Acceptable Use (IT) Policy

RIDGEWAY EDUCATION TRUST

Approved by Trust Finance & General Purposes Committee:
06 November 2019

Review date: November 2022

Overview

This policy covers the proper use of the IT facilities and services owned and operated by Ridgeway Education Trust.

Definition

The phrase ‘IT facilities’ as used in this policy shall be interpreted as including any computer hardware, software or ICT service (e.g. Wireless Internet or Remote Access services) owned or operated by Ridgeway Education Trust.

Ownership

IT facilities owned by Ridgeway Education Trust (RET) and software and/or data developed or created by staff or students on that equipment remains in all respects the property of Ridgeway Education Trust.

Reporting

Breaches of this policy that occur in a RET secondary school must be reported to the PA to the Headteacher of the individual school, who will liaise with the Headteacher, Trust Director of Finance & Services and the Data Protection Officer.

Breaches of this policy that occur in a RET primary school should be reported directly to the Headteacher and School Business Partner.

Use of IT facilities

When using IT facilities Staff and Students must:

- Comply with the Online Safety Policy and GDPR guidelines.
- Keep personal passwords secret; staff and students must not share their personal password with others.
- Treat all hardware with the utmost respect and any damage or loss must be reported immediately. Any damage of equipment caused by malicious intent will be charged against the department responsible for that equipment/room (from there the cost may be passed onto the staff member, student or group involved).
- Use internet access for the purpose of performing duties; access to sites that do not support teaching and learning (e.g. games) are blocked by the web content filtering and any breaches of this are to be reported immediately. Reasonable use of the internet by staff for personal use is permitted during breaks/off duty hours.
- Not use IT facilities for business, fundraising, commercial or advertising purposes.
- Use only authorised software which has been preinstalled on PCs. Staff and students must not to attempt to download/install/run unauthorised software.
- Make no changes to the configuration (including location) of IT services or equipment, without the express authorisation of the IT Services Department.
- Not store confidential or sensitive data (e.g. student records) on portable media (e.g. USB memory sticks).

- Not attempt to gain unauthorised access to any data for which permissions is not granted or use the ICT facilities for malicious/illegal purposes that might bring the Trust or its schools into disrepute.
- Not attempt to access the account of another staff member or student.
- Not share (via email or other forms of communication) confidential or sensitive material with unauthorised persons. In the event that confidential or sensitive material is accidently shared it must be reported immediately.
- Not engage in any activity which is likely to result in damage to IT services, equipment or the reputation of the Trust or its schools.

Loan of hardware

Any staff member or student must follow the same policy when using loaned equipment at home. When offsite loan equipment is not covered by the Trust's insurance policy the staff member or student takes full responsibility for the replacement cost of the item of equipment in the event that it is lost, stolen or damaged. The staff member or student should also consider taking out insurance for the item of equipment and the IT Services department can provide advice on its value.

Monitoring

All staff and student activity when using IT facilities is logged and recorded to investigate suspected breaches of this policy. This monitoring may include (but is not limited to) live screen capture, recording of web browsing history, email/instant messaging/phone call transcripts as well as the contents of documents and files kept in user areas.

Breaches of policy

Any breach of this policy may be dealt with as a disciplinary or misconduct issue. Every user is responsible for the proper use of his/her equipment. The Trust is legally responsible for the content and nature of all materials stored on or accessed from its network and will take action against any illegal acts. In exceptional circumstances, where there are reasonable grounds to suspect that a staff member or student has committed a serious criminal offence, the police will be informed, and a criminal prosecution may follow.