Brownhills School

Staff Electronic Devices Policy

Review PT/ September 19

Contents

Statement of intent

Brownhills School accepts that personal electronic devices are widely used by staff members.

As a school, we must have a sensible and practical response. We understand that these devices are carried by staff members; however, this policy is intended to ensure:

- That staff will be responsible users and remain safe while using the internet.
- That school ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- That staff are protected from potential risk in their everyday ICT use.

ICT can enhance work, learning opportunities and enable people to be creative. In return, staff members need to agree to be responsible users.

1. Key roles and responsibilities

1.1. Brownhills School governing body has overall responsibility for the implementation of the policy and procedures of Brownhills School.

1.2. Brownhills School governing body has overall responsibility for ensuring that this policy, as written, does not discriminate on any grounds, including but not limited to: ethnicity/national origin, culture, religion, gender, disability, or sexual orientation.

1.3. Brownhills School governing body has overall responsibility for reviewing this policy annually.

1.4. The headteacher has responsibility for handling complaints regarding this policy as outlined in the school's Complaints Policy.

1.5. The headteacher will be responsible for the day-to-day implementation and management of the policy and procedures of Brownhills School

2. Acceptable use policy agreement

I understand that I must use the school's ICT systems in a responsible way whether in school, or at home. Even when I am using my personal device for work activities, I will ensure that my use is responsible. I recognise the value of using ICT to aid learning for my pupils, and I will, where possible, educate my pupils in the safe use of ICT and embed e-safety in my work with them.

2.1. For my professional and personal safety, I understand that:

- The school will monitor my use of the ICT systems, email and other digital communications.
- The rules set out in this agreement also apply to the use of school ICT systems (e.g. laptops, email, virtual learning environment (VLE) etc.) out of school.
- The school ICT systems are primarily used for educational use, and that I will only use the systems for personal or recreational use within the policies and rules set out by the school.
- I must not disclose my username or password to anyone else, or use anyone else's.
- I must immediately report any illegal, inappropriate or harmful material or incident that I become aware of, to the appropriate person.
- When using my personal electronic devices in school, I will follow the rules in this agreement in the same way as if I was using the school's ICT equipment. I will additionally ensure that all my devices are protected by up-to-date anti-virus software and are free from viruses.
- I must not open any attachments to emails unless the source is known and trusted.
- My data needs to be regularly backed up, in accordance with the school's policies.

- I must not try to upload, download or access any materials which are illegal, inappropriate, or may cause harm or distress to others. I will not use any programmes or software which may allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I must not download or upload large capacity files without permission.
- I must not install programmes of any type on a machine, store programmes, or alter computer settings unless it has been sanctioned by the Senior IT Technician.
- I must not damage school's/other people's equipment.
- All data I have access to must be kept private and confidential, except when I am required by law/school policy to disclose such information to an appropriate authority.
- I must report any damage or faults involving equipment or software.

2.2. I will be professional in my communication and action when using school ICT systems by:

- Not accessing, copying, removing or altering any other user's files without their permission.
- Communicating with others in a professional manner.
- Ensuring I only take and publish photos of people that have given me their permission to do so, and I am in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. If images are posted on the school website/VLE, I will have sought and received permission from the pupil and/or parents/carers.
- Ensuring I do not use social media websites, in accordance with the school's policies.
- Communicating with pupils/parents/carers using only the official school systems, and ensuring the manner in which I speak is professional.
- Not engaging in any online activity that may compromise my professional responsibilities.
- Ensuring that I have permission to use the original work of others in my own work.
- Not downloading or distributing copies of copyright-protected work.

2.3. Finally, I understand that:

- This policy applies not only to my work and use of school ICT equipment in school, but the use of school ICT systems and equipment out of school, and my use of personal equipment in school or in situations related to my employment by the school.
- If I fail to comply with this policy, I could be subject to disciplinary action.

3. Portable and mobile ICT equipment

3.1. All activities carried out on school systems and hardware will be monitored in accordance with the school's policies.

3.2. Staff must ensure no school data is kept on personal devices.

3.3. Synchronise all data with the school server on a regular basis.

3.4. Staff must ensure all devices are made available for anti-virus updates and software installations, patches or upgrades.

3.5. Electronic devices must not be left unattended, and must be kept out of sight where possible.

3.6. Portable equipment must be transported in its protective case, if supplied.

4. Personal mobile devices (including phones)

4.1. Staff members must not contact pupils or parents/carers using their personal device.

4.2. Technology may only be used for off-site educational purposes when mutually agreed with the headteacher.

4.3. The school is not responsible for the loss, damage or theft of any personal mobile device.

4.4. Inappropriate messages must not be sent to any member of the school community.

4.5. Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

4.6. Users bringing devices into school must ensure there is no inappropriate or illegal content on the device.

4.7. During lesson times, mobile phones must be kept in a lockable cupboard housed in the staffroom or classroom.

5. School-provided mobile devices (including phones)

5.1. Inappropriate messages must not be sent to any member of the school community.

5.2. Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

5.3. Where the school provides mobile technologies, such as phones, laptops and PDAs for off-site visits and trips, only these devices should be used.

6. Removable media

6.1. Only use recommended removable media.

6.2. Store all removable media securely.

6.3. Removable media must be disposed of securely by the Senior IT Technician

7. Cloud-based storage and work systems

Brownhills School is aware that data held in remote and cloud-based storage is still required to be protected in line with current GDPR legislation. Brownhills School's staff members must ensure that even cloud-based data is kept confidential and no data is copied, removed or adapted.

GDPR Compliance

ICT Devices - Staff Emails

Devices such as mobile phones & tablets must have at least 2 levels of authentication/security in order for Staff to access their School emails.

If a member of Staff requires School email on their device they must see a member of ICT Support.

USB Sticks & Portable Hard drives

Any files E.G. Word documents etc… with Student/Staff details/information on must be password protected. If a member of Staff is unsure how to do this they must see a member of ICT Support.

Data Protection Officer

The Data Protection Officer is responsible for overseeing data protection within the School so if you do have any questions in this regard, please do contact them on the information below: -

Data Protection Officer: Craig Stilwell

Company: Judicium Consulting Ltd

Address: 72 Cannon Street, London, EC4N 6AE

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0203 326 9174