

Acceptable Computer, Internet, and WiFi Use Policy

This policy protects students, staff, and the school by clearly defining acceptable and unacceptable use of computer resources. A copy of this policy is available at on our website.

Personal Responsibility

As a representative of the school, I accept personal responsibility for reporting any network misuse to a staff member.

Acceptable Use

The school network, including internet access, is provided to support education and research by providing access to unique resources and opportunity for collaborative work. Users must ensure their activities align with Ferndown Upper School's educational objectives.

Users must not:

- Access, share, or create content related to:
 - Pornography (including child sexual abuse material)
 - Discrimination of any kind
 - Racial or religious hatred
 - Illegal activities
 - Material that may offend colleagues, staff or other students
- Use another user's account or modify/delete their files or passwords.
- Install or attempt to install programs of any kind without explicit permission from the relevant manager.

Privileges

Access to the computer network and internet is a privilege, not a right. Inappropriate use may result in loss of privileges, as determined by system administrators. Staff may request the denial, revocation, or suspension of specific user accounts. Personal financial gain, gambling, political activities, gaming, or advertising are prohibited.

Services Disclaimer

Ferndown Upper School makes no warranties regarding network service and is not responsible for damages, including data loss due to delays, errors, or service interruptions. Users should back up their files regularly using an appropriate storage device. Information obtained via the network is used at the user's own risk.

Network & Email Etiquette

Users must adhere to these guidelines when using the school computer systems:

1. Be polite; avoid abusive messages.
2. Use appropriate language; do not swear or use inappropriate terms.
3. Do not engage in illegal activities.
4. Protect personal information (e.g., addresses, phone numbers).
5. Understand that emails are not private and may be monitored.
6. Avoid disrupting network use for others (e.g., gaming, downloading music).
7. Do not send anonymous messages or chain letters.
8. Chat rooms are not permitted.
9. Additional considerations:
 - a. Be concise and proofread messages.
 - b. Recognize that humor and satire can be misinterpreted.
 - c. Respect others' rights and beliefs.

Email Use

Students must use email responsibly. Sending or receiving inappropriate content is strictly forbidden. Spamming (sending excessive emails) can overload the system and may result in a loss of privileges, ranging from two weeks to permanent removal.

Security

Security is a priority. Users must:

- Report security issues to IT Services or an IT teacher.
- Never use another person's account.
- Avoid attempting to log in as a system administrator.
- Understand that security risks or past misuse may result in denied access.
- Regularly change their password.

Vandalism

Intentional damage to IT resources, including creating viruses, hardware damage, or deleting data, may result in revoked privileges. Users must report issues to IT Services instead of attempting repairs themselves.

Monitoring

The school reserves the right to monitor computer use, including website access and email interception. Inappropriate or unauthorized use may result in content deletion.

Sanctions

Violations may result in revoked IT access and disciplinary action. Authorities may be involved if necessary.

Use of School Wi-Fi

Ferndown Upper School provides wireless internet for staff, students, and visitors. Users must abide by all relevant laws and regulations.

Terms & Conditions

- The school is not liable for device damage or data loss.
- Personal devices are used at the owner's risk.
- Users may not charge devices using school power outlets.

Security Considerations

- There is no expectation of privacy when using the school's WiFi.
- The school is not responsible for compromised personal information.
- Users must have up-to-date antivirus protection and security patches.
- A security certificate must be installed to allow web traffic inspection.
- VPNs (Virtual Private Networks) are prohibited. Use may result in sanctions or WiFi bans.

Web Filtering & Monitoring

Ferndown Upper School uses the Netsweeper filtering solution provided by our ISP (Internet Service Provider). This includes:

- Installing a security certificate on all devices using the Wi-Fi network.
- Filtering and monitoring website access to ensure educational appropriateness.
- Blocking unauthorized content and applications.

The security certificate does not track users and has no effect outside the school network.

Code of Conduct

The school's **Code of Conduct Policy** applies to WiFi use. Misuse may result in loss of access and disciplinary or legal action.

Users agree not to create or transmit:

1. Offensive, obscene, or indecent images.
2. Material causing annoyance, inconvenience, or anxiety.
3. Defamatory content.
4. Copyright-infringing material.

Issues should be reported to the IT helpdesk. The WiFi service may be temporarily unavailable for maintenance without notice.