out that schools should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems,
- review filtering and monitoring provision at least annually,
- block harmful and inappropriate content without unreasonably impacting teaching and learning,
- have effective monitoring strategies in place that meet their safeguarding needs.

The school is also aware of the Department for Education's 'plan technology for your school service' and will use this as necessary to self-assess against the filtering and monitoring standards and receive personalised recommendations on how to meet them.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:
content: being exposed to illegal, inappropriate, or harmful content, including: pornography, fake news, misinformation, disinformation, conspiracy theories, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer 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: online behaviour that increases the likelihood of, or causes, harm; for example, 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.
commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we felt that our pupils, students or staff were at risk, we would report it to the Anti-Phishing Working Group (https://apwg.org/).

4.1 Personal devices and mobile data:

The School's filtering and monitoring applies to School devices and the School network. Phones and smart watches that use their own mobile data (3G, 4G or 5G) are not covered by it. This is one reason pupils may not have personal devices in school. Staff who see a pupil using a personal device on site must remove it under the Behaviour Policy and report any online-safety concern to the DSL.

4.2 Roles and responsibilities for filtering and monitoring at the School:

- The LLP Board has overall strategic responsibility for filtering and monitoring. Marina Wood is the Board member responsible for ensuring the DfE Filtering and Monitoring Standards are met, and is involved in the annual review.
- The Head of IT is the member of the team responsible for filtering and monitoring. They are responsible for procuring systems, documenting decisions on what is blocked or allowed and why, overseeing reports, and leading the review of the school's filtering and monitoring provision at least once every academic year. The IT team has technical responsibility for maintaining the filtering and monitoring systems, providing reports, and completing actions following concerns or checks. They work with the Head of IT and the DSL to procure systems, identify risk, and carry out reviews and checks.
- The DSL has lead responsibility for safeguarding and online safety, including oversight of filtering and monitoring systems, reviewing safeguarding concerns identified through those systems, and ensuring that concerns are acted upon appropriately.
- The School network uses Lightspeed Cisco Umbrella and SmartShield DNS for web filtering and monitoring. Alerts go to the DSL and IT daily, the Office signs off a weekly report, and the Headteachers receive a monthly report.
- The Head of IT receives regular filtering and monitoring reports identifying attempts to access inappropriate or potentially harmful material and other flagged activity. These reports are reviewed promptly and any safeguarding concerns are referred to the DSL and/or Headteacher as appropriate. The DSL will determine what action, if any, is required in response to safeguarding concerns identified through filtering or monitoring systems.
- Staff are asked to report any concerns about a pupil's use of technology or online activity, whether in school or outside school where relevant safeguarding concerns arise, to the DSL in accordance with the School's safeguarding procedures.
- Filtering and monitoring systems and processes are reviewed regularly to ensure that they remain effective, proportionate and appropriate to the School's safeguarding needs.

5. Use of technology in the classroom and beyond: staff, pupils and visitors – permissions, restrictions and sanctions

Pupils:

- use MacBooks for computing lessons. Years 4, 5 and 6 use iPads. Ys 5&6 take the iPads home to complete homework
- are not allowed to have mobile phones, smart watches, smart glasses, e-readers or other personal devices with internet, camera, messaging or calling functions in school, at Early Birds, at clubs or on school trips. The School is phone-free throughout the school day. The full rule, including the exceptions for independent travel and medical needs, is in the Behaviour Policy.
- are only allowed to use the internet at school in the presence of a teacher and are instructed as to the websites that they can view
- are reminded of the need for internet security both in school and when out of school in both computing and in PSHE lessons (see PSHE policy, syllabus and schemes of work and computing policy and curriculum)

- those with school iPads have profiles restricting them from sending messages, emails, and accessing the app store. Use of the internet is limited to pre-approved "allowed" sites
- when using iPads are reminded in all lessons of the restrictions and rules they must follow when using iPads. These include:
    - Only using an iPad if a teacher or parent has given them permission.
    - Only using the iPads for educational purposes.
    - Not taking any photos on the iPad unless teachers give them permission.
    - Not changing any of the settings.
    - If pupils do not adhere to these rules their iPad is locked or removed for the day at the teachers' discretion.

Staff:

- use MacBooks and PC's, laptops are taken home if needed (see Staff code of conduct)
- are prohibited from cyber contact with pupils or former pupils aside from in a purely academic context e.g. homework (see Staff Code of Conduct)
- are aware that all internet usage via the school's systems and its wifi network is monitored

Visitors/Parents:

- are asked to put away any devices on school premises
- are not allowed access to the school wi-fi
- are only allowed to photograph their own children in concerts etc. and are requested not to upload any such photographs to social media

6. Artificial Intelligence (AI)

The School only permits the use of generative AI tools on the School's devices/systems in specific circumstances as referred to in the Safeguarding Policy and Staff Code of Conduct.

7. E-Safety in the Curriculum and School Community

IT and online resources are used across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

Pupils are taught in computing and PSHE lessons how best to protect themselves and their peers online (please see PSHE and computing Policy and Curriculum for more details).

7.1 Computing lessons include constant reminders to pupils that they should:

- Only access the internet in the presence of a teacher
- Only access only sites and material approved by their teacher and relevant to their work in school
- Log on to the school's computer network using their unique username and password (from Year 4) and will not allow any other pupil to use their username and password
- Log off at the end of each session.
- Not at any time log on to any internet chatroom or similar facility which may result in any personal details being disclosed or may identify them to persons unknown.

- Only send and receive emails, or open attachments under the supervision of a teacher
- Report any incidence of bad language or distasteful images to a teacher if they come across them accidentally.
- Be aware that unkind actions online – cyber bullying: posting photos, snide comments or meanness or bullying online is totally unacceptable and is subject to the Falkner House Behaviour Policy.

7.2 Communication with parents:

- Parents are invited to come in for annual in-house sessions on online safety led by the school's Head of IT. The notes and advice from these sessions are also available within the Parent Handbook.
- Parents are reminded each year that pupils may not bring phones or smart watches to school, and are given advice on safe use of these devices at home, including parental controls and supervision.
- There is a technical guide for parents available on the school's website.

7.3 Reporting Mechanisms available for all users to report issues and concerns and how they are managed and/or escalated:

- Any issues or concerns are reported as they arise directly to the school's Head of IT and the DSL, or the Headteacher. The Head of IT would refer any concerns to the Headteacher.
- Issues or concerns are dealt with and managed as they arise

8. Management of personal data in line with statutory requirements (please also see Data Protection policy)

- Falkner House uses Google Apps for Education to store data, to allow for fast, easy collaboration and for seamless compatibility between devices. The data centre network from Google Apps provides exceptional security and guarantees reliable access to our data. All data is automatically backed up onto Google servers https://edu.google.com/why-google/privacy-security/?modal_active=none
- Google Workspace is backed up automatically three times a day by Backupify (Kaseya). All data is hosted by iSAMS and is backed up every hour, every day of the year, with copies held both on and off site. Upper school pupils' work in Goodnotes is stored on Goodnotes Cloud and syncs automatically across the pupil's signed-in devices.
- The school database is stored in Azure https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data
- Access to the database is managed by iSAMS.
- Falkner House data is owned by Falkner House and is accessed by private logins and usernames.
- Pupils are only given access to their personal documents.

- Staff have access to the school's data both in school and out of school. Staff are all required to sign a data privacy form and understand the importance of keeping data private.

- Staff all have to sign the Falkner House Staff Code of Conduct on an annual basis.