Priory School Network

Acceptable Use Policy

About this policy

All staff, governors and visitors using computers at Priory must follow this policy. It is designed to make sure that the network runs efficiently, everybody gets the best out of the school facilities, and all data is kept safe.

This policy is a basic guide, not an exhaustive list. In particular, staff and governors should also ensure that they are familiar with the school's Data Protection Policy and follow its associated procedures. If users are unsure as to whether something is acceptable, they should contact ICT Support in the first instance. As circumstances change – for example as new technologies come into use – this policy may undergo minor revision without further notice.

Although it is not school policy to systematically check material on the network (e.g. user areas, emails or internet history) it is not private and the school reserves the right to monitor any information on it for auditing, maintenance and security purposes.

Users must

- only log on as themselves, protect their password, and never give it to anyone else
- lock their computer if it is left logged on and unattended, whether in school or externally
- limit any personal use of the network to outside normal working hours
- report information security or e-safety incidents
- only use school systems to communicate with students online (e.g. school email)

Users must not

- allow anyone else to use their computer whilst they are logged on
- try to change computer system settings or tamper with connections
- access or attempt to access any areas other than those to which they have been authorised
- threaten the security of any computer systems, either local or remote
- store logon details of school systems externally e.g. in a browser on a home computer or in an app on a phone
- use public computers (e.g. libraries), public networks (e.g. café wifi) or shared logons (e.g. a family account) when accessing sensitive material such as student data
- create, search for, store or distribute inappropriate material (e.g. material that is defamatory, obscene, illegal or in breach of copyright)
- try to bypass the school's internet filter
- give out personal details of other users online
- deliberately waste resources such as network bandwidth

Please turn over

Bring Your Own Device (BYOD) e.g. laptops, tablets, smart phones

Use of a personal device in school carries unique risks such as access or theft by a student – so users must take particular care that their device does not have any sensitive data (such as network passwords or school emails) stored or cached on it.
Although the school does not actively monitor BYOD activity or the contents of connected devices, it reserves the right to inspect either for safety or security purposes.
The school cannot be held responsible for damage, loss, theft, malware infections or any costs incurred by the use of devices.
Users must report any theft of a device and change their passwords immediately if that occurs.

Devices must

- be password protected
- have antivirus software installed if appropriate
- have their software kept up to date e.g. with security updates
- be kept charged – chargers cannot be used in school
- be regularly checked for electrical safety

Devices must not

- be connected to the wired network
- be used to record audio, still images or video of anyone in school without their permission
- be used as a wireless "hotspot" without permission from ICT Support

---

Remote Learning

A ***Staff Remote Learning Acceptable Use Agreement*** with procedures relating to the provision of live or interactive distance learning is to be agreed separately.

Agreement

I have read and understood this policy and agree to abide by it.

I understand that

- breach of this policy may lead to sanctions including the removal of my access
- repeated or serious offences by staff could be viewed as a disciplinary offence up to and including dismissal
- if I do not comply with the relevant laws, the school may involve the police or local authority

Signed _____

Print name _____

Date _____