Wyvern Academy
Enriching Lives, Inspiring Ambitions

E-Safety

Policy

Date of approval:	September 2023
Approved by:	Consilium Academies
Date of next review:	September 2024

Consilium Academies

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

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

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.

Students 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.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community;
- The Headteacher and Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- Our e-Safety Policy has been written by the school. It has been agreed by senior management and approved by governors.
-

Online safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of the Trust, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for Online Safety has been designated to a member of the Senior Leadership Team.

On Site School Network Technician

The onsite school network technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets the online Safety technical requirements outlined in any relevant Trust online Safety policy and guidance;
- that users may only access the school's networks through a properly enforced password protection policy.
- School ICT systems' capacity and security will be reviewed regularly.
- Virus protection will be updated regularly by the School based technician.
- Security strategies will be discussed with the Headteacher, school based technician and the school external network support.
- The school network technician controls access to social networking, messaging and blogging sites. All have been blocked unless requested by staff and use for educational purpose
- The school will keep a record of any incident resulting in a pupil's access being withdrawn.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective

Teaching and Support Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. Central to this is fostering a 'no blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Teaching and support staff are also responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety policy and practices;

- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP);
- they report any suspected misuse or problem to the Online Safety Co-ordinator or another senior leader for investigation, action and possible sanction.
- 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.

All staff should be familiar with the school's policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- Online bullying procedures;
- Their role in providing online safety/acceptable ICT use education for pupils;
- Their role in preventing terrorism and extremism.

Designated Safeguarding Lead (DSL)

The DSL should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

Students

- Introducing the e-safety policy to students
- are responsible for using the school ICT systems and mobile technologies in accordance with the Climate for Learning Policy, which they will be expected to sign before being given access to school systems;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Students may use e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication.
- E-mails cannot be sent by pupils to an external organisation.
- Students will be advised never to give out personal details of any kind which may identify them or their location

We include online safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Students need to know how to minimise online risks and how to report a problem.

Parents/Carers

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site

The school will take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns and literature.

Students and parents will be advised that the use of some social network spaces outside school is inappropriate for certain aged groups(11-16yrs)

Photography

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 Web site in association with photographs unless explicit permission is given in line with trust guidance and safeguarding priorities.

• Written permission from parents or carers will be obtained before photographs of students are published on the school Web site, social networking and personal publishing

Online Safety Education and Training

Education – students

Online Safety education will be provided in the following ways:

- A planned online safety programme will be provided as part of ICT lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school;
- Key online safety messages will be reinforced as part of a planned programme of assemblies;
- Students will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• All new staff will be required to read this policy as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use policies.

Sexting/Peer on Peer Abuse/Cyberbullying

All staff should be aware that safeguarding issues can manifest themselves via peer on peer abuse. This could include cyberbullying and sexting. Staff should be clear as to the school policy and procedures with regards to peer on peer abuse.

Further guidance on Sexting and Cyberbullying and how to handle incidents can be found below:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_S chools_WEB__1_.PDF
https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Searching devices, viewing and deleting imagery

Adults should not view youth produced sexual imagery unless there is good a clear reason to do so. If the capture involves Child Abuse images (or suspected child abuse images):

- Do not print or copy images.
- Do not email a copy of the image to anybody.
- Do not show the image/capture to a minor.
- Do not show the image on the system to anybody who does not need to be exposed to the image.
- Ensure that the image/capture is saved in the Saved Capture area, for review, if required by those responsible for dealing with the issue.

Any printing, emailing or copying of a child abuse image is an offence under English Law. A child abuse image or indecent image of a child is an image of a sexual nature which depicts a child under the age of 18.

If the capture involves Adult pornography:

- Do not print out or copy images out unless necessary
- Do not email a copy of the image to anybody, unless necessary
- Do not show the image on the system to anybody who does not need to be exposed to the image.

- Ensure that the image/capture is saved in the 'Saved Capture' area, for review, if required by those responsible for dealing with the issue.
- Do not show the image/capture to a minor.

An offence against English law may be committed if adult pornography image is shown to a child. If there is a need to print out the image to show an adult this must be kept secure and not for general circulation.

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 hand held 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 administrations and returned to the student's carer

Filtering and Monitoring

The network technician controls all internet filtering. If staff or pupils discover an unsuitable site which is not filtered, it must be reported to the network technician.

The school should be doing all that they reasonably can to limit children's exposure to the risks below in regards to online material

-content: being exposed to illegal, inappropriate or harmful material;
-contact: being subjected to harmful online interaction with other users; and
-conduct: personal online behaviour that increases the likelihood of, or causes, harm.

As part of this process the school has appropriate filters and monitoring systems in place.

The Trust and Headteacher will ensure that, staff to undergo regularly updated safeguarding training and that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information and support

There is information available to support schools to keep children safe online. The following is not exhaustive:

www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.childnet.com/cyberbullying-guidance
www.pshe-association.org.uk
educateagainsthate.com www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

How Complaints will be handled

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 or mobile device. Neither the school nor the Trust can accept liability for material accessed, or any consequences of Internet access.

Complaints of Internet misuse will be dealt with by the Assistant Head teacher for Behaviour and Attitudes and pastoral leaders. 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.

Discussions will be held with the Police if any e-safety issue with legal implications arises.

Staff and students are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by teacher / Head of Year / Headteacher;
- Informing parents or carers;

- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework);
- Referral to LA / Police.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / Academy/ LA child protection procedures.

Documents used in preparation of this policy Teaching online safety in schools KCSIE 2021 WSCB e-safety Booklet NGFL Acceptable Use Policy for Adult Users BECTA Signposts to Safety: Teaching E-Safety.