

Acceptable Computer and Internet Usage Policy

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students.

All KS3 and 4 students will be **actively supervised at all times** when using computers. Post 16 students do have unsupervised access to computers to allow for independent research and study. All reasonable precautions to ensure that students only access appropriate material have been taken.

However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never be accessed. The school does not accept any liability for the material accessed, or any consequences thereof.

To ensure that all students understand what is acceptable when using any computer system or the Internet a Code of Practice has been created. (see overleaf)

This Code of Practice will be discussed with every student and copies will be displayed in appropriate places.

Post 16 Students will have to sign a copy of this Code of Practice before access to the school's network is allowed.

If a student breaches this Code of Practice then severe penalties will be enforced to protect the school, student and computer systems. The penalties will be decided by IT staff depending on the severity of the incident. In serious cases the management team will be consulted and the student may have to appear before a sub-committee of the governing body. Sherburn High School may also report concerns to other appropriate bodies.

Post 16 students may find it difficult or impossible to continue with their studies depending on the penalty imposed.

Staff

The same Code of Practice also applies to all staff of Sherburn High School. Penalties for staff breaching the Code of Practice will be decided on an individual case basis.

Staff must ensure that all KS3 and KS4 students are **actively supervised at all times** when using computer equipment. Failure to do so may result in that member of staff being unable to book and/or access IT resources such as computer rooms.

The email system and Internet access facilities are provided by the school as a business tool to enable authorised users to carry out their job role efficiently. The school regards any e-mails sent or received via the school email system as impersonal and access to emails may be granted by the line manager or senior leadership team if the need arises, such as staff absence or leaving the employment of the school.

Staff must ensure that they regularly check for new emails. Each email address has a limited storage space and therefore staff must delete old emails regularly. Once the storage limit has been reached no further emails will be received.

Acceptable Computer and Internet Usage Policy

This Acceptable Computer and Internet policy will help protect students, staff and the school by clearly stating what is acceptable and what is not.

Code of Practice

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or the staff member's job role
- Viewing of any offensive or pornographic materials is not allowed. Accidental access should be reported at once to the appropriate member of staff.
- The playing of games / quizzes is prohibited at all times unless authorised by a member of staff.
- Copyright and intellectual property rights must be respected.
- Users are responsible for e-mail they send and for contacts made.
- E-mail should be written carefully and politely.
- The use of public chat rooms or instant messaging services is not allowed.
- The security of IT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Users are not to physically tamper with IT equipment, attach unauthorised hardware or install / run unauthorised software.
- The school has various systems in place to monitor computer use, internet access, files stored and emails. Attempting to bypass any monitoring or security systems will result in disciplinary action being taken. These systems will be used to ensure that this Code of Practice is followed.
- Irresponsible use of any IT facilities will result in the loss of Network and / or Internet access. Depending on the severity of the abuse further action may be taken by school or the appropriate authorities.

June 2006
June 2007(Revised)
June 2008 (Reviewed)
June 2009

Next Review Date June 2010