Boroughbridge High School and King James's School Federation

POLICY STATEMENT

Acceptable Use Policy Agreement

Policy last reviewed (date)	March 2025
Ratified by Governors (date)	March 2025
Next policy review due (date)	February 2027
Due for review by Governors (date)	March 2027
Staff Lead	Director of Business Services

MISSION STATEMENT:

This policy will support the school by being reflective of the Governors' direction and School's development plan. It will be used in an efficient and effective manner by ensuring that all members of staff are aware of their professional responsibilities when using any form of technology.

Significant revisions since the last review:

Added section regarding use of group/generic email accounts
Added section regarding access to school/department social media accounts

This agreement is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of technology. Technology relates to ICT systems, hardware, software, internet, email, learning platforms, web-based technologies, mobile devices, cameras, laptops and memory devices.

Members of staff:

- Must only use the school's technologies for professional purposes as outlined in this document. It is a criminal offence to use an ICT system for uses other than those permitted by its owner.
- Must not browse, download or send material that could be considered offensive, and should report any accidental access of inappropriate materials to their line manager. If a member of staff has need to access what might be considered inappropriate materials – for legitimate research purposes – then permission must be sought in advance from the school's Headteacher or Director of Business Services. Any such access must not be made when students are present.
- Have a duty to protect their passwords and email, network, Bromcom, Its Learning (online learning platform) and other school system login information, and should lock (Ctrl-Alt-Del) or log off the network and other systems when leaving a workstation or electronic device unattended. Personal passwords should be entered each time a member of staff logs on: passwords should never be remembered in automated log on procedures. The ICT technicians should be contacted immediately if a member of staff suspects that their password security may have been compromised.
- Must only access information on school servers through a controlled mechanism, with access granted on a need-to-know-basis/least privilege basis. Users should be vigilant when accessing sensitive or personal information to ensure that no one else, who may be unauthorised, may see the information.
- Should not attempt to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology**.**
- May be permitted to send and receive emails from group and/or generic email accounts. These accounts must not be used in a personal capacity and users must ensure they sign each email with their name so that emails can be traced to individuals. The IT Network Manager will have overall responsibility for allowing access to group emails but this may be devolved to other members of the IT support team.
- Must not install any software or hardware, with the exception of a printer driver for home use, without permission from an ICT/Network Manager.
- Must not sign up for any third-party software or trials that require the use of personally identifiable information of students or staff, i.e full name, school email, DoB, without first obtaining a completed Data Protection Impact Assessment (DPIA) from the schools

IT/Network Manager.

- Should ensure, in accordance with the General Data Protection Regulations 2018 that all personal data of pupils, staff or parents/carers is kept private and secure, and is not held longer than outlined in the schools Document Retention Policy. Any data which is being removed from the school site should be encrypted using school approved methods. For this purpose staff laptops have an encrypted hard drive and encrypted memory sticks are available from the ICT technicians. Personal data sent over the internet should use the NYC approved systems.
- Should password protect any portable device that is used to access e-mails or to collect assessment information. These devices should not be used by pupils. Theft of such devices must be reported to the ICT/Network Manager immediately.
- Should use only school equipment to create digital images, video and sound for school use. Should only take and use digital photographs and videos in accordance with the policy communicated to parents annually. Images of pupils should be used only within school electronic systems and should not be made public, e.g. by posting on the internet, without permission of the school's Headteacher and express permission of the parents. Current consent status for the use of pupil photographs is viewable within Bromcom.
- Should ensure that their use of web-based technologies, including social networking sites, such as Facebook, X, Tik-Tok etc. does not question or bring their professional role into disrepute. Staff should be aware that once posted online, by themselves or others, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
- Should ensure that they are aware of, and compliant with, the Social Media Policy.
- Nominated users may be given access to school/department social media accounts across multiple platforms. Those authorized will be given the usernames and passwords of the account(s) which must not be disclosed to any other individual within or external to the school. Any posts made on these platforms must comply with the schools Social Media Policy and GDPR policy.
- Should only communicate with pupils using the appropriate LA/school learning platforms or other electronic systems. They should not communicate with pupils, in relation to either school or non-school business, using personal accounts using web based or electronic technologies.
- Must only use approved, secure school email systems for any school business.
- Are not permitted to contact or communicate with pupils, parents or conduct school business using personal email addresses or telephones, without specific permission from the school's Headteacher.
- Should not give out their own personal details, such as telephone/mobile number.
- Should only use a school mobile phone for school duties**.** Where a member of staff has to use their own phone in an emergency they should use their own device and hide (by inputting 141 before) their own mobile number.
- Must ensure that all electronic communication with pupils and staff is compatible with their

professional role. E-mails sent to an external organisation should be written carefully, and reviewed, before sending, in the same way as a letter on school headed paper.

- Must not click on links in emails from un-trusted or unverified sources.
- Must respect and comply with copyright and intellectual property rights.
- Must promote and model positive use of current and new technologies and e-safety.
- Can access information about e-safety on the schools document sharing site.
- Should report any suspected damage to the ICT system due to virus or malware to the ICT technicians immediately any suspected damage to a school system.
- Should report all incidents of concern regarding children's safety online to the designated child protection coordinator as soon as possible.
- Must not make video or audio recordings (e.g. recording a teaching session), or take digital images of other members of staff without the express, prior permission of those staff.

User Signature

The school may exercise its rights to monitor use of its information systems, including internet access. I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy

Signature …….

Date ……..

Full Name (Printed)…….