CHELMSFORD LEARNING PARTNERSHIP

TECHNOLOGY ACCEPTABLE USE POLICY (STAFF, GOVERNORS AND TRUSTEES)

March 2019

Committee Responsible	Board of Trustees
Lead Member	CEO
Approved by	Board of Trustees
Date Approved	25th March 2019
Version	1
Review Date	Spring 2021
Staff Consultation Date	6th March to 20th March 2019

Building Futures Inspiring Success

Barnes Farm Junior School

Roding Valley High School

THE Beaulieu Park SCHOOL

THE Boswells SCHOOL

Contents

INTRODUCTION

1.1. The Trustees are committed that members of staff within the Trust use computer and mobile technology to aid student learning and enable them to carry out their work as effectively as possible. This policy is designed to make clear the responsibilities of staff with regard to the use of the Trust computers, hardware and facilities.

1.2. This policy fulfils the requirements that technology paid for from the public purse is used judiciously.

1.3. This policy applies to all staff within the Trust who are on, or remotely connected to, a school or trust site/network and to those allowed access to the school or trust's resources.

ROLES AND RESPONSIBILITIES

RESPONSIBILITIES FOR ICT USAGE

2.1. In relation to ICT usage, the Network Manager or nominated person is responsible for:

- ensuring that staff can use ICT equipment safely;
- putting systems in place to identify staff training needs;
- recommending any improvements to the environment in which ICT is used (for example, furniture, lighting, and ventilation).

RESPONSIBILITIES OF STAFF

2.2. Staff have a responsibility to comply with the following usage policy:

2.2.1 Laptops, tablets or mobile devices that are provided for staff use should never be used by students. Staff are permitted to use classroom ICT equipment when it is not required by students.

2.2.2 Staff have access to their school's network, internet and e-mail and must ensure they use it appropriately and within the parameters of this policy, Data Protection Policy and Staff Code of Conduct Policy.

2.2.3 Staff must ensure they only use data available to them for the purposes it is intended and within the parameters of their job role (Computer Misuse Act).

2.2.4 Equipment (laptops, tablets, mobile devices etc) provided to staff by the trust remains the property of the trust and must be available for inspection at all reasonable times.

2.2.5 Software has been installed to monitor all usage of each school network by students, Trustees, governors, staff and the wider community. Staff should also be aware that computers "leave a trail" of documents worked on, websites visited, e-mails sent/received, etc. and must consider how they use the Trust equipment and software.

2.2.6 In order to comply with the General Data Protection Regulations, it is imperative that staff use strong passwords for their network, SIMS and other logons and change them on a regular basis. Staff must not disclose their password to anyone nor should they log on using anyone else's password. When leaving a computer that is logged on, staff must lock the computer every time.

2.2.7 Staff will only use personal mobile devices during out-of-school hours and break and lunch times. Staff will ensure that mobile devices are either switched off or set to silent mode during school hours. There will be exceptional occasions where staff need to take/make personal calls during the school day (family emergency, domestic emergency etc) and the use of personal mobile devices are permitted in these circumstances.

2.2.8 Staff will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content. Under no circumstances should members of staff undertake any unlawful, libellous, immoral or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material. If such material is accessed by accident, the individual member of staff must report the incident to the Network Manager or nominated person. Evidence of visits, the downloading of materials, and the use of search criteria (i.e. individual words) that might lead to inappropriate sites, will be treated as a disciplinary matter.

2.2.9 Staff must adhere to the procedures for reporting any e-safety concerns to their network manager/Headteacher

2.2.10 Staff must report to the Network Manager or designated person immediately if they believe they have access to data they should not have.

2.2.11 Staff laptops and desktops may only have Trust licensed software installed, this will need to be completed by the IT Network Team and a register of installed software maintained. Staff may not install personal software on school or trust laptops and desktops.

2.2.12 Staff with personal accounts on social media websites, e.g. Facebook, must not be "friends" with students or use this as means to communicate with students. Past students should be off roll for a minimum of two years and be over the age of 18 before there is any social media contact to protect the staff member.

2.2.13 Staff will ensure that they apply the necessary privacy settings to any social networking sites to ensure students, parents do not have access to personal information relating to staff.

2.2.14 Staff will not publish any comments or posts about their school or the academy trust on any social networking sites which may affect the trust's reputability. Staff will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.

2.2.15 Staff will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.

2.2.16 In line with the above, staff will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.

2.2.17 Staff will not give their home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels. Where there are Home-School Liaison workers employed in schools (or staff with similar roles) it is acceptable for them to pass their work mobile number to families

2.2.18 Staff with personal accounts on social media platforms, (e.g. Facebook) or messaging platforms (e.g.Whatsapp) must not discuss work, school or trust issues, regardless of the nature of these discussions. It is accepted, however, that staff may use a Whatsapp group as a method of keeping each other informed about urgent matters (school closure etc) . In these circumstances it is acceptable for staff to use Whatsapp and to discuss operational matters relating to work. Staff using Whatsapp in this way should take into account Section 2.2.8, 2.2.14 and 2.2.15 of this policy.

2.2.19 Staff must never make reference to or name an individual child, family member of that child, colleague, governor or trustee on any social media platform or messaging platform.

2.2.20 Staff must ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal or sensitive data taken off site must be encrypted.

2.2.21 Staff will respect copyright and intellectual property rights.

SCHOOL/TRUST E-MAIL

3.1. E-mail communications are no different to any other form of written communication and are legally binding.

3.2. E-mails must not contain personal data, if personal data is sent via e-mail it must be in an encrypted and password protected document attached to the email, the password should be sent separately and ideally by another method i.e. SMS messaging.

3.3. The e-mail system is the property of the Trust and content will be monitored. The system is not for personal use. Deleting an e-mail will not remove all instances of that message.

3.4. Each school will keep and archive of all emails.

3.5. The e-mail system must not be used inappropriately. Staff must not solicit e-mails that are unrelated to the school's educational, academic, curriculum activities or for personal gain. In addition, they are not permitted to send or receive any material that is obscene, defamatory or which is intended to annoy, harass, and intimidate or waste the time of another person, and personal opinions must not be represented as those of the Trust.

3.6. Staff must not send personal data to countries outside the European Economic Area without the agreement of the Information Compliance Unit.

3.7. Staff must have regard to the security of their accounts and, under no circumstances, are they to pass on their user name/password or log in details to any third party. This particularly applies to 'phishing' emails. Staff will delete any chain letters, spam and other emails from unknown sources without opening them and will not enter their log in details in response to these spam/phishing email.

3.8. Staff must not use their personal e-mail accounts for school business and must not use school accounts for personal business or personal communications

ACCESS TO E-MAIL ACCOUNTS ON DEPARTURE

3.9. Entitlement to access an individual's e-mail account will automatically cease on the date on which an individual's relationship/contract with the Trust terminates.

CONFIDENTIALITY

5.1. The Trust holds information about ICT usage (including access to the internet, network and emails). This information will only be used with the consent of the Senior Team or within an investigation.

5.2. Staff are reminded that ALL information is confidential to the school and they must treat all data appropriately. Staff must ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal or sensitive data taken off site must be encrypted.

5.3. Staff will respect copyright and intellectual property rights.

ACCEPTABLE USE

6.1. Responsible use of ICT resources and the internet by staff is permitted and encouraged where such use is suitable for academic and educational purposes and supports the objectives of the Trust and its curriculum activities.

6.2. The internet connection provided by the school should not be used for anything other than school-sanctioned browsing; staff must not waste time, resources and bandwidth on non-school activities.

6.3. Use of the internet may be subject to monitoring for security and network management reasons. Users may also be subject to limitations on their use of such resources.

6.4. The distribution of any information to external sources is subject to the scrutiny of the Trust or school and the Trust reserves the right to determine the suitability of this information. Inappropriate use will be dealt with under staff discipline and dismissal procedures.

6.5. The use of computing resources is subject to UK law and any illegal use will be dealt with accordingly.

6.6. You must check any computer for which you are responsible (e.g. laptop) to ensure that critical updates and anti-virus updates are being implemented and that they are up to date.

6.7. Staff are forbidden from uploading, downloading or otherwise transmitting software of any kind to the school or trust's computers or network areas, tampering with, or causing damage to, any hardware or software so as to impede its use.

SECURITY

7.1. Staff are not permitted to intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high-volume traffic that substantially hinders others in the use of the network.

7.2. Access is denied to any areas of the school network, other than those specifically created for staff and students to save/obtain work.

7.3. Staff must have explicit authorisation to examine, change, or delete another person's files.

7.4. Staff must comply with the ICT system security and not disclose any passwords provided to them by the school or other related authorities.

DATA PROTECTION

8.1. Please refer to the separate Data Protection Policy for full details.

8.2. The use of portable media to store Trust/school-related data is prohibited. This refers to any data that includes personal information about students, staff or information that might bring the Trust's name into disrepute.

8.3. You must not **disclose** (in writing, speech or electronically) information held by us unless you are authorised to do so, and the recipients are authorised to receive it.

8.4. When you print, photocopy, scan or fax personal data, you must not leave the information **unattended.** Take the utmost care that you are sending to the correct recipient. For other devices, if there is no secure release facility which requires you to be present, you must ensure you wait for the process to complete and remove any originals and copies from the equipment.

8.5. Staff must not make personal use of the information available to them that is not available to the public.

GENERAL

9.1. The Network Manager or designated person reserves the right to identify any other inappropriate uses, in respect of the above points.

9.2. The Trust also retains the right to report any illegal violations to the appropriate authorities. There is a procedure for dealing with any breaches of this agreement.