Acceptable Use Policy for Trust Employees in the use of:

IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices

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

Acceptable Use Policy for Trust Employees

In using technology for the use of communication for education and personal use, including but not limited to: IT software, internet, email, social media, via laptops, PCs, tablets, mobile phones and other mobile devices

This acceptable use policy is for all trust employees, to ensure safe and acceptable use of technology for the use of communication for education and personal use, including but not limited to: IT software, internet, email, social media, via laptops, PCs, tablets, mobile phones and other mobile devices and lists the responsibilities they have in ensuring any form of communication using technology that they use in their role is used appropriately and in line with GDPR rules.

The trust/schools will try to ensure that everyone has good access to IT to enhance their role and to be able to provide the relevant learning opportunities for pupils.

Trust employees must ensure, that they take responsibility for reading and upholding the standards laid out in this policy and that they ensure:

- That all technological devices have password/encryption facilities installed, for mobiles this must be a minimum of a 4 digit passcode.
- That they lock their PC/laptop or other equipment when leaving it unattended to ensure unauthorised access is prevented.
- They do not disclose or share any passwords provided for their use to others and will not attempt to gain access to anyone else's passwords. Passwords will not be written down and kept where anyone else can gain access to them.
- They do not install any hardware or software on any trust-owned device without the trusts permission (delegated to the headteacher if school based.)
- They are using a trust or school email address for any correspondence they send in relation to their role in the trust/school.
- They ensure that any emails with attachments that contain personal or sensitive data are encrypted or are saved onto a secure shared site giving the link to where it can be accessed.
- When replying to personal email addresses attachments that contain personal data is not attached, attachments containing personal data must always be sent via a business email address, with any attachments encrypted.
- They respect the technical safeguards which are in place, and any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services is unacceptable.
- Ensure all data is kept secure and used appropriately as authorised by the trust (delegated to the headteacher if school based).

- They know where any trust/school owned 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.
- They do not download apps to enable access to work emails/files on their personal devices. Access to emails/files must only be accessed through a web browser, but they must ensure that they log out each time they access it. If the only means of calling the emergency services to an incident is by using a personal mobile phone that is automatically approved.
- 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.
- They 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.
- They do not participate in communicating with pupils/parents outside of their role at the trust 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.
- That no personal details are exchanged with pupils that would allow contact directly via personal email, telephone, address.
- All communications with pupils must be via the trusts/school's internal network.
- They do 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 the use of trust/school equipment to access personal sites (social media) is not to be used unless they are on a break and is not in an area that affects others nearby.
- That personal mobile phones must not be used in schools where children are present. Mobile phones should be locked away during school hours but can be used when on a break away from pupils.
- They report any incidents of concern regarding social media misuse to their line manager in the first instance, this includes but is not limited to illegal, inappropriate or harmful material.
- That if any work device (laptop/mobile phone/ipad or similar) is stolen it must be reported to the DPO ***immediately*** as this is considered a breach under GDPR and will need reporting within 72 hours.
- 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.

All employees, are asked to sign and date the form below to confirm they have received a copy of the Acceptable Use Policy for Employees and have read and agree to adhere to it.

Agreement to adhere to the Acceptable Use Policy:

I confirm that I have received a copy, read and understand that I must adhere with the above policy and understand that any breach could result in disciplinary action.

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

I will report any incidents of concern regarding misuse of technology/software/social media to my line manager in the first instance.

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: _____