The Weald
community school
and sixth form

STAFF E-SAFETY POLICY

Last review date:	September 2021
Next Review date:	September 2024
Approved by governing body on:	FGB 16th September 2021
Signed by Chair of Governors:	

THE WEALD SCHOOL - e-safety and ICT acceptable use policy for staff

School networked resources, including all shared drives (both cloud and local based), and Google Apps for Education, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the user's use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

CONDITIONS OF USE

Personal Responsibility Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the user to take all reasonable steps to ensure compliance with the conditions set out in this policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the Network Manager or school leader responsible for eSafety.

Acceptable Use Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the ethos of the school.

1. I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or cause needless anxiety to any other person 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 be calculated to incite hatred against any ethnic, religious or other minority group.

5. I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.

6. Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.

7. I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.

8. I will not trespass into other users' files or folders.

9. I will ensure that if I think someone has learned my password then I will change it immediately and/or contact Network Support.

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 will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the senior leadership team.

13. I am aware that email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous 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, receipt of inappropriate materials or filtering breaches/ unsuitable websites to the senior leader responsible for e-safety .

16. I will not use USB drives, portable hard-drives, tablets or personal laptops on the network without having them approved by the school and checked for viruses.

17. I will not attempt to visit websites that might be considered inappropriate or illegal.

18. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.

19. I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.

20. I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.

21. Damage to professional reputations can inadvertently be caused by seemingly innocent postings or images. I will monitor carefully access to my personal social network sites via lists of friends and third parties. I will be particularly vigilant with regard to those connected to my professional duties, such as parents of children at the school.

22. I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.

23. I will support and promote the school's e-safety and data security policies and help students be safe and responsible in their use of the Internet and related technologies.

24. I will not send or publish material that violates the Data Protection Act or breach the security this Act requires for personal data, including data held in SIMS.

25. I will not receive, send or publish material that violates copyright law. This includes materials sent / received using video conferencing or web broadcasting.

26. I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.

27. I will ensure that portable ICT equipment such as Chromebooks, iPads, laptops, digital still and video cameras are securely locked away when they are not being used.

28. I will ensure that any personal data (where the Data Protection Act applies) that is sent over the Internet (or taken off site in any other way) will be encrypted or otherwise secured.

The following expectations then apply when using BYOD (bring your own device) with students or as a member of staff:

1. Clearly state which tasks devices can be used for.
2. Clearly state when devices need to be turned off or put away.
3. Provide meaningful opportunities to use devices for feedback, collaboration, engagement and personal organisation.
4. Check how devices are being used to ensure everyone is safe and learning effectively.
5. Confiscate devices if necessary.
6. Take photos and videos of assignments only.
7. Use only the school wifi not 5G, 4G, 3G or other mobile data.
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.

The flowchart on the next page shows the steps that staff should take when actioning an e-safety incident.

What to do if a pupil or a teacher reports an e-safety incident