Wyvern Academy
Enriching Lives, Inspiring Ambitions

E-Safety

Policy

Date of approval:	March 2025
Approved by:	Consilium Academies
Date of next review:	June 2027

Consilium
Academies

Writing and reviewing the E-Safety Policy

The E-Safety Policy relates to other policies including those for ICT, Acceptable Computer Use, Anti-Bullying and for Safeguarding.

- Our E-Safety Policy has been written by the school. It has been agreed by senior management and approved by LAB Members.
- The E-Safety Policy and its implementation will be reviewed annually.
- Our E-Safety Policy relates to both existing and emerging technologies.

Teaching and learning

All internet use by staff and pupils is governed by the school's Acceptable Internet Use Agreement.

Why internet use is important:

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
- Pupils need to be aware of the dangers in cyberspace and taught how to use the internet safely.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Pupils using the internet:

- The school internet access is designed for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable, in accordance with the school's Acceptable Internet Use Agreement, and given clear objectives for internet use.
- Pupils will be taught how to use the internet safely.

Managing Internet Access Information system security

- School ICT systems' capacity and security will be reviewed regularly.
- Virus protection will be updated regularly by the school-based technician.
- Internet access will be filtered by more robust software such as Sophos and Classroom Cloud to give more protection and security to users.
- Security strategies will be discussed with the Head of School, school-based technician and the school external network support.

E-mail

- Pupils may use e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication.
- E-mails cannot be sent by pupils to an external organisation.
- Published content and the school website.
- The contact details on the website should be the school address and school e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head of School has overall editorial responsibility and will ensure that content is accurate and appropriate.

Publishing pupils' images and work on the school website

- Photographs that include pupils and any published work will not enable individual pupils to be clearly identified unless permission has been given by parents.
- Pupils' names will not be used on the website in association with photographs unless explicit permission is given in line with trust guidance and safeguarding priorities.
- The school-based technician controls access to social networking, messaging and blogging sites. All have been blocked unless requested by staff and use for educational purpose.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of some social network spaces outside school is inappropriate for certain aged groups (11-16yrs).

Managing filtering

The Trust Network Manager controls all internet filtering.

- If staff or pupils discover an unsuitable site which is not filtered, it must be reported to the school-based technician.

- The school use Sophos filtering system to manage their computer systems.

Other Communications technologies

- Emerging technologies will be examined for their educational benefit and a risk assessment will be carried out before any use in school is allowed.
- Mobile phones or other handheld communication or games devices are not used during lessons or formal school time. Any such devices seen or heard will confiscated by staff, securely held in administration and returned to the pupil’s carer(s).

Protecting personal data

Personal data will be recorded, processed, transferred and made available in accordance with GDPR.

Authorising Internet access

- The school will keep a record of any incident resulting in a pupil’s access being withdrawn.
- Pupils will be allowed to browse the internet appropriately and only under the supervision of staff.

Assessing risk

- 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 the Trust can accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT provision to establish if the E-Safety Policy is adequate and that its implementation is effective.

Handling e-safety complaints or incidents.

Complaints of internet misuse will be dealt with by the Assistant Headteacher for Behaviour & Attitudes. Any complaint about staff misuse must be referred to the Head of School. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police if any e-safety issue with legal implications arises.
- Cyberbullying or other abuse between our pupils taking place offsite can seriously affect relationships in school. Any cyber bullying incident which has such an effect will be dealt with in accordance with the school’s Anti-Bullying policy.

Community use of internet

Any community user of the school’s ICT facilities will be made aware of this policy and our Acceptable Internet Use policy and their agreement to abide by them required before such use is granted.

Introducing the E-Safety Policy to pupils

Network use, including e-safety, rules will be posted in all areas with networked computers in accordance with the school’s Acceptable Internet Use Policy.

- Pupils will be informed that network and internet use will be monitored.
- Pupils should be taught what to do if they access material they are uncomfortable with.

Staff and the E-Safety Policy

- All staff will be made aware of the School E-Safety Policy and its importance explained.
- Staff will be made aware that internet traffic can be monitored and traced to the individual user, in accordance with the school’s Acceptable Computer Use and ICT policies.
- Staff must adhere to the Code of Conduct regarding the use of mobile phones and other personal technology in school and on school business.

Enlisting parents’ support

Parents’ attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school website.