E-SAFETY AND ACCEPTABLE USE POLICY

for

Wentworth Primary School

Reviewed: October 2023
Next Review: October 2026

E-Safety and Acceptable Use Policy

Wentworth's Computing Vision
At Wentworth Primary School we will develop the learning environment to provide a range of Computing opportunities and tools. This will empower our children to make relevant and safe choices and be flexible as they develop their personalised learning, in line with our school's vision.

The aims of this Acceptable use Policy are to:

- Ensure that pupils benefit from all learning opportunities offered by the internet resources provided by the school in a safe and controlled manner.
- Ensure that all staff benefit from internet access, with clear guidance on safe and acceptable use.
- Make staff and pupils aware that internet use in school is a resource and a privilege. If the terms are not met, the privilege will be taken away.
- Provide guidance to staff and pupils about the acceptable use of mobile technologies, both the school's and personal items that are brought into school.

General

- Virus protection software is used and updated on a regular basis.
- The Head Teacher, Leadership Team and Computing Subject Leader are responsible for the school's e-safety.

Pupils' Access to the Internet

- Wentworth Primary School use a "filtered" Internet Service, which minimises the chances of pupils encountering undesirable material.
- We will only allow children to use the internet when there is a responsible adult present to supervise.
- However it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of pupils.
- Teachers and the Computing TA will have access to pupils' It'sLearning area, to ensure expectations of behaviour are being met.

Expectations of Pupils and Staff using the Internet

- All pupils are expected to read and agree the Internet Agreement.
- At Wentworth, we expect all pupils and staff to be responsible for their own behaviour on the internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.
- Pupils and staff using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils or staff encounter any such material accidentally, they are expected to report it immediately to the Computing Subject Leader, so that the Service Provider can block further access to the site.
- Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. They have been taught the rules of etiquette in email and are expected to follow them.
- Pupils and staff are expected not to make derogatory comments about other members of staff, pupils or parents in their e-mail communications or on social media.

- Pupils must ask permission before accessing the internet and have a clear idea why they are using it.
- Pupils and Staff should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork.
- No program files may be downloaded and installed to the computer from the internet. This is to prevent corruption of data and avoid viruses.
- No programs on disc or CD Rom should be brought in by pupils from home for use in school, although staff can seek permission from the Head. This is for both legal and security reasons.
- Homework completed at home may be brought in on a CD-ROM or memory stick, but this will have to be virus scanned by the Computing TA before use.
- No personal information such as phone numbers and addresses should be given out and arrangements to meet someone should never be made.
- Pupils and Staff consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to internet resources. They will also come under the general discipline procedures of the school which comprises an escalating set of measures including a withdrawal of privileges.
- Uploading and downloading of non-approved software will not be permitted. Approval must be sought from the Computing Subject Leader first.

School Website and Social Media

- Prior to publishing photographs, images and videos staff must check that parents have given consent to these being published via the school office.
- The website and social media will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The publication of children's work will the decided by a teacher.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Photographs and video focusing on individual children will not be published on the school website and social media without parental permission.
- The school website and social media will avoid publishing the full names of individuals in a photographs, audio and video clips.
- The school will ensure that the image files are appropriately named and will not use pupils' names in image file names if published on the web.

Personal Devices

Staff and pupils may only use their own technology in school as part of a pre-arranged educational activity, with permission from a member of the SLT or Computing Subject Leader. Inappropriate use is in direct breach of the school's acceptable use policy.

School Devices

Staff can take electronic devises off-site for an educational purpose, for example: a school trip. On such occasions, it is the staff member's responsibility to sign the equipment out and back in again on the 'Off-Site register' – which is located in the school office. While off-site, the electronic equipment is the responsibility of the staff member and must be kept safe and secure at all times. If it is damaged, lost or stolen then this must be reported to the Head Teacher immediately, who must be informed of any data breeches.

Data Security

All staff must ensure that data on pupils and adults in the school is kept secure at all times and stored in a safe manner in line with the school's GDPR requirements and policies. Any breech of this could result in

disciplinary action against a member of staff or a fine. All breeches must be reported to the Head as soon as possible.

Filtering and Monitoring

The school's filtering system is age and ability appropriate for the users, and suitable for an education setting. An effective system should not unreasonably impact teaching and learning or school administration; or restrict students from learning how to assess and manage risks themselves. The school's filtration system is operational, up to date and applied to users, including guest accounts, school owned devices and devices using the school broadband connection. These systems are monitored and regularly reviewed to ensure they are effective. They will be checked by the school's IT support provider to ensure they work on new devices and services before they are released to staff and pupils. All staff receive annual online safety training, including how to report concerns.

No filtering system can be 100% effective. To try to ensure that undesirable material is unavailable to pupils, the school always uses firewalled services to filter information and block access to harmful sites and inappropriate content. Talk Straight provide the 'Schools Broadband' and set filtering preferences, working with the UK Safer Internet Centre. A document entitled, 'Appropriate Filtering for Educational Settings' can be viewed on request from the school's business manager, which gives further detail on how Schools Broadband meets the national defined 'appropriate filtering standards'.

No personal devices are to be connected to the school's Internet. All staff must follow the school's safeguarding procedures if there are concerns and report these immediately to the designated safeguarding lead.

To understand and evaluate the changing needs and potential risks, the school's filtering and monitoring provision will be regularly reviewed by the designated safeguard lead, members of the senior leadership team, Computing Subject Leader, IT provider, IT support provider and involve the responsible governor. Blocklists are reviewed and modified in line with changes to safeguarding risks.

The school will refer to the DfE 'Filtering and Monitoring Standards' online document to ensure that best practise is followed.

Sanctions

Persistent misuse of the internet by pupils will result in reducing access to the internet. Misuse of other technologies will result in a complete ban and/or confiscation. Both of these actions will take place for a set period of time agreed by the Head Teacher. Parents will always be notified.

Misuse of the internet by a member of staff could result in the disciplinary procedure being followed.

Wentworth Primary School Pupil Internet and Computing Agreement

This is to be read through with your parent(s) and then signed. You will be allowed internet access after this is returned to school.
At Wentworth Primary, we expect all pupils to be responsible for their own behaviour on the internet, just as they are anywhere else in school.
This includes materials they choose to access, and language they use.

- Pupils must ask permission before accessing the internet.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. It is forbidden to be involved in sending chain letters.
- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork.
- No program files may be downloaded to the computer from the internet.
- No programs on disc or CD Rom should be brought in from home for use in school.
- Homework completed at home may be brought in on a CD ROM or memory stick, but this will have to be virus scanned by the class teacher before use.
- Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to internet resources.

I have read through this agreement with my child and agree to these safety restrictions.

Signed: _____ (Parent/Responsible Adult)

Name of child: _____

Wentworth Primary School Staff Internet and Computing Agreement

I have read through this agreement and agree to these safety restrictions.

Signed_____
Print_____

Counter signatory_____
(Computing Subject Leader or Head Teacher)