ICT Acceptable Usage Policy for Students

Person Responsible:	Network Manager	**Frequency of Review:**	2 Years
Authorisation By:	Headteacher	**Notice Date:**	25/04/2025
Authorisation Date:	25/04/2025	**Review Due By:**	25/04/2027

1 RATIONALE

Upper Wharfedale School provides ICT facilities for use by our students. These facilities come with responsibilities and this document summarises the standard of acceptable use that is expected from all students using ICT facilities in school.

2 ACCEPTABLE USAGE

1. Students will be given an individual log in and email account for use at school and for homework and to communicate with staff and students within the school. Students are responsible for safeguarding their password for the system. For security reasons passwords should not be printed, stored on-line or given to others. Students are responsible for their login account and must not allow any other user access to resources through their account. The school email account should be used in a professional manner. The use of Teams should also be professional and not used as an unofficial chat tool.

2. Year 7, 8 & 9 students will only be able to communicate between existing Upper Wharfedale students, staff and selected third parties via email. There is monitoring software in place which will alert the school if any abusive language is used in any email.

3. Students at Upper Wharfedale School are allocated a certain amount of file space to store their personal work on the school network plus secure cloud storage as part of our cloud software package. This service also provides free access to Microsoft Software for use at home.

4. Users must not store non-curriculum materials (such as videos and music) on the school systems. All storage areas are monitored by school IT staff and files can be removed without warning.

5. Students must act responsibly when printing work and be economical in their use of paper and ink, proof reading their work and using preview functions to avoid wasted printouts. To encourage this, students are given an allowance per half term for printing. If the student uses up this allowance they can add print credit to continue printing.

6. Students must respect the privacy of other users and not attempt to access, modify or copy data or passwords belonging to other users. They must not attempt to install or download software (e.g. music, games or other program files), unless specifically instructed to do so, or interfere with the proper operation of software or hardware on local machines or on the network.

7. The network also provides Internet access. No user should attempt to access unlawful or undesirable materials such as obscene, racist or indecent material. If undesirable material is accessed in error, then they should exit from that site and inform a member of staff immediately. All internet access is filtered, monitored and logged and can be reported on if required. A daily safeguarding report is reviewed by the DSL and any concerns followed up. This includes the bring your own device (BYOD) wireless service offered to students

8. Students are expected to act responsibly and use the network and Internet for school related work only. For example students **must not**:

    a. subscribe to mailing lists
    b. take part in online auction sites
    c. play online games
    d. use email accounts, except for their official school email account
    e. visit chat rooms, social networking sites or instant messaging/text sites
    f. participate in or respond to chain letters e-mails
    g. send feedback to sites or take part in online surveys or questionnaires without the permission of a teacher
    h. send or forward inappropriate emails
    i. reveal personal details about themselves online

9. Students should not engage in actions in which they attempt to bypass the filtering process or restrictions of the system.

10. ICT equipment belonging to school, such as laptops, should not be taken from school; unless this is part of a formal loan process.

11. Students must respect copyright and must not attempt to pass off the work of others as their own.

12 The School will monitor and record use of the Network to investigate or detect unauthorised use. The School retains the right to intercept, check and delete (where appropriate) all written, graphic, audio and other materials created, produced, communicated, stored or accessed on school IT or connected equipment by students, including emails. We may also intercept, check and log internet usage including encrypted traffic.

13 All school systems are monitored for Safeguarding reporting, including the tracking of keystrokes. Allowing entered data, screenshots and contextual information to be sent to members of the safeguarding team.

14 Appropriate disciplinary measures may be taken against any student who does not comply with the above.

3 PERSONAL DEVICES

This policy is designed to ensure that potential issues involving personal portable devices such as 'mobile phones, smart devices, tablets and laptops can be clearly identified and addressed. UWS is keen to utilise the benefits of personal devices during school life.

3.1 Mobile Phones

The widespread ownership of mobile phones requires that teachers, students, parents, carers and volunteers take the necessary steps to ensure that mobile phones are used responsibly at school.

At Upper Wharfedale School it is recognised and accepted that parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety. There is also increasing concern about children travelling alone on public transport or commuting long distances to school. Excursions, camps and extra-curricular activities may well require that a student has a mobile phone to remain contactable.

Mobile phones can be brought into school, but must be away in a pocket or bag whilst on site, unless directed to be used by a member of staff.

Mobile phones must not be used for making calls, sending SMS messages (texting), using instant messaging, taking photos or making videos during lesson times or between lessons unless express permission is given by a teacher.

If students need to contact their parent/carer during the day they should visit the school office.

3.2 Bring Your Own Device

The school recognises the importance of emerging technologies in mobile devices. As such we employ a 'Bring Your Own Device' scheme to take advantage of this technology during lessons. Any personal devices brought into school must only be used in lessons where the teacher has authorised their use.

It is the responsibility of the students who bring personal devices to school to abide by the guidelines set out in this policy. Students must acknowledge that it is a privilege to be permitted to bring mobile devices to school and failure to comply with these guidelines may lead to a curtailment of this privilege. Action may be taken by staff to confiscate any device if necessary and arrangements be made for its return at the end of the school day.

- Parent/carers should be aware if their child has a personal device in school and give permission for them to be carrying one, by signing this agreement.
- Sole responsibility for the device lies with the student. Upper Wharfedale School does not take any responsibility for loss, damage or theft of the device. Parents and carers are encouraged to check the device is covered under their home insurance when on the way to/from in school.
- Personal devices are only to be used during the school day with the express permission of a member of staff.
- Students are advised to use passwords or pin numbers to ensure that unauthorised access cannot be made (e.g. by other students, or if stolen). Passwords and pin numbers must be kept confidential.
- Any mains powered chargers must be taken to the AV room before being used to be PAT tested. This check needs to be performed annually.
- Devices should not use mobile broadband while in school. A dedicated protected BYOD network is provided for personal devices.
- IT Support is only provided for connecting personal devices to the BYOD network or when using school provided resource sites.
- All files must be saved within the school-provided online storage.
- No external media should be used between personal devices and school owned devices.
- Personal devices cannot, under any circumstances, be taken into examination rooms.
- Students must not use their devices to broadcast music. Headphones must only be worn when authorised by the staff member in charge of the lesson.
- Students must only use software and apps they have been given express permission to use and for educational use only.
- Students must ensure that any file stored on their device does not contain material that:
    - displays images of violence, injury or death
    - is pornographic in nature or abusive
    - promotes intolerance, and/or discrimination on grounds of race, sex, disability, sexual orientation, religion or age
    - relates to criminal activity e.g. buying and selling drugs
    - relates to unlawful activity e.g. breach of copyright
    - may generate a security risk to the school or cause offence
- Students must not use personal devices to bully or threaten, in particular taking videos or pictures of acts to denigrate and humiliate another student. Devices are not to be used in the changing rooms or toilets or used in any situation that may cause embarrassment to their fellow students, staff or visitors to the school.
- Cyber-bullying is unacceptable and will not be tolerated. It is a criminal offence to use a mobile to menace, harass or offend another person and almost all calls, text messages and emails can be traced.

4 SOCIAL MEDIA

Social media sites are blocked by the internet filter in school. Students must not use social media sites or apps (such as Facebook, Twitter, Snapchat, Instagram, Tiktok) to do anything which might bring the school into disrepute. Students must not attempt to create friendships with members of staff (past or present) through social media sites.

5 ONLINE SAFETY RULES

The following online rules help to protect students when using the internet. These online safety rules help to protect students and the school by describing acceptable and unacceptable computer use.

- It may be a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the Headteacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- All network and internet usage is monitored including private encrypted traffic.

6 ACCEPTABLE USAGE RULES

The following points are a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, and file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal devices (e.g. mobile phone/tablet/laptop) in school at times that are permitted. When using my own devices I understand that I have to follow the rules set out in this document and that I bring the device to school at my own risk.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.