ASQUITH PRIMARY IT & E-SAFETY POLICY

Date Adopted:	27/11/2024
Review Date:	Autumn Term 2025

IT and E-Safety Policy

E-Safety Policy Overview

E-Safety includes internet technologies and electronic communications such as mobile phones and wireless technology. E-safety of Wynndale embraces educating children about the benefits and risks of using new technology, while also providing them with the skills and knowledge to become digital citizens of the 21st century. We want to enable the children to control their online experiences in a positive and safe way.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, GDPR & Data Protection and Safeguarding.

E-safety Policy

Our E-Safety Policy has been approved and read by all staff.

It has been agreed by the senior management team and approved by governors during the Autumn Term 2024. The E-Safety Policy will be reviewed annually by the ICT subject leader, senior members of staff and the governors.

Good Practice at Asquith

Here is our overview to e-safety at Asquith:

• Responsible ICT use by all staff and pupils; supported by the children's computing education and staff's knowledge and training if required.
• Implementation of e-safety policy in all areas of school by every child and every member of staff.
• Safe and secure broadband including the effective management of content filtering. This is provided by Infotechdirect.
• Any material that the school believes is illegal must be reported to Infotechdirect and recorded on CPOMS.

How does the use of the Internet benefit Asquith?

• It promotes pupil achievements through the website and on social media.
• It shows Pupils' progress in foundation through Tapestry.
• It enhances the school's administration system.
• It is used for the children to learn how to evaluate internet information.
• It gives access to world-wide educational resources.
• It gives access to experts in many fields for pupils and staff.
• It gives the children the chance to communicate with authors.
• It helps with professional development for staff as they get access to national developments, educational materials, and shared effective curriculum practice.
• It allows staff to track and monitor classes.
• It allows staff to track and evaluate children's ICT learning.
• It assists with teachers' submitting data
• It is used for safeguarding through CPOMS.
• It helps children know what Internet use is acceptable and what is not, both at school and at home.

How is the internet used in education at Asquith?

• Internet access will be carefully planned to enrich and extend learning activities through the use of laptops and iPads.

• Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.
• Pupils will leave Asquith as digital citizens ready to use technology in their everyday life.
• Children will follow the ICT curriculum to make sure they are getting a fulfilled and enriched computing experience.
• The children have access to educational apps such as, Spelling Shed and Timetable Rockstars.

Email

• Pupils may only use approved e-mail accounts on the school system.
• Pupils should know staff can see and monitor all emails on the school system.
• E-mails from staff that are sent to external organisations should be written carefully before sending and always from a school email address.
• The forwarding of chain letters is not permitted.
• Staff should not email to their personal accounts or send work to themselves over email. Staff can access documents and information on the server through their school laptop when at home.

Social Networking

• School should block/filter access to social networking sites unless a specific use is approved.
• Pupils will be advised never to give out personal details of any kind which may identify them or their location.
• Pupils should be advised not to place personal photos on any social network space.
• Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
• Pupils should know that images can be edited online and that not everything they see is a true reflection.
• Pupils should know that the information they put online can be traced back to them, even if it is deleted.

Filtering

• The school will work in partnership with Infotechdirect to ensure filtering systems are as effective as possible.
• Staff are aware that they need to report any unsafe sites to Infotechdirect and record them onto CPOMS.

Managing Emerging Technologies

• Emerging technologies will be examined for educational benefit before use by the ICT leader.
• The ICT leader will send out any useful emerging technologies that can be used in school. These will first be checked by the GDPR leader & Infotechdirect.
• A staff meeting will be held if there is a new technology to be used at school so all staff can access the content successfully.

Mobiles

• Mobile phones will not be used for personal use during school time by staff or children unless there is a safeguarding concern.
• The sending of abusive or inappropriate text messages is forbidden.

Published Content and the School Website

• The contact details on the Website should be the school address, email, and telephone number. Staff or pupils' personal information will not be published.
• The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

• Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name.
• Pupils' names will not be used anywhere on the internet.
• Parents sign consent form on entry to school detailing if/when children's images may be used/shared.

Infotechdirect

• School ICT system and security will be reviewed regularly by Infotechdirect.
• Virus protection is installed and updated by Infotechdirect.
• Security strategies and concerns will be discussed with Infotechdirect.
• Infotechdirect continue to manage the school filtering and monitoring requirements and ensure that the school has the filtering and monitoring requirements in place, in line with KCSiE 2024.

Personal Data

Personal data will be recorded, processed, transferred, and made available according to the GDPR & The Data Protection Act 1998.

Handling e-safety Complaints and Concerns

• Complaints of Internet misuse will be dealt with by a senior member of staff and needs to be recorded on CPOMS.
• Any complaint about staff misuse must be referred to the headteacher.
• Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and reported on CPOMS
• Parents wishing to complain about e-safety issues should use the established school complaints procedure.

Communication of Policy

• Rules and Guidance for Internet access will be posted in all networked rooms.
• Pupils will be informed that Internet use will be monitored.
• All staff will be informed about and given access to the school e-Safety Policy.
• Staff should be aware that Internet traffic can be monitored and traced to the individual user. Professional conduct is essential.
• Parents' attention will be drawn to the school e-Safety Policy on the school website and through a letter sent home.