FALKNER HOUSE SCHOOL INTERNET POLICY AND PROCEDURES Nursery – Year 6 (therefore includes EYFS) DCSF STANDARD 3 (2) c & d (drawn up with regard to DCSF 2011: Health and Safety DfE advice on Legal Duties and Powers for Local Authorities, Head Teachers and Governing Bodies)

Please also see the

- Falkner House Child Protection Safeguarding Policy for the definition of Peer on Peer abuse (including bullying and cyber bullying).
- Falkner House Behaviour Policy .
- PHSEE Policy and syllabus and schemes of work
- Pupil iPad policy and Procedures
- Staff code of conduct

INTERNET SECURITY

The online security of pupils, staff and visitors is of great importance.

Defined roles and responsibilities for online safety

- The school's head of computing is responsible for day-to-day internet, technology and IT security at school (as part of the school's wider safeguarding strategy) following the protocols agreed with the headteacher, set out below and the Falkner House Safeguarding and Child Protection policy. The head of Computing would refer any concerns to the Principal who is the Designated Safeguarding Lead (DSL)

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, 5&6 take the iPads home to complete homework.
- Pupils are not allowed to have their own personal mobile devices or Kindles (aside from their school iPads) in school or on school trips, unless for medical reasons.
- If a pupil is travelling to school independently and parents feel it is essential for their child to have a mobile phone, the parents must liaise with the school in advance. A mobile phone would have to be left in the school office for the day, as pupils are not allowed personal devices in school.
- Staff use MacBooks and PC's, laptops are taken home if needed (see Staff code of conduct).
- Pupils 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.
- Pupils are reminded of the need for internet security both in school and when out of school in both computing and in PHSEE lessons (see PHSEE policy, syllabus and schemes of wotk and computing policy and curriculum)
- Visitors are asked to put away any devices on school premises
- Visitors are not allowed access to the school wi-fi.
- Staff are prohibited from cyber contact with pupils or former pupils aside from in a purely academic context e.g. homework (see Staff Code of Behaviour).
- Pupil iPads have school profiles restricting pupils from sending messages, emails, accessing the app store and use of the internet is limited to preapproved sites.
- Pupils 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.

Technical structure and safeguards in place to filter and monitor inappropriate content and alert the school to safeguarding issues

- The school network uses Smoothwall for web filtering to ensure, to the best of our ability, that pupils and staff are protected from unsuitable sites. The head of computing and the bursars receive a weekly email alerting them to any attempts by pupils to access inappropriate content or any sites containing flagged content that were accessed by staff (the staff network has fewer restrictions). These reports are investigated and referred to the Principal (DSL) if relevant.
- If staff have concerns about a pupil's use of the internet or technology at home, this would be referred to the Principal (DSL)

How the school builds resilience and teaches pupils to protect themselves and their peers through education and information

- Pupils are taught in computing and PHSEE lessons (see PHSEE and computing Policy and Curriculum) how best to protect themselves and their peers online

  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 on line is totally unacceptable and is subject to the Falkner House Behaviour Policy.

Staff safeguarding professional development including online safety

- Staff sign a Falkner House Staff code of Conduct (includes use of IT) before starting work at Falkner House
- New staff are to the school induction programme
- Staff have safeguarding training at least every two years and have updates as regards online safety issues on a regular basis

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 directly to the school's head of Computing or the Principal. The head of Computing would refer any concerns to the Principal.
- Issues or concerns are dealt with and managed as they arise

How the school informs, communicates and educates parents / carers in online safety

- Parents are invited to come in for annual in-house sessions on online safety led by the school's head of Computing. The notes and advice from these sessions are also available within the Parent Handbook.
- There is a technical guide for parents available on the school's website.

Management of personal data in line with statutory requirements (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
- Falkner House also uses Backupify to backup data from Google Apps for Education. All the data is stored in an EU data centre https://www.backupify.com/blog/how-backupify-helps-support-gdpr-compliance
- 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 Scott Marketing.
- 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 on an annual basis the Falkner House Staff Code of Conduct