THE SAMARA TRUST

Enriching Lives

GDPR ACCEPTABLE USE POLICY

General Data Protection Regulation

Acceptable Use Policy for Staff, Governors, Trustees and Volunteers 2019

This policy/notice was written in November 2019.

Introduction

The Samara Trust commits to protecting the privacy and security of the personal information it holds for staff, governors, Trustees and volunteers. Please note our Privacy Statements.

To complement the data protection duties of the school there are duties shared by all staff, governors, trustees and volunteers because, as a professional organisation with responsibility for children's safeguarding, it is essential that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using information communication technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This agreement covers all digital and physical data systems, e.g. the internet, intranet, network resources, learning platform, software, communications tools (online and offline), equipment (access devices) and paper records, whether printed or handwritten and however stored.

1. I understand that data held by the school may only be processed (acquired, processed, stored, deleted or transmitted) on the legal bases that the school has registered with the Information Commissioner's Office.
2. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation 2018. This means that all personal data will be processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted. Any images or videos of pupils will always take into account parental consent. I will ensure that data no longer needed will be effectively deleted or shredded.
3. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation. Such misuse is also covered by the GDPR and any such misuse must be reported to the ICO, and to the data subjects (people) affected, within 72 hours.
4. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my device as appropriate. I will not use personal equipment to access school data.

5. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password. I will adopt school procedures for the safe storage of my passwords and for acquiring new ones.
6. I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). Where possible I will use the school server to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft. I will not share any files or folders on the school server with any other user. I will be mindful that when working in a public space that others may be able to see my laptop, tablet or mobile phone screen and will use my discretion as to whether information should be hidden from sight. I am aware that enabling Bluetooth connectivity on mobile devices can be a security threat and will switch this off when it is not needed for a specific connection.
7. I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
8. I will respect copyright and intellectual property rights.
9. I have read and understood the school's Data Security Policy and e-Safety Policy which cover the security of data and safe and appropriate access to data.
10. I will report all incidents of concern regarding children's online safety to the designated child safeguarding lead and/or the e-Safety coordinator and/or the lead for prevent as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable/extreme websites to the e-safety coordinator. The designated child safeguarding trustee is Paula Conlin. If I am unsure who the other leads are I will contact the principal at my school in the first instance.
11. I will not attempt to bypass or alter any filtering and/or security systems put in place by the school.
12. My communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. I will ensure that a BCC of any emails to parents/carers are sent to the school's admin mailbox. All written notes will be copied to the school's admin mailbox. Any pre-existing relationships which may compromise this will be discussed with the senior leadership team.
13. I will refrain from using any form of social media to discuss any aspect of school life except purely social events that involve colleagues. I will follow any guidance issued when contributing to the use of social media by the school as an official communication channel.
14. My use of ICT and information systems and my written communication will always be compatible with my professional role whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites or postal addresses. My use of ICT and other forms of communication will not interfere with my work duties and will be in accordance with the school AUP and the law.
15. I will not create, transmit, display, write, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.
16. I will promote e-safety (including privacy) with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create. Similarly, I will promote care for others in the pupils' writing and any other content that they create.

17. I understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance.
18. The school may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the school suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.
19. If you leave the business you must return any IT equipment assigned to you unlocked, and unencrypted to the school office before you leave. This includes but is not limited to laptops, iPads, phones and memory devices.

I _____ (please print name) acknowledge that I have received and read and understood a copy of The Samara Trust Acceptable Use Policy.

Signed: _____

Dated: _____