Ascot Heath Primary School

"Preparing our children for all of their tomorrows"

Online Safety Policy

Introduction

The internet is an essential element for education and social interaction. It opens doorways to a wealth of information, knowledge and educational resources, increasing opportunities for learning in and beyond the classroom. The school has a duty to provide pupils with quality internet access as part of their learning experience. Pupils need to be taught how to evaluate internet information and to take care of their own safety and security whilst online.

Aims

The primary aim of this policy is to ensure the safety, well-being and protection of our pupils and staff whilst online.

Teaching and Learning

The internet offers access to enrich and support activities. Internet usage is a part of the statutory curriculum and a necessary tool for staff and pupils and will enhance the learning experience.

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will take all reasonable steps to ensure that the use of internet derived materials by staff and pupils complies with copyright and any other applicable laws.
- Children will be taught about online safety each year. This covers how to keep information private, how to report unkind or upsetting behaviour and how to behave appropriately on the internet.

MANAGING INTERNET ACCESS

Information system security

- System security is managed by an external IT provider, TSI
- The school ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

E-mail

- There is no e-mail facility on the children's laptops, unless accessed via an internet browser.
- Children are taught how to send safe, appropriate emails through computing lessons.
- All email must be written in a professional manner.
- TSI have access to all emails if needed.

- The forwarding of chain letters is not permitted.
- Any direct communication, staff/parent will be via a school email address.
- A standard footer on school emails will be used stating content is private and confidential.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher and deputy will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Teachers are able to publish content on the website. All content must be professional and in line with the school's expectations.

Publishing pupil's images

- Photographs of the children will not be used on the school website or social media pages without signed parental permission. Children's names will not be included alongside any images.

Social networking and personal publishing

- Pupils and parents will be advised that the use of social network spaces outside school can expose them to hazards or risks. Such sites can offer entertaining and educational benefits but as they are effectively unregulated they can expose children to risks. Parents are advised that if they wish their child to use these sites they select together and the parent supervises the child's use.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- The school will block/filter access to social networking sites.
- The school uses Facebook as its social network site. Only photos of the backs of children are routinely used unless explicit permission has been granted from parents e.g. through signing permission on a school trip form or email agreement to a special event photo.

Managing filtering

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. This is managed by TSI.
- If staff or pupils discover an unsuitable site, it must be reported to the headteacher and TSI.
- TSI will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies-

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be advised to use the school phone where contact with a pupil's parent is required.
- Children in Year 5 and Year 6 are permitted to bring their phones in. These will be handed in to the office at the start of the day and can be collected again at home time. The pupils and parents sign a mobile phone code of conduct agreement at the start of the year.
- A mobile phone audit is conducted half termly by the DSL or the deputy DSL.

GDPR

- Personal data will be recorded, processed, transferred and made available.
- More information can be found in the GDPR policy.

POLICY DECISIONS

Authorising Internet access

- All staff must read and complete the Teams questionnaire to confirm they have read the 'Acceptable Usage Policy' before using any school ICT resource.
- All staff have access to the shared drive, internet and platforms, such as Teams. When a member of staff leaves their access is removed by TSI.
- Throughout the school access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor BFC can accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT provision to establish if the Online safety policy is adequate and that its implementation is effective.

Handling Online Safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher using the low level concern form or self declaration reporting form.
- Complaints of a child protection nature must be recorded on Safeguard my School.
- Pupils and parents will be informed of the complaints procedure.

Community use of the internet

- The school will liaise with local organisations to establish a common approach to Online safety.

COMMUNICATIONS POLICY

Introducing the Online safety policy to pupils

- Online safety rules will be taught through online safety lessons during each school year and through the class charter.
- Pupils and parents will be informed that network and internet use will be monitored.

Staff and the Online safety policy

- The Online safety policy is saved on the Safeguard training Teams page in the policies folder and is accessible to staff at all times.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Reports are shared with the DSL and any concerning use of the internet is flagged to the DSL immediately.

Enlisting parents' support

- Parents' attention will be drawn to the School Online safety policy and is available on the school website.
- Parents are encouraged to keep informed about the internet sites their children might visit.
- Parents are encouraged to talk to their child about their use of the internet and technology, this dialogue is the key to future safety.
- Families should be encouraged to have a computer "routine", whereby the parent supervises computer usage; the computer is located in a family room with the screen situated where it can be seen.

The Online safety policy relates to our Safeguarding, Computing, Anti-bullying and Acceptable Usage policies.

Document Management and Control

Initial Issue Date:	January 2021
Last reviewed / Revised: Date of Next Review:	September 2025 September 2026
Reviewed By:	Rachel Bradley
Agreed & Adopted By:	FGB September 2024

Amendments Made at Last Review:	**Added:** Reports are shared with the DSL and any concerning use of the internet is flagged to the DSL immediately to section 'Staff and the Online safety policy'