Green Lea First School

Acceptable Use Policy

Date of review: November 2024

Next review: November 2026

All authorised users of the school's network, systems, information and communications equipment, devices and the data and information they process must comply with the schools Information Security Policy, this Acceptable Use Policy, related policies, and associated guidance.

It is your responsibility to read, understand, and adhere to the contents of these policies and guidance. If you are not clear about any policy requirements or guidance you must seek advice.

All school network, systems and services including internet, email, and messaging activity is logged for audit and monitoring purposes, including performance monitoring and to identify inappropriate use. You are responsible for all activity logged against your access credentials.

All users should be aware that there can be no expectation of privacy on the school's network, systems and services. By using the networks, systems and services including email and messaging services, and by using the school's data and information, users are agreeing to abide by the contents of the Data Protection Policy and the Acceptable Use Policy.

1. You must not, nor attempt to, bypass any security measures in place for the protection of the school's networks, systems, data and information.

2. You are solely responsible for the security of the ICT systems you are authorised to use along with any system passwords. All passwords must remain confidential and must not be shared with anyone else.

3. You must only access data and information that you are entitled to as part of your job role.

4. You are responsible for the security of the school's data and information wherever and however you are accessing it.

5. The school provides information and communications equipment, devices and access to systems for business purposes only. You must not store personal (non-school) data, documents or downloads on the school network, equipment, or devices.

6. Equipment and devices provided by the school must only be used by school employees or authorised third parties. Only encrypted USBs can be used to store any school work.

7. You are responsible for the creation, capture and appropriate management of all data and documents carried out under your account credentials on the school's systems.

8. You must not connect equipment or device(s) that have not been provided by the school to the school network unless you have explicit authorisation from the school (unless there are 'bring your own device' arrangements in place).

9. You must ensure that unattended equipment and devices are secure and rendered inaccessible.

10. You must not upload school data or documents to personal network storage sites, social media sites, or any other non-approved third-party locations.

11. You must not use a personal email account for school business. You must not forward school data or documents to your personal email account(s). You must not use a school email account for personal purposes except as permitted.

12. You must not access or distribute, nor attempt to access or distribute, illegal material or any material which may bring the school into disrepute.

13. You must not download or install any software, applications (Apps), or other forms of executable files from the internet, personal, or third-party storage locations.

14. You must report any incidents, misuse, security breach or suspicious activity, including suspicious emails. Deliberate failure to report, deliberately concealing an incident, or deliberately withholding information regarding a breach, or a suspected breach, may mean that you are subjected to disciplinary action.

If you deliberately or recklessly break any conditions in the Data Protection Policy or the Acceptable Use Policy, the school may:

- Restrict or remove access to email, internet or any other systems on a temporary or permanent basis
- Take disciplinary action against you (if you are staff)
- Take legal action against you (if you are a volunteer, contractor or other third party)
- Refer the matter to the Police if the matter is also a criminal offence

Or, a combination of these actions

Signed by all staff and new staff on induction