

# E SAFETY & ICT ACCEPTABLE USE POLICY FOR STUDENTS

Approved by [Committee/FGB] on	12th September 2022
Next review date:	September 2025
Signed by [Chair of Governors/Chair of Committee]:	

# E-safety and ICT acceptable use policy for students

All students must follow the conditions described in this policy when using school ICT networked resources including Internet access, Google Apps for Education and student share both in and outside of school.

Breaking these conditions may lead to:

- Withdrawal of the students' access,
- Close monitoring of the students' network activity,
- Investigation of the students' past network activity, and
- In some cases, criminal prosecution.

Students will be provided with guidance by staff in the use of the resources available through the school's network. School staff will regularly monitor the network to make sure that it is being used responsibly.

The school will not be responsible for any loss of data as a result of the system or student mistakes in using the system. Use of any information obtained via the network is at the students' own risk.

## Conditions of Use

Student access to the networked resources is a privilege, not a right. Students will be expected to use the resources for the educational purposes for which they are provided.

It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this policy. Students must also accept personal responsibility for reporting any misuse of the network to their Head of House.

## Acceptable Use

Students are expected to use the network systems in a responsible manner. It is not possible to list every rule regarding appropriate use of ICT. All use, however, should be consistent with the school's Wildly Important Goals and Beliefs, ethos and other policies. The following list does provide some examples that must be followed, but is not exhaustive:

1. I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the school (or West Sussex County Council) into disrepute.
2. I will use appropriate language. I will remember that I am a representative of the school on a global, public system.
3. Illegal activities of any kind are strictly forbidden.
4. I will not use language that could stir up hatred against any ethnic, religious or other minority groups.
5. I understand that files held on the school network will be regularly checked by the Network Support team or other members of staff.
6. I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
7. I will not trespass into other users' files or folders.
8. I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people's username and password.
9. I will ensure that if I think someone has learned my password then I will change it immediately and/or contact my Head of House.
10. I will ensure that I log off after my network session has finished.
11. If I find an unattended machine logged on under another user's username I will not continue using the machine. I will log it off immediately.
12. I understand that I will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
13. I am aware that e-mail is not guaranteed to be private. Messages relating to illegal activities will be reported to the authorities. Anonymous unnamed messages are not permitted.

14. I will not use the network in any way that would disrupt use of the network by others.
15. I will report any accidental access to other people's information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to my Head of House.
16. I will not introduce USB drives or other portable devices into the network without having them checked for viruses.
17. I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
18. I will not download and/or install any unapproved software, system utilities or resources from the Internet.
19. I realise that students under reasonable suspicion of misuse in terms of time, activity or content may have their usage closely monitored or have their past use investigated.
20. I will not receive, send or publish material that violates copyright law. This includes materials sent I received using video conferencing or web broadcasting.
21. I will not attempt to harm or destroy any equipment, work of another user on the school network, or even another website or network connected to the school system.
22. I understand that unapproved system utilities and executable files are not allowed in my work areas or attached to emails.
23. I agree to comply with the acceptable use policy of any other networks that I access.

The following expectations then apply when using BYOD (bring your own device) both in lessons and in other activities:

1. Bring devices to school fully charged.
2. Turn off devices or put to sleep when not in use.
3. Only use your own device or those provided by the school.
4. Take photos and videos of assignments only.
5. Use only the school wifi, not 4G, 3G or other mobile data.
6. Do not use devices in hallways, communal spaces or during lesson changeovers.
7. Do not wear headphones or ear-buds unless in specialist subject areas and with teachers' permission.
8. Know how to use your own devices, take responsibility for all hardware issues on your own devices and do not bring viruses into school.

A child's 'own device' will be confiscated for any inappropriate use