USE OF PERSONALLY OWNED ICT DEVICES BY STAFF (BYOD)

Reviewed and updated: March 2022
Next review: March 2025
Status: non-statutory

This policy should be read in conjunction with a useful guide issued by the Information Commissioner's office – Data Protection Act – Bring your own device (BYOD).

This policy should also be read in conjunction with CEFM's other ICT related policies:

- Internal data security.
- Management and retention of records.
- E-safety (useful for legal references).
- ICT and use of the internet and intranet by staff.
- Social media.
- Staff email.
- Staff professional identity protection.

Background

ICT is a vital tool in the administration of the school. Increasingly, teachers and support staff are needing to use their own personal devices, as well as the network of devices owned by the school, to support their work. This trend is known as 'Bring your own device' (BYOD) and involves the use of mobile devices such as smart phones, laptops and tablets.

Teachers and support staff need to be aware of what is acceptable to the school when using their own devices, particularly when dealing with confidential matters and any data which is covered by the Data Protection Act and the General Data Protection Regulation (GDPR) for which the school data protection officer is ultimately responsible.

USE OF PERSONALLY OWNED ICT DEVICES BY STAFF (BYOD)

AT ELTHORNE PARK HIGH SCHOOL

ALL OUR SYSTEMS ARE CLOSELY MONITORED

Introduction

This policy is in place for the occasions when staff use their own ICT equipment when dealing with data belonging to the school.

There is a small network of computers which are used in the administration of the school (finances, pupil records, timetables, registers etc). Many more computers are available for use by pupils and staff and the majority of these have access to the internet through the school network. All pupils and staff have a login name, password and an email account.

The email system is available for use both from within the school and externally using a web browser. There are specialist centres serving design, mathematics and science together with general purpose rooms. A growing number of other computers are located within individual departments/classroom areas.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's internal data security policy and as required by the General Data Protection Regulation (GDPR).
- Logs are maintained of access by users and of their actions while users of the system.

When staff use their own devices (e.g. laptops, tablets, smartphones) it is imperative that:

- The protocols already in use are maintained.
- No vulnerabilities are introduced into the school's existing secure environments.
- Data protection matters are complied with.

Any queries regarding this policy should be addressed to the headteacher.

Objectives and targets

The objective of this policy is to develop an appropriate code of practice for the use of ICT by staff at Elthorne Park High school when using their own devices (BYOD).

Action plan

The following code of practice must be adhered to by staff who have the privilege of using BYODs to carry out their work. Not all staff will have this privilege.

All staff who are permitted to use BYOD at Elthorne Park High school are expected to have read, understood and abide by the following school policies:

- Internal data security.
- E-safety (useful for legal references).
- Management and retention of records.
- ICT and use of the internet and intranet by staff.
- Social media.
- Staff email.
- Staff professional identity protection.

They are expected to sign the acceptable BYOD usage agreement – see appendix – to ensure that they understand their responsibilities. They will also have signed the acceptable computer usage agreement and, if they have received any portable ICT equipment which is the property of the school, they will also have signed the acceptable portable ICT equipment usage agreement.

All BYODs must have appropriate security in place, including anti-virus protection, and it must be updated regularly. It is the staff member's responsibility to ensure this.

Periodic audits and checks on compliance will be undertaken by the school's network manager, who is also available to offer guidance on what is and is not acceptable use of BYODs.

Handling personal data (where Data Protection Act and GDPR apply)
Any sensitive information held on BYODs and relating to the school must be accessible only by a password, PIN or encryption. This is to prevent personal data relating to school matters being accidentally or deliberately compromised or accessed by anyone other than the member of staff. This also applies wherever data is stored (e.g. on the device, portable hard drive, memory card, SD card, intranet or cloud). Such data may include:

- Information relating to staff, e.g. performance reviews.
- Pupil reports.
- SEN records.
- Letters to parents.

- Class-based assessments.
- Exam results.
- Whole school data.
- Medical information.

Care should always be taken to log out after each session to ensure that unauthorised access is not possible, e.g. in the event of the device being lost or stolen.

Members of staff should speak to the network manager about whether an encrypted channel (e.g. VPN or HTTPS) could be set up to offer better security when transferring data of a secure nature from a BYOD to the school's network. Similarly, before using BYODs in cafes, hotels etc staff should seek advice from the network manager about the safety of such operations.

Where personal data relating to the school is stored on the BYOD, it should be deleted safely and securely as soon as it is no longer required. This also applies to data held on removable media e.g. USB drives.

When a member of staff leaves the employment of the school, she/he will be requested to remove all school-related data from any BYODs, having previously ensured that the school retains the data.

Handling other data relevant to the school
Where a BYOD is used for work purposes that do not involve personal data (and therefore have data protection implications) it is appropriate to maintain a clear separation of the work on the device from work which is of a confidential nature.

It is still important that school-related non-sensitive data held on BYODs must be accessible only by a password, PIN or encryption. This is to prevent data relating to school matters being accidentally or deliberately compromised or accessed by anyone other than the member of staff.

It is essential that any data not relating to school matters cannot be accidentally or deliberately uploaded to any device belonging to the school.

It is essential to be careful when installing any third-party software onto a BYOD. Untrusted sources have the potential to contain malware which could compromise any personal material belonging to the school. If in doubt, consult the network manager before uploading.

Members of staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Any images must only be taken on school equipment, never on personal equipment.

Misuse of BYODs by staff
Misuse or abuse of the facility to use BYODs by staff is a serious matter and will be dealt with under the school's disciplinary procedures. The penalties for improper use may include dismissal either with or without notice.

Monitoring and evaluation

All use of BYODs at Elthorne Park High school is a privilege. The headteacher may request access to personal devices if the senior management team considers that this policy has been contravened, in order to investigate alleged abuse. The policy itself will be monitored and evaluated regularly, taking

into account, any incidents which occur or technological developments which might need a change in the policy.

Reviewing

The efficacy of the policy will be discussed annually as part of the governors' rolling programme of reviews.

Next school review due: March 2025

APPENDIX

ACCEPTABLE BYOD USAGE AGREEMENT

- I understand that anyone other than myself must never have access to any sensitive data held on the BYOD.
- I understand that I am responsible for the safety of sensitive school data that I use or access.
- All personal data is subject to the General Data Protection Regulation (GDPR) and if I am in any doubt as to the sensitivity of data I am using, I will refer to the school's internal data security policy, and to the data protection officer if still unsure. I understand that if an incident is considered to be a breach under the Data Protection Act or the GDPR this may require investigation by the Information Commissioner's Office and heavy financial or other sanctions could apply to the school.
- I will always adhere to copyright.
- I will always log off the system when I have finished working.
- I will only access the school's systems with my assigned login name and registered password.
- Passwords that I use to access school systems will be kept secure and secret.
- If I have reason to believe my password is no longer secure, I will change it immediately. I will inform the network manager as soon as possible so that any access with my old password can be monitored and appropriate action taken.
- When I leave the school's employment, all data relating to the school will be returned to the school.
- I understand that when in school and not being used, the BYOD must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.
- I understand that, whenever possible, the BYOD must not be left in an unattended car. If there is a need to do so, it will be locked in the boot.
- I will check that the BYOD is covered by my normal household insurance, whether in England or abroad.
- I understand that I have the responsibility to ensure the virus protection software that has been installed is kept up-to-date. I also understand that I must *always* follow the virus protection procedures as directed by the school's network manager to ensure virus protection is always kept up-to-date.
- I will follow the guidance provided by ICT support staff to ensure the anti-virus protection on my BYOD is kept up-to-date.
- If I use removable media I will ensure that this has been carefully checked to ensure it is free from any type of virus.

- I understand that I may load software onto the BYOD but it must:
  - Be fully licensed.
  - Not corrupt any software or systems already installed on the BYOD.
  - Not affect the integrity of the school networks when connected to either the curriculum or administration networks.
- I will check with the network manager/technician should I need to install additional software.
- I will always adhere to the following associated school policies:
  - E-safety (useful for legal references).
  - ICT and use of the internet and intranet by staff.
  - Use of personally owned ICT devices by staff (BYOD).
  - Management and retention of records.
  - Internal data security.
  - Social media.
  - Staff email.
  - Staff professional identity protection.
- I understand that the school may monitor my BYOD activity.
- I understand that members of staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. I understand that such images must only be taken on school equipment, never on personal equipment.
- I understand that activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- In order to maintain the security of data, I will take the following steps:
  - I will store data only for as long as is necessary for me to carry out my professional duties.
  - If I need to transfer data files, I will only do so using encryption as advised by the network manager.
  - I will not use email to transfer data files but save them to the school network area if other staff need access to the information.

I understand that if I do not adhere to these rules outlined in this agreement, my privilege of working with the BYOD could be suspended and other disciplinary consequences may follow, including notification to professional bodies, where appropriate.

If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may require investigation by the police and could be recorded on any future criminal record checks. Breaches of the GDPR may cause the school significant financial penalties.

Name……(please print your name)

Signed ……(please sign your name)

Date……..