Banovallum School

Acceptable Use Policy (Staff)

Reviewed September 2020

Banovallum School

Acceptable Use Policy

Introduction

The computer system at Banovallum School is the property of the School and is a resource shared by all Staff and Students. Computer facilities, including mobile units, are made available to further education and for staff to enhance their professional activities. The School's Acceptable Use Policy has been drawn up to protect all parties – the Students, Staff and the School.

All users are reminded that internet and email activity may be monitored. This policy applies to all devices, including personal ones and to all access be it through the school network or other methods such as 3G.

We filter to ensure:

(as much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
(as much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

We monitor for assurance

(as much as possible) that no inappropriate or illegal activity has taken place. To add to any evidential trail for disciplinary action if necessary.

Key Points

The School reserves the right to examine or delete any files, including emails, that may be held on its computer network systems and to monitor or restrict access to any Internet sites visited.

- All Internet activity should be appropriate to Staff professional activity or Student education.
- Access to the School servers and the Internet should only be made via the user's authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the School ICT systems or that attacks or corrupts other systems is forbidden.

- Users are responsible for all e-mail sent and as such should not forward any material that may be deemed inappropriate or offensive. In addition, users are responsible for contacts made that may result in e-mails being received.
- All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.
- Email is provided primarily for business use, however reasonable personal use is allowed provided it remains professional, responsible and appropriate
- Copyright of materials must be respected
- Use for personal financial gain, gambling or political purposes is forbidden
- Use of the network to access inappropriate materials is forbidden
- Users are not to visit, use, download, or store any game (either application or browser-based), music or videos without permission of a member of ICT or supervising teacher, and then only for educational purposes.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for Students. The school will take all reasonable precautions to ensure that users access only appropriate material. The school will block access to social networking sites. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The School will not accept liability for the material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Should any of these points be broken the School reserves the right to remove any individual from the School Network.

ICT Equipment Use

Users will:

- Report any accidental infringement of the above conditions to the ICT Staff.
- Treat all equipment with respect.
- Lock away laptops and other portable equipment when leaving them unattended.
- Staff will ensure classrooms are locked after each lesson.
- Leave the public work areas tidy.
- Ensure equipment is shut down and switched off overnight.
- Ensure that they have either locked the computer or logged out of their session before leaving the computer unattended.
- Ensure that when taking a school laptop home, it is kept secure and out of sight, e.g. when travelling by car, the laptop should be locked in the boot or hidden from view.
- Be responsible for any costs incurred as a result of the laptops being damaged/lost through their negligence.
- Ensure all school laptops are stored securely at the end of the school day.

Users will not:

- Divulge their password to anyone other than a member of the ICT Support team.
- Allow any other person the use of a computer to which they have logged on.
- Leave the computer unattended whilst logged on.
- Install software of any kind on any computer owned by the school without the expressed permission of the Network Manager.
- Copy any software from any computer owned by the school.
- Delete any software from any computer owned by the school.
- Change the configuration of any computer owned by the school.
- Attempt to enter any restricted area for which they have not been granted access.
- Store undesirable material on any part of the system (offensive literature, pornographic images etc.).
- Attempt to repair any ICT equipment owned by the school.
- Leave laptops or other portable equipment unattended and vulnerable to theft.
- Attempt to introduce a virus or malicious code to the network.
- Attempt to bypass network or system security.
- Attempt to access another user's account.
- Attempt to use any form of hacking/cracking software or system.
- Use or attempt to use a Virtual Private Network (VPN)
- Connect any device to the network that acts as a Wireless Access Point (WAP), bridge or router.
- Connect any device to the network that has access to the Internet via a connection not provided by the school. (e.g. via a dongle/modem provided by a mobile phone network provider).
- Physically damage or vandalise any computer equipment.
- Access, download, create, store or transmit material that is indecent or obscene, could cause annoyance or offence or anxiety to others, such as: material that promotes discrimination of any kind, including material that promotes intolerance on the basis of gender or sexual orientation; promotes racial or religious hatred; promotes illegal acts; promotes drugs and substance abuse or shows graphic portrayal of violence or self-endangerment, or contain instructions for making weapons of violence or the sale of such weapons, infringes copyright or is unlawful, brings the name of the school in to disrepute.
- Send or display offensive messages or pictures
- Use obscene language
- Bully, harass, insult or attack others
- Violate copyright laws
- Engage in activities that waste technical support time and resources
- Engage in any activities deemed unacceptable by the Senior Leadership Team and Governors: if in doubt, refer, at all times to the Staff Code of Conduct
- Any breaches will be dealt with by the Headteacher in accordance with the Staff Discipline Policy and Staff Code of Conduct