Acceptable Use Policy for the use of IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices for

Trustees and Governors

In the development of this policy consideration has been given to Equality and Diversity and Data Protection.

Equality and Diversity

CAMPFIRE EDUCATION TRUST is committed to promoting equality of opportunity for all staff and job applicants. The Trust aims to create a supportive and inclusive working environment in which all individuals are able to make best use of their skills, free from discrimination or harassment, and in which all decisions are based on merit. We do not discriminate against staff based on age; race; sex; disability; sexual orientation; gender reassignment; marriage and civil partnership; pregnancy and maternity; religion, faith or belief (Equality Act 2010 protected characteristics). The principles of non-discrimination and equality of opportunity also apply to the way in which staff and Governors treat visitors, volunteers, contractors and former staff members.

Data Protection

CAMPFIRE EDUCATION TRUST will process personal data of staff (which may be held on paper, electronically, or otherwise). CAMPFIRE EDUCATION TRUST recognises the need to treat it in an appropriate and lawful manner, in accordance with the Data Protection Act 2018 (DPA).

This policy is to be used across all CAMPFIRE EDUCATION TRUST a all its schools	Version	Date
CAMPFIRE EDUCATION TRUST Officer responsible for updating con DPO	1	Nov 2019
Date approved by CAMPFIRE EDUCATION TRUST Board		
Effective date as determined by CAMPFIRE EDUCATION TRUST	1	1st Nov 2019
Policy to be reviewed annually from date last approved by CAMPFI EDUCATION TRUST Board	1	Annually
Policy to be reviewed by CAMPFIRE EDUCATION TRUST Trustees		Nov 2020

Policy Contents

Application of the Policy

This policy is to be used by all Trustees and Governors appointed by CAMPFIRE EDUCATION TRUST.

Acceptable Use Policy for the use of IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices for Trustees and Governors

This acceptable use policy is for all trustees and governors in their roles supporting CAMPFIRE EDUCATION TRUST and the schools.

It is a requirement that we ensure the safe and acceptable use of technology for the use of communication within education, including but not limited to: IT software, internet, email, social media, laptops, PCs, tablets, mobile phones and other mobile devices and lists the responsibilities to ensure any form of communication using technology that is used for their role is used appropriately and in line with GDPR rules.

Documents that do not contain personal/sensitive data are not covered by GDPR requirements.

Trustees and governors must ensure, that they take responsibility for reading and upholding the standards laid out in this policy. Due to the nature of the roles being voluntary, the decision has been made that the use of personal devices may be used only if this policy is followed.

All governors/trustees will be given access to GovernorHub to support the sharing and storage of documentation on a secure platform.

- All personal devices that are used for the role must be protected by a minimum of a 6 digit/numeric passcode/fingerprint ID/Facial recognition or similar to prevent access by unauthorised persons.
- All devices are locked when left unattended to ensure unauthorised access is prevented.
- Passwords for their use should not be shared with others and they will not attempt to gain access to anyone else's passwords. Passwords will not be written down or kept where anyone else can gain access to them.
- Governors/trustees must ensure they keep their contact details up to date in GovernorHub as per GDPR requirements. This ensures that any notifications from GovernorHub are sent to the correct address.
- Loss / theft of a personal device must be reported to CAMPFIRE EDUCATION TRUSTs DPO immediately if it contains any personal data in relation to their role within CAMPFIRE EDUCATION TRUST as this is considered a breach under GDPR and will need reporting within 72 hours.
    - Governors/trustees are required to contact their service provider to get the device blocked where possible, ensuring that all passwords for emails, GovernorHub etc are changed as soon as possible and within 24 hours.
- Any documents sent by email that contain personal data/sensitive data must be password protected – see Appendix 1, the password should where possible be phoned through to the recipient or sent via a separate email using a different heading to safeguard it. The use of email for sending personal/sensitive data should be limited and only used where other means are not available.
    - Documents containing personal/sensitive data could include, but are not limited to:
        - Safeguarding issues against staff
        - Recruitment

- Salaries
- Exclusions
- Complaints

  - Documents in GovernorHub containing personal data should as best practice be marked as not downloadable, but, if there is a requirement to download any documents then passwords must not be removed from the document when downloaded, this protects the data from being accessed by unauthorised persons. The downloaded document must not be kept for any longer than is absolutely necessary, ensuring that when deleted, the item is also deleted from the deleted/trash folder. Any governor information downloaded that does not fall under GDPR should be deleted after 18 months. GovernorHub should be used for archival purposes.

- Where deemed appropriate an appointed person will create groups within GovernorHub that enables access to named persons only where personal/sensitive data can be accessed. Governors will be made aware of the groups they are in by the clerk or school and can also see this within GovernorHub.
- If given the use of trust/school equipment trustees/governors are responsible for knowing where the device is at all times and to be responsible for ensuring it is securely stored when not in use (this is for any item that is allocated to them for use in their role). Laptops/mobile devices that are taken off-site must be stored out of site securely. If left in a vehicle they must not be left in view but stored in the boot and the vehicle locked, items must not be left in a vehicle overnight.
- They do not use/duplicate/remove or amend anyone else's documents without their prior permission.
- They do not download, copy or distribute anything that is protected by copyright.
- To maintain professional boundaries when using the internet and social media for personal use. That when posting on personal forums/social media that there is the understanding that the use of any comments or photos regardless of whether they are positive or negative can be shared with others (parents, pupils, colleagues) and this could lead to losing control of who sees them or a misinterpretation of what was written, this could then bring your professional role and workplace into disrepute.
- Do not participate in communicating with pupils/parents outside of their role at the trust/school when using work or personal technology/devices for the use of social media, texting, calling. It is important to ensure that a professional relationship is adhered to at all times to prevent any misinterpretation of any actions made.
- Must not communicate any confidential information that they become aware of in their role at the trust/school to anyone that is not entitled to it during discussions or via any IT / social media regardless of whether a personal device or trust/school device is used.
- That in their role at the trust/school no personal details are exchanged with pupils that would allow contact directly via any means. It is understood that trustees/governors may have contact with pupils as friends/parents outside their role at the trust/school.
- All communications with pupils must be via the trusts/school's internal network and only in relation to their role with specific permission from the headteacher in the case of schools.

- Must not use trust/school equipment to upload, download any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or anything that is inappropriate or may cause harm or distress to others.
- No device is used for bullying or harassment of others in any form.
- That personal mobile phones must not be used in schools where children are present. Mobile phones should be kept secure and away during school hours but can be used when in an area away from pupils.
- They report any incidents of concern regarding social media misuse to the trust or headteacher in the first instance, this includes but is not limited to illegal, inappropriate or harmful material.
- They agree to be responsible users at all times and understand that they are responsible for their actions and misuse or failure to comply with this policy could result in disciplinary action of a verbal, written warning, suspension, and the involvement of the police in the event of illegal activity. Trust HR and the DPO will be notified of any misuse.

All must understand that the trust/schools will monitor the use of ICT systems including email and other digital communications where they have provided equipment for the use of people's roles. GovernorHub is also monitored by the trust/school.

All Governors and Trustees are asked to sign and date the form below to confirm they have received a copy of the Acceptable Use Policy for the use of IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices for Trustees and Governors and have read and agree to adhere to it.

Agreement to adhere to the Acceptable Use Policy for the use of IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices for Trustees and Governors:

I confirm that I have received a copy of the IT acceptable Use Policy for trustees/governors, read and understand that I must adhere with it and understand that any breach could result in a verbal warning, suspension of duties, and the involvement of the police in the event of illegal activity. Trust HR and the DPO will be notified of any misuse.

I will **immediately** report the loss of any equipment covered by this policy to the DPO at DPO@CAMPFIRE EDUCATION TRUST.co.uk

I will report any incidents of concern regarding misuse of technology/software/social media to the head teacher or trust DPO.

I understand that the trust/schools will monitor the use of ICT systems including email and other digital communications.

Name: _____

Signed: _____

Position: _____

Location _____

(School name or Trust):

Date: _____

Appendix A

How to password protect a document for Word and Excel documents:

Choose file save or save as

Choose file destination

At bottom to the left hand side of SAVE click on TOOLS

Choose General Options

Then type a password into the Password to open, then you will be asked to re-type the password

You can prevent anyone from modifying the document by adding a password into the modify box – this allows them to view the document but make no changes unless you send them the password you have used

Appendix B

Acceptable Use Policy for all users in the use of: IT/Social Media/Electronic Communications/ Mobile Phones/Laptops/Portable Devices

How to change your Office 365 Password:

1) Sign in to your Office 365 account
2) Go to **Settings** > **Office 365 settings** > **Password** > **Change password**.
3) Type your old password, and then type a new password and confirm it.
4) Click **Submit**.

How to Remove a Saved Password from a Browser

If you store passwords for regular accessed web addresses (eg Pupil Asset, The Key etc) these saved password lists can expose the data it protects to anyone else who uses your computer, and possibly to others on the Internet, particularly if your compute is 'hacked'. CAMPFIRE EDUCATION TRUST therefore ask you not to store these passwords. If you already have stored passwords, below are a few ways to delete them depending on the Web Browser you use:

Internet Explorer

To delete individual passwords:

1. Open internet explorer
2. Select … top right corner (the three dots)
3. Choose settings (towards bottom of list)
4. Choose Advanced Settings
5. Choose Manage Passwords
6. Click each web address and choose (**remove/delete**) until all gone

To prevent being prompted to save passwords, make sure the slide button under passwords is marked as OFF.

Chrome

To delete individual passwords:

1. Open Chrome
2. Select … top right corner (the three dots)
3. Choose settings (towards bottom of list)
4. Choose Passwords
5. Click each web address and choose **remove** until all gone

To prevent being prompted to save passwords, make sure the slide button opposite Offer to save passwords is marked as OFF.