Wychwood School
OXFORD

e-Safety Policy
Author: AKJ
Last Reviewed: March 2022
Date of Next Review: March 2024

The e-Safety Policy relates to other policies including those for ICT, Anti-Bullying, Safeguarding, and for Anti-Plagiarism.

The e-Safety Lead will be the Designated Safeguarding Lead for Child Protection which at Wychwood School is the Head.

Principles

- 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 high-quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.
- Staff will be made aware of and pupils will be educated in the safe use of the internet.
- Clear boundaries will be set and discussed with staff and pupils, for the appropriate use of the internet and digital communications.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation and the avoidance of plagiarism.
- Wychwood School will ensure that the use of internet-derived materials by staff and by pupils complies with copyright law as far as the School is able to do so by education and informing pupils of their duties.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

1. Information system security

Wychwood School's ICT system security will be reviewed regularly.
Appropriate virus protection and firewalls will be installed and updated regularly.

2. E-mail

Pupils and staff should be encouraged to use approved e-mail accounts.
Pupils must be made aware that they can report abuse to any member of staff or gap assistant but especially their form teacher.
Staff have a duty to inform the Head of any abuse and to inform the ICT Manager if appropriate.
Pupils must report offensive or inappropriate e-mail.
In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

For pupils and staff, incoming e-mail should be treated as suspicious and attachments not opened unless the author is known to the recipient.
The starting or forwarding of chain letters is not permitted.

3. Published Contact Details and the School Website

Staff or pupil personal contact information will not be published. The contact details given online should be the school office or school e-mail addresses.
The Director of Marketing and Admissions will take overall editorial responsibility and ensure that published content is accurate and appropriate.

4. Publishing Pupils' Images and Work

Photographs or videos that include pupils will be selected carefully so that images of individual pupils cannot be misused.
Pupils' full names will not be used anywhere on the school's website or other on-line space, particularly in association with photographs or videos.
Written permission, using the approved permission form, from parents, guardians or carers will be obtained before photographs or videos of pupils are published on the school's web site.
Work can only be published with the permission of the pupil and parents, guardians or carers.

5. Social networking and personal publishing

The School will educate people in the safe use of social networking sites, and educate pupils in their safe use.
Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
Pupils must be made aware that they can report abuse to any member of staff or gap assistant but especially their form teacher.
Pupils should be taught the reasons why personal photographs or images should not be posted on any social network space without considering how the photograph or image could be used now or in the future.
Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils should invite only known friends and deny access to others.
Pupils should be educated as to their responsibility to ask for consent before publishing or posting quotations, images or video material involving other people and the possible consequences of a GDPR violation.

6. Managing, Monitoring and Filtering

The School will work in line with the OSCB guidelines to ensure that systems to protect pupils are reviewed and improved.
If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Lead (DSL) or the ICT manager.
The ICT manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. S/he will report this to the Head on a regular basis.
The School reserves the right to decide which internet sites are inappropriate viewing when deciding what to filter.
Where a pupil or staff member accesses a site that is inappropriate in the eyes of the School, they will be regarded as being in breach of this policy and the School may then bar the individual from further internet access or take disciplinary action as the School feels is appropriate to the type of site accessed.

7. Managing Skype, Teams and Zoom

Videoconferencing or Skypeing, using Teams or Zoom will be appropriately supervised for the pupil's age. Please see the separate protocols for e-learning.

8. 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.
The Senior Leadership Team should consider in their policy making that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
Where contact with pupils is required to facilitate their learning or security, staff may give out their personal mobile phone numbers or e-mail addresses but MUST inform the Head in writing that they have done so and the reason for so doing.
Mobile phones will not be used during lessons or formal school time except when they are being used as translating dictionaries or, with staff permission, to take photographs of work. In this case, supervising staff have the right to ask to see the device to ensure this is what is actually occurring.
The sending of abusive or inappropriate text messages is forbidden (see the Anti-Bullying Policy).
The use by pupils of cameras in mobile phones will be kept under review.
It should be noted that games machines including the Wii, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

9. Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Acts 1998, 2003 and 2018.

Policy Decisions

1. Authorising Internet Access

All staff must read and sign the 'Staff Acceptable Use Policy and Code of Conduct for ICT' before using any school ICT resource, including any laptop issued for professional use.
The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
All pupils must apply for internet access individually by agreeing to comply with the Pupil ICT Network, Mobile Phone and Acceptable Use agreement on an annual basis.
Parents, guardians or carers will be asked to sign the same agreement on an annual basis.

2. Assessing risks

The School will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Wychwood School cannot accept liability for any material accessed, or any consequences of inappropriate internet access.
The School should audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety Policy is appropriate and effective.
Schools must ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the School.

3. Handling e-Safety Complaints

Complaints of internet misuse will be reported to the e-Safety Lead (DSL), and action in line with the School's policies will be taken.

Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children should be reported to the LADO/MASH within one working day in accordance with OSCB and Wychwood School, Oxford's Safeguarding Policies.

Any complaint about staff misuse must be referred to the Head and if the misuse is by the Head it must be referred to the Chair of Governors or Safeguarding Governor in accordance with OSCB and Wychwood School, Oxford's Safeguarding Policies.

Pupils, parents and staff will be informed of the complaints procedure.

Communicating e-Safety

1. Introducing the e-Safety Policy to Pupils

All system users will be informed that network and internet use will be monitored.

A programme of e-safety training and awareness raising will be put in place.

2. Staff and the e-Safety Policy

All staff will be given access to the school e-Safety policy and its importance explained.

Staff must be informed that network and internet traffic can be monitored and traced to the individual user, including staff laptops.

Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and work to clear procedures for reporting issues.

Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship. Staff should notify the head as described above if they give out e-mail addresses or mobile phone numbers to pupils.

3. Enlisting Parents', Guardians' and Carers' support

Parents' and carers' attention will be drawn to the School e-Safety policy in letters, and on the school website.

Specific e-Safety Concerns

This section identifies a number of areas of concern that Wychwood School, Oxford will attempt to monitor and will manage on a case-by-case basis, bearing in mind both victim and perpetrator will need support if not adults. Pupils are always encouraged to inform a responsible adult of any instances of dangerous internet-related behaviours of peers

1. Unrestricted access to the internet by pupils who bypass the school's e-safety systems via mobile phones or VPNs
2. Cyber bullying
3. Sexual harassment of pupils by peers or adults
4. Sexual grooming by pupils or of pupils
5. Consensual or non-consensual sharing of inappropriate images
6. Viewing pornography
7. Viewing other damaging and harmful content e.g. excessively violent or misogynistic content
8. Playing age-inappropriate games
9. Use of chat rooms for radicalisation