

Dorset Education Partnership



Computer Use, Internet Acceptance and WIFI Policy

Policy first adopted: 2010

To be reviewed every 3 years

Reviewed: May 2018

Reviewed: May 2021 (Revised
March 2023)

Reviewed

Reviewed

Reviewed

Reviewed

Reviewed

This Acceptable Computer, Internet and WiFi use Policy helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not. A copy of this policy can be obtained from our website at <https://fernup.dorset.sch.uk/wp-content/uploads/policies/non-statutory/Computer-Use-Policy.pdf>

Personal Responsibility

As a representative of the school, I will accept personal responsibility for reporting any misuse of the network to a staff member. Misuse is as described below.

Acceptable Use

The purpose of the school network including Internet access is to support research and education by providing access to unique resources and the opportunity for collaborative work. The use of your account must be in support of education and research and consistent with the educational objectives of Ferndown Upper School.

Users Shall Not Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Pornography (including child pornography)
- Promote discrimination of any kind
- Promote racial or religious hatred
- Promote illegal acts
- Any other information that may be offensive to colleagues.
- Use any other users account nor amend or delete any of their files or passwords.
- Install or attempt to install programs of any type.

Privileges

The use of the computer network and Internet **is a privilege, not a right** and inappropriate use may result in a cancellation of those privileges. The system administrators will deem what is inappropriate use and their decision is final. Also, the system administrators may deny, revoke or suspend usage of an account at any time as required. The staff may request the system administrator to deny, revoke, or suspend specific user accounts at any time. Use for personal financial gain, gambling, political purposes, playing games or advertising is not permitted.

Services

Ferndown Upper School makes no warranties of any kind whether expressed or implied, for the network service it is providing. Ferndown Upper School will not be responsible for any damages suffered whilst on this system. These damages include loss of data as a result of delays, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Users are recommended to make backups of their files on a regular basis using a suitable medium such as a USB memory stick. Use of any information obtained via the network or other information systems is at your own risk. Ferndown Upper School Specifically denies any responsibility for the accuracy of information obtained via its Internet services.

Network and E-mail Etiquette and Privacy

You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

1. Be polite. Do not get abusive in your messages to others.

2. Use appropriate language. Do not swear, or use any other inappropriate language.
Remember that you are a representative of the school on a global public system. You may be alone with your computer, but what you say and do can be viewed by others.
3. Illegal activities are strictly forbidden.
4. Do not reveal your personal address or phone numbers or that of fellow students.
5. Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
6. Do not use the network in such a way that you would disrupt the use of the network by other users. i.e. playing games, downloading music and inserting music or mobile devices into the USB port.
7. Anonymous messages and chain letters are not permitted.
8. The use of chat rooms is not allowed.
9. Other considerations:
 - Be brief. Few people will bother to read a long message. Proof read your message to ensure that it is error free and easy to understand and double check the recipients.
 - Remember that humour and satire are very often misinterpreted.
 - Respect the rights and beliefs of others.

Electronic Mail

Electronic mail (Email) is widely available via the Internet. Students are expected to use this facility in a responsible manner. The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden. Spamming (sending large volumes of an email to various recipients) could potentially overload the system and it will be looked on as a serious matter, warranting the removal of Internet or E-mail privileges for periods from 2 weeks to permanent removal.

Security

Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the network or Internet, you must notify the IT Services Department or your ICT teacher. Do not demonstrate the problem to other users. Do not use another individual's account under any circumstance. Attempts to logon to the network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network and Internet.

Vandalism

Vandalism of any IT resources may result in cancellation of all privileges. Vandalism is defined as any malicious attempt to damage or destroy any part of the computer system and network infrastructure, data of another user, or any Internet sites. This includes, but not limited to, the uploading or creation of computer viruses, the willful damage of computer hardware, whether connected to the network or not and the deletion of data from its place of storage. Do not attempt to fix anything yourself, please notify a member of the IT Services team who will carry out the necessary repairs.

Monitoring

The school may exercise its right to monitor the use of the school's computer systems, including access to web sites, the interception of e-mail and the deletion of inappropriate or non-educational materials where it believes unauthorized use of the school's computer system is or may be taking place.

Sanctions

Violations of these rules may result in the withdrawal of access to ICT resources, and may lead to disciplinary action as deemed appropriate by the School. Where applicable, police or local authorities may be involved, or other legal action taken.

Use of School Wi-Fi

Ferndown Upper School provides wireless Internet access across its site for staff, students and visitors. You are expected to use access to the wireless system and the Internet in a legal and responsible manner. By using the wireless network, the user acknowledges that he/she is subject to, and agrees to abide by all laws, rules and regulations applicable to Internet use. Students agree that they will bring devices with sufficient power and are strictly forbidden from charging devices using any power outlets on site.

Terms and Conditions of Use

Ferndown Upper School assumes no liability for any damage or loss as a result of using the wireless system. Ferndown Upper School's insurance policy does not cover any accidental damage to individual's devices. As such personal devices are used at the owner's own risk.

Security Considerations

Anyone using Ferndown Upper School's wireless network is forewarned that there can be no expectation of privacy when using the wireless network. Users assume all associated risks and agree that Ferndown Upper School and its employees do not accept responsibility for any personal information (e.g. bank details) that is compromised, or for any damage caused to users' hardware or software due to electric surges, security issues or consequences caused by viruses or hacking. All wireless access users should have up-to-date virus protection on their personal laptop computers or wireless devices, as well as staying up-to-date with applicable operating system security patches. Users of the WiFi system must install a security certificate to their device which allows our web filter to inspect the traffic to ensure it does not contravene what is deemed educational. Use of VPNs (Virtual Private Network) apps or websites are prohibited as they circumvent our filtering and security provisions. Users found to be using a VPN may face sanctions or a ban from the WIFI system.

Ferndown Upper School utilise the Netsweeper filtering solution provided by our ISP (School's Broadband). The Netsweeper filtering solution uses a security certificate installed on all devices (owned by Ferndown Upper School and users own devices when using the WiFi network). Users agree to the installation of this security certificate on to their own device to make use of the WiFi network. The security certificate's purpose is to be able to inspect secure traffic between a user's device and a website, app or service online thus allowing Ferndown Upper School to block or monitor web searches or requests for websites, apps or services. The certificate serves no other function and is not used for tracking and has no effect when the user's device is away from the Ferndown Upper School network.

Code of Conduct

Ferndown Upper School's Code of Conduct Policy applies to this service and any misuse will result in withdrawal of access for the individual(s) concerned and may result in disciplinary or legal proceedings.

I agree to comply with Ferndown Upper School's policy and will not create or transmit:

- (i) Any offensive, obscene or indecent images.
- (ii) Material which is designed or likely to cause annoyance, inconvenience or needless

anxiety.

(iii) Defamatory material.

(iv) Material that infringes the copyright of another person.

Any issues should be reported to the IT helpdesk. The wireless service may also be temporarily withdrawn at any time for essential maintenance without notice.