REPTON

IT Acceptable Use Policy

Purpose

a) This policy is designed to protect pupils, staff, and the school. It is in accordance with the UK Computer Misuse Act, (1990), and any subsequent revision, and may be subject to change without notice.
b) This policy covers all Pupils, Staff, Teachers, Employees, Contractors, Volunteers, Interns, Casual workers, temporary and agency workers, and anyone who has access to our IT and communication systems, on any part of the school campus or via any means of remote access.
c) Our IT and communications systems include fixed devices, mobile devices and telephones and this policy applies whether or not the device or system in question is owned by the school.
d) Our IT and communications systems are intended to promote effective learning, communication, administration and working practices throughout our schools. This policy outlines the rights and obligations of Users, the standards that must be observed when using these systems, the circumstances in which we will monitor system use, and the action we will take in respect of breaches of these standards.
e) Misuse of IT and communications systems can damage our educational outcomes, pupil and staff wellbeing, our school, and our reputation. This policy is designed to ensure a clear, defined balance between the need for open communication and the protection of the school's pupils, staff, assets, and reputation.
f) The school takes compliance with this policy very seriously. Failure to comply could put pupils, staff, and the school at risk. Failure to comply with any requirement of this policy may result in disciplinary action up to and including dismissal (staff) or exclusion (pupils), and criminal proceedings.

Repton · Derbyshire · DE65 6FH
Charity number: 1093166 Company number: 04390219

Security and Passwords

a) You are personally responsible for the security of the equipment allocated to or used by you. You must not allow it to be used by anyone other than in accordance with this policy.
b) You should always lock or log-off from any electronic device when not in use, to prevent unauthorised access.
c) Users will not attempt to bypass security systems / internet filtering on school networks by any means.
d) IT and communication devices should always be kept secure. If you misplace or have any IT or communications device stolen, you must notify the Digital Development Manager immediately.
e) You will be held personally responsible for any activity carried out using your user credentials for any school system, which must therefore not be shared with anyone except for the IT support team (OLC), for the purposes of troubleshooting.
f) Additional passwords should be used where appropriate to secure access to sensitive / confidential information stored on electronic devices.
g) Users will not attempt to gain or use any password other than their own.
h) The school reserves the right to install / uninstall software on user devices at any time, as required by the Safeguarding team, compliance function, or HR department, without prior notice.

Internet / Network Access

a) All internet traffic via school networks / Wi-Fi is filtered and monitored to prevent access to content deemed inappropriate.
b) Any Internet connection outside the school network presents a higher risk to your personal information and may allow access to content not normally permitted in school.
c) Particular care should be taken to ensure pupil mobile devices (phones, tablets, laptops) with mobile data capability have appropriate controls set by parents / guardians.
d) School-owned devices must only connect to the Internet using school networks and must never be connected / tethered to mobile devices with data capabilities.
e) A separate network is provided for personal devices (mobile phones, tablets, laptops) which is subject to the same filtering / monitoring rules.
f) Users must not attempt to connect any networking device to the school network (network hubs / switches / wireless access points / wireless routers / wireless extenders / routers etc).
g) Users will not use the school Network to access, distribute or make available inappropriate material. For the avoidance of doubt, this includes any material that may be deemed illegal, offensive, discriminatory, in bad taste, immoral or in breach of copyright, in any format.
h) Users will not access school networks or the internet for fraud, financial gain, software

piracy, copyright infringement or any other malicious act.

i) Users will not make use of any type of file sharing technology for the purposes of sharing non-school related content.
j) Users must not add / remove / modify any hardware or software on school computers
k) Any additional software required in the pursuance of your studies / work must be requested from the IT support team (OLC), who will obtain academic / administrative guidance before any installations are undertaken.
l) Social Media is not deemed appropriate for use in school and is blocked from the main school network – please check with the Safeguarding team if you have a specific requirement. Certain sites may be permitted for specific use.

Electronic communication (email, MS Teams)

a) Users will not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic, or otherwise inappropriate emails or messages via any means of electronic communication. If you feel that you are being or have been harassed or bullied, or if you are offended by material received from a peer / colleague, you should inform your Housemaster or the Safeguarding team (pupils) or the HR department (staff).
b) School systems should not be used to access non-school email services (Hotmail, Gmail, Live, Yahoo, etc).
c) Users must not use electronic communication tools for the mass distribution of unsolicited messages and must not create or distribute materials which are designed or likely to cause annoyance, inconvenience, or needless anxiety.
d) Users must not forward messages to other people without first obtaining the original sender's permission.
e) Users must remember that any undertakings given by e-mail may be legally binding.

Legal Requirements

a) Users will accept full responsibility for the legality of all software installed on their devices.
b) Users will observe and adhere to the law on copyright and the General Data Protection Regulations (GDPR) at all times.

Enforcement, monitoring and privacy

a) Users agree to all monitoring and filtering by School systems while their devices are connected to the school network.
b) Where an alleged breach of this policy has occurred, or is reasonably suspected to have occurred, the IT support team are legally permitted to inspect electronic devices. This may involve confiscation of the device and inspection of the contents of a user's files or email messages, as defined in the Department for Education "Searching, screening and Confiscation (2018) guidance", which can be found here.

School Data

a) By following standard practice and ensuring any work is always created in and saved to the systems provided by the school (OneDrive, SharePoint, Outlook, etc) backups of work will be created automatically. Saving any data locally to a PC / laptop / Surface / USB drive / mobile phone or other device is strongly discouraged as this provides NO backup of your data and it is unlikely that you will be able to recover any work saved locally in the event of device failure.
b) Staff are reminded that school data should not be saved to any location outside school systems (Dropbox, iCloud, etc).

Personal Data

a) Personal data should always be backed up externally from school systems to an individual's personal choice of location (USB stick, external hard drive, Dropbox, iCloud, etc). The school does not back up personal files or any data not stored on school systems (OneDrive, Teams, etc). In the event of loss of this type of file, the school is under no obligation to attempt to retrieve / restore these files.

General Notes

a) Boarding pupils may only use electronic devices after bedtime with express permission to do so from the Housemaster.
b) Any comments on websites concerning the school or individuals representing the school should always be responsible, thoughtful, considerate and bring credit to the individual and the school.
c) Only those authorised by the Headmaster may participate on Wikipedia pages.

M. Shepherd - Digital Development Manager
October 2022