



WALSH

M E M O R I A L

C.E. (Controlled)

I n f a n t S c h o o l

ONLINE SAFETY POLICY

DATE FOR REVIEW: SEPTEMBER 2022



Walsh Memorial CE Infant School



The School aims to serve its community by providing an education of the highest quality within the context of Christian belief and practice. It encourages an understanding of the meaning and significance of faith, and promotes Christian values through the experience it offers to all its pupils.

Online Safety Policy

This policy is part of the school's safeguarding responsibilities. It relates to other policies including those for behaviour, safeguarding and data handling.

Our Online Safety Manager works alongside the Designated Safeguarding Lead (DSL) as the roles overlap.

- Our Online Safety Policy has been written by the school community, building on best practice and government guidance. It has been agreed by staff and approved by Governors
- The Online Safety Policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, phones, tablets and hand held games consoles used on the school sites

Teaching and learning

Why Internet and digital communications are important

- Internet use is a part of the statutory curriculum and a necessary tool for staff and 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
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- Pupils will be taught online safety in accordance with the Hector scheme of work and reinforced regularly. It aims to bridge the gap between school IT systems and the more open systems outside of school.
- The school will have an age appropriate filtering system
- The School will ensure that its networks have virus and anti-spam protection
- Access to the internet is password protected
- Online safety will be embedded in all areas of the curriculum
- Pupils will be taught the earliest skills of building resilience to radicalization by providing a safe environment for discussing controversial issues. The school will ensure that children are safe from terrorist and extremist material
- Pupils will be taught about the importance of safe use of passwords

Managing Internet Access

Information system security

- School ICT systems security will be reviewed annually
- Virus protection will be updated regularly
- Pupils will only have access to wireless devices owned by the school and staff and children are not permitted to bring their own devices to school.

E-mail

- All pupils will be taught that we can send and open polite and friendly e-mails to people we know
- All digital communications with parents and pupils should be on a professional level and on a school system

Published content and the school web site

- Staff or pupils' personal information will not be published – pupils will be identified by first name and initial of surname only, staff by title and surname.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate

Social networking

- Social networking sites will only be used if it enhances the life of the school
- Pupils and parents will be advised that the use of social media outside school brings a range of dangers for primary aged pupils

Publishing pupils' images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- The school will ensure that the use of photographs on the school website will not allow children to be identified by surname
- The online-safety policy will be shared with parents on induction and will be available on the website

Managing filtering

- The school will work in partnership with Eduthing ensure systems to protect pupils are in place.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to a DSL who will inform Eduthing. It will then be blocked.
- Children will be taught to press the 'Hector' button to cover any information they feel is unsuitable.

- The DSL team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Serious breaches of this policy by a member of staff will be reported to Surrey County Council LADO
- Parents will be informed of any incidents of inappropriate online safety behaviour that takes place in school. Incidents of inappropriate behaviour that is outside of the school will only be investigated if it is linked to a member of the school community.

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
- iPads and associated cameras will be used during lessons or formal school time for taking photographs, as part of an educational activity.
- Sony Play station, Microsoft Xbox etc will not be used in school unless a risk assessment has been carried out.
- Staff will use a school phone where contact with pupils or parents is required unless on a school trip or otherwise unavailable (in which case dial 141 before the number is dialled to protect identity).

Protecting personal data

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

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems
- All staff must read and sign the 'Acceptable Use Agreement' before using any school ICT resource
- Any person not directly employed by the school will be asked to sign the 'Acceptable Use Agreement' before using any school ICT resource
- When pupils have free access to search the internet, staff will be vigilant in monitoring the content of the site visited.
- Parents will be asked to sign and return an internet access consent form which is part of the home-school agreement

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Introducing the Online-safety policy to pupils

- Appropriate elements of the Online-safety policy will be shared with pupils
- Pupils will gain awareness of Online-safety and cyber bullying through the Online-safety Scheme of Work called Hector's World which will be taught throughout the school as a discrete topic and woven throughout the curriculum when appropriate

Staff and the E-safety policy

- When asked to sign the 'Acceptable Use Agreement', all staff will be aware of and have access to the school's Online-safety Policy
- Staff should be aware that Internet access can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Parents' and carers' attention will be drawn to the school's Online-safety Policy in newsletters and on the school web site
- Parents and carers will from time to time be provided with additional information on Online-safety

Ensuring Compliance

- Any concerns should be reported to a DSL
- Concerns about breaches of the Online Safety Policy or Acceptable Use Agreement should be referred to the Headteacher
- Concerns of a child protection nature must be dealt with in accordance with school safeguarding procedures
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- The use of mobile phones during the teaching day is not permitted by staff, visitors or helping parents.