The Whitby Secondary Partnership

INTERNET POLICY

Governance Status

This policy will be reviewed as required in the light of new Government legislation and/or Local Authority guidance or every three years.

Review dates	By Whom	Approval dates
June 2022	Staff and Governors	21 June 2022
June 2025		

Signed by the Chairs:

Student access to the Internet

The Whitby Secondary Partnership (WSP) encourages use by students of the rich information resources available on the internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills are fundamental in the society our students live in.

On-line services significantly alter the information landscape for education institutions by opening teaching to a broader array of resources. In the past, teaching and library materials could usually be carefully chosen. All such materials would be chosen to be consistent with national policies, supporting and enriching the curriculum while taking into account the varied teaching needs, learning styles, abilities and developmental levels of the students. Internet access, because it may lead to any publicly-available site in the world, will open classrooms to electronic information resources which have not been selected by tutors as appropriate for use by students.

Electronic information research skills are fundamental in the development of our young citizens and

employees of the future. The WSP expects that staff will begin to investigate possibilities and blend use of such information as appropriate within the curriculum and that staff will provide guidance and instruction to students in the appropriate use of such resources. Staff will consult the Network Manager for advice on content, training and appropriate teaching levels consistent with the commitment to ICT across the curriculum.

Independent student use of telecommunications and electronic information resources will only be permitted upon submission of permission and agreement forms by parents of students and students themselves.

Access to on-line resources will enable students to explore libraries and databases, and to exchange messages with people throughout the world. The WSP believes that the benefits to students from access to information resources and increased opportunities for collaboration exceed the disadvantages. However, ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the WSP supports and respects each family's right to decide whether to apply for independent access.

The WSP ICT Working Groups will prepare appropriate procedures for implementing this policy and for reviewing and evaluating its effect on teaching and learning.

Resource Development

In order to match electronic resources as closely as possible to the national and schools' curriculum, teachers need to review and evaluate resources in order to offer materials that are appropriate to the age range and ability of the group being taught. Staff will provide appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies. All students will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group.

As much as possible, schools' chosen information provider has organised information resources in ways that point students to those that have been reviewed and evaluated prior to use. While students may be able to move beyond those resources to others that have not been evaluated by staff, they will be provided with guidelines and lists of resources particularly suited to the specific learning objectives. Students may pursue electronic research independent of staff supervision only if they have been granted parental permission and have submitted all required forms. Permission is not transferable and may not be shared.

WSP Rules

The WSP has developed a set of guidelines for Internet use by students. These rules will be made available to all students, and kept under constant review. All members of staff are responsible for explaining the rules and their implications. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards students.

<u>Student Guidelines for Internet Use</u>

General

The internet is provided for students to conduct research and communicate with others. Parental permission is required before students can gain access. Access is a privilege, not a right and that access requires responsibility.

Individual users of the internet are responsible for their behaviour and communications over the

network. It is presumed that users will comply with WSP standards and will honour the agreements they have signed.

Computer storage areas and USB drives will be treated like student lockers – ie, staff can review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or drives will always be private. During school hours, tutors will guide students towards appropriate materials. Outside of school, families bear responsibility for such guidance, as they must also exercise with information sources such as television, telephones, film, radio and other potentially offensive media.

The following actions are not permitted:

1. Using any other individual's computer account or password or allowing other users' access to your own.
2. Leaving your user account open and unattended; failing to log out after use or not securing removable media, eg, USB drives, when unattended.
3. Inappropriate, unethical, or illegal use of another individual's computer.
4. Using computing resources, facilities, and equipment for personal commercial gain.
5. Intentionally seeking information on, obtaining copies of, modifying, or tampering with files, tapes, passwords, or any type of data belonging to other users.
6. Using resources including mobile telephones and removable media to develop or execute programs that could harass other users, infiltrate the systems, damage or alter the software components of the systems, or disrupt school activities.
7. Violating any network-related policy whether set by the Government, WSP or a network governing body.
8. Accessing social networking sites and chat rooms; including but not restricted to: Messenger, SnapChat, TikTok, Instagram, Twitter and Facebook.
9. Making excessive use of resources, controlled or otherwise, eg, excessive printing.
10. Misrepresenting oneself or others through email or other electronic communication.
11. Using, duplicating, or distributing licensed software and documentation without the express written permission of the original copyright owner.
12. Using unauthorised copies of licensed software.
13. Abusing, harassing, intimidating, threatening, stalking, or discriminating against others through the use of computing resources.
14. Accessing and playing games from unauthorised websites (excluding educational sites).
15. Engaging in vandalism or mischief that incapacitates, compromises, or destroys school resources either physically or via electronic means.
16. Eating or drinking at or near computer equipment.

Sanctions

1. Violations of the above rules will result in firstly a restriction on site access, then a temporary ban, on internet use, and finally a permanent ban of internet access and use of the Learning Centre facilities.
2. Additional disciplinary action may be added in line with existing practice.
3. When applicable, police or local authorities may be involved.

The following guidance has been written in line with the recommendations made in the 'Superhighway Safety Pack'. A full version of the text may be found at http://safety.ngfl.gov.uk

Images of students on the websites

Students should be protected from being individually identified by persons with potential ill intent. Therefore, when using images or names of students on the websites the following must be done:

- Images of students must be appropriate for public viewing
- If a student is named, avoid using their photograph
- If a photograph is used, avoid naming the student
- Group photographs should also avoid the use of student names.

Photographs of student work, with the author acknowledged, are to be encouraged. This enables students to exhibit work to a wider audience. The ICT Network Manager will check images of students on the websites and remove any deemed inappropriate. The internet agreement will also include the option as to whether or not the parent agrees to their child's photograph being used on the websites.

Internet filtering and supervision

The ICT Network Manager will ensure that the schools are provided with an effective internet filtering system. This may be provided by the ISP (Internet Service Provider) and/or a 'firewall' installed on the WSP network. The ICT Network Manager will monitor usage of the Internet and report any access to inappropriate material to relevant senior staff.

Individual teachers are responsible for the supervision of students when using the internet in their lessons. When websites have been identified before the lesson, teachers should check the content before use by students. It is advisable to access the site some time prior to the lesson. This means that all web pages accessed can be saved onto the network, resulting in much quicker access by students.

Computer viruses

The ICT Network Manager will ensure that up-to-date anti-virus software is installed across the network. This must cover the internet connection and disk drives. Any reports of potential viruses should be reported to the ICT Network Manager immediately. Any deliberate attempt to download, install, write or spread viruses must be reported to the ICT Network Manager immediately who will report the matter to the Principal or other, designated, senior member of staff. Resulting action will be in line with the ICT Behaviour Policy.

Student Email addresses

Some students already will have their own email address(es). These might be through web-mail accounts, which may be accessed across the Internet from any location.

The students are issued with a school email address. This is through Gmail and is available whether at home, in school or on a mobile device utilising Google Classroom. Teachers should encourage students to use these accounts at home and in school. However, students are reminded that infringements of the policy will result in ICT staff being informed and action being taken as appropriate.

Students must only use e-mail in lessons under the direction and supervision of the teacher. On occasions where there is heavy Internet traffic, through high simultaneous demand, students may be

refused access to their e-mail accounts.

Students should be taught the social conventions involved in sending e-mails (known as 'netiquette') and be informed that the e-mails they send may be monitored.

Staff are provided with an e-mail facility, but to protect their own privacy and for safety, all e-mails to staff must be through post@ccwhitby.org or admin@eskdale.n-yorks.sch.uk and the subject line should have the recipient's name. Staff will not be able to e mail students.

Payment for goods over the Internet

Students must not order or pay for goods over the internet using school facilities.

Intellectual property and copyright issues regarding the Internet

Intellectual Property is a series of legal rights that give protection for different types of invention, design, brand name or original creation. The legal rights, which include patents, trade marks and copyright, give the creator the right to prevent the unauthorised use of the invention, design, brand name or creation, for the period of protection. They are provided to reward creativity and encourage innovation. Unauthorised use can be a criminal offence (equivalent to theft).[1]

The Copyright, Designs and Patents Act mentions 'fair dealing' with respect to:

"A literary, dramatic, musical or artistic work for the purposes of research or private study does not infringe any copyright in the work."[2]

Although 'fair dealing' has no legal definition, the following do not constitute fair dealing:

- Copying by a person other than the researcher or student him/herself
- The person doing the copying knows or believes that it will result in more copies of the same material (in the case of staff copying of resources, existing school rules apply).

Web pages on the Internet are subject to copyright law. Each page may contain several copyrights if it contains text, music, graphics and so on. Students should therefore only make one copy of the material and acknowledge the source of the information in their work. Students should be encouraged to look for copyright information on web sites or to seek permission by contacting the webmaster of the site. Any staff or students who are unsure of copyright issues of regarding a particular website or web page should consult the Network Manager, ICT Technical support staff or Learning Resource staff.

Teachers should ensure that the work produced by students is their own and not plagiarised from other sources. Staff should be made aware that a number of 'essay banks' are available on the Internet for students to copy and submit for assessment as though it were their own work. Additionally students can submit their own essays to an 'essay bank' in return for a fee. Any sites discovered by staff should be reported to the ICT Network Manager who will, in turn, block access to them in school. Any incidence of plagiarism using Internet resources or resources copied electronically (eg: scanned) should be dealt with by subject leaders, as appropriate.

---

[1] From the Superhighway Safety Pack - Full text found on the NGfL

[2] Copyright, Designs and Patents Act 1988

ICT Health and Safety

All students will be introduced to the school ICT facilities when they arrive at each site usually at the beginning of Year 7. This will include a session on ICT Health and Safety. The ICT Network Manager will report any potential or actual health and safety risks to the WSP Health and Safety Officer to be dealt with as necessary. Teachers should ensure that students use computers safely. All computer maintenance must only be carried out by ICT Technical Support staff.

Introduction to the ICT facilities

This should include the following:

- Introduction to the facilities
- Access to the facilities during and after normal WSP hours
- ICT health and safety
- Internet safety
- Use of passwords
- The Internet Agreement
- ICT Do's and Don'ts
- The school website and associated web-based platforms.
- The opportunity for all students to log on to and off the network and to access some resources
- Issue of information for parents and students, as appropriate.

Internet Agreement

The Internet Agreement will be included in the student planner. This will incorporate the issues previously covered in this document. Tutors should draw students' attention to the content of the agreement. When a student first attends school, tutors must ensure that each student signs the agreement. Tutors should also check that parents have signed the agreement. Tutors will keep a checklist of students and parents who have signed the agreement. When complete, this should be returned to the Network Manager. Students retain the agreement in the planner. The agreement will also include the option as to whether or not the parent agrees to their child's photograph being used on the school website.

Should an incident arise involving breach of the rules of the agreement, staff should follow the ICT Behaviour Policy, referring students as appropriate. To reinforce this with the student, staff may refer to the signed agreement in the student planner.

ICT Behaviour Issues

Any attempt at damaging equipment, theft, installing software, violating copyright laws, using other student or staff passwords, altering, copying or deleting the work of others, wasting resources, sending abusive, obscene or inappropriate e-mails, bullying, producing inappropriate web pages, unauthorised or inappropriate use of the Internet, hacking or tampering with the school networks must be reported to the ICT Network Manager who will report the matter to the Principal/Headteacher or other, designated, senior member of staff. The resulting action will be in line with the ICT Behaviour Policy.

A simplified list of ICT Do's and Don'ts will be displayed in all rooms containing ICT equipment.