Student Acceptable Use of ICT Policy

Reviewed: September 2016

All students must follow the conditions described in this policy when using school ICT networked resources including: internet access, the school Virtual Learning Environment (VLE) “Moodle” both in and outside of school.

Breaking these conditions may lead to:

- Withdrawal of the student’s access
- Close monitoring of the student’s network activity
- Investigation of the student’s past network activity
- 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.

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 Mr Ashdown (Deputy Headteacher).

Acceptable use

Students are expected to use the network systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable.

The following list does provide some examples that must be followed:

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. Illegal activities of any kind are strictly forbidden.
3. I will not sue language that could stir up hatred against any ethnic, religious or other minority group.
4. I realise that files held on the school network will be regularly checked by Mr Ashdown or other members of staff.
5. I will not reveal any personal information (e.g. Home address, telephone number) about myself or other users over the network.
6. I will not trespass into other users’ files or folders.
7. I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people’s usernames and passwords.
8. I will ensure that if I think someone has learned my password then I will change it immediately and/or contact Mr Ashdown.
9. I will ensure that I log off after my network session has finished.
10. If I find an unattended machine logged on under other users username I will not continue using the machine – I will log it off immediately.
11. 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.

12. I am aware that email is not guaranteed to be private. Messages supporting of illegal activities will be reported to the authorities. Anonymous/unnamed messages are not permitted.
13. I will not use the network in any way that would disrupt use of the network by others.
14. I will report any accidental access to other people's information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to Mr Ashdown.
15. I will not introduce "USB drives" or other portable devices into the network without having them checked for viruses.
16. 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.
17. I will not download and/or install any unapproved software, system utilities or resources from the internet.
18. 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.
19. I will not receive, send or publish material that violates copyright law. This includes materials sent/received using Video Conferencing or Web Broadcasting.
20. 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.
21. I understand that unapproved system utilities and executable files are not allowed in my work areas or attached to emails.
22. I agree to comply with acceptable use policy of any other networks that I access.

Unacceptable use

Examples of unacceptable use include, but are not limited to:

- Logging in with another person's user ID and password, or using a machine left unattended, but logged in by another user
- Creating, transmitting, displaying or publishing any materials (text, images or sounds) that are likely to harass, cause offence, inconvenience or needless anxiety to any other persons.
- Authorised access to data and resources on the school network system that belong to other "users".

User action that would cause:

- Corruption or destruction of other users' data,
- Violate the privacy or dignity of other users
- Intentionally waste time or resources on the school network or elsewhere.

NETWORK SECURITY

If you discover a security problem, for example, being able to access other user's data, you must inform Mr Ashdown immediately and not show it to other users. Students identified as a security risk will be denied access to the network.

M Ashdown

Deputy Headteacher