IT Acceptable Use Policy for Staff, Volunteers, Visitors & School Governors

Approved by:	Governing Body	
Last Reviewed:	30/09/2024	
Reviewed by::	Sarah Luff Head of School Polly John Deputy Head of School	
Next review due:	October 2025	

Policy Overview:

1.0 Policy introduction & overview

2.0 Acceptable use of mobile phones in school

3.0 Acceptable use of social media

4.0 Virtual Board and SMC meetings

5.0 Declaration

1.0 Introduction

Technology has become integral to the lives of children and young people in today's society, both within schools and in their personal lives. The internet, and other digital information and communications platforms, are powerful tools which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work and delivery of lessons. All users should have an entitlement to safe access to the internet and digital technologies at all times. This acceptable use policy is intended to ensure:

• that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• that school and Rainbow Multi Academy Trust systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• that staff are protected from potential risk in their use of technology in their everyday work. The Trust will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Please note, where the Trust's IT Team are referenced, those responsible include:

Andrew Manning (TME): Senior Network Engineer

Ransi Bandara: Operations & Finance Director

Sarah Luff: Digital Safeguarding Co-ordinator:

Andrew @ ICT4: Data Protection Officer, (DPO)

As a professional organisation with responsibility for children's safeguarding, it is important 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 Rainbow Multi Academy Trust Information Communication Technology systems, they are asked to read and sign this Acceptable Use Policy.

Acceptable use of personal mobile phones is also summarised in the document, when used in school, on site, or when off site and working with pupils; acceptable use of personal social media accounts is also summarised below.

This is not an exhaustive list and all members of Rainbow Multi Academy Trust staff are reminded that ICT use should be consistent with your school's ethos, any internal procedures and, always, to any relevant national and/or local guidance and expectations, and the law:

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include: laptops, mobile

phones, tablets, digital cameras, email, social media sites and video conferencing platforms such as teams, zoom and google platforms.

2. Trust 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.

3. 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 login as appropriate. I will not remove any IT equipment from my school without prior authorisation from the Head of School or my line manager.

4. I will respect system security and I will not disclose any password or security information and will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. It is changed regularly, or when required). Mobile devices will be protected with a passcode or using an approved biometric system.

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from Rainbow Multi Academy Trust IT team. Apps installed on tablet and mobile devices should be for educational purposes and are monitored by the trust IT team.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act. This means that all personal data will be obtained and 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 (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN and/or SharePoint).

7. I understand that emails should not be sent from my school/trust account to my personal email address; this constitutes a data breach.

8. Memory sticks, and other storage devices, are not condoned by Rainbow Multi Academy Trust and should not be used. Any data required should be accessed via SharePoint. I will use the SharePoint platform as a means of accessing and sharing data remotely. Memory sticks and removable storage should not be used within the school/trust, or for remote working, due to the associated risks that they carry for data protection and IT system security.

9. Any images or videos of pupils will only be taken and used as stated in the Trust's digital safeguarding policy and will always take into account parental consent. I will respect copyright and intellectual property rights.

10. I will not keep, or access, professional documents which contain school/trust-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, tablets, mobile phones). Where possible, I will use SharePoint to upload any work documents and files in a password protected environment. I will protect devices in my care from unapproved access or theft.

11. I will not store any personal information on the school/trust computer system, including any school/trust laptop or similar device issued to members of staff that is unrelated to school/trust activities, such as personal photographs, audio and video files or financial information.

12. I have read, understood and will implement the terms within the Trust's Digital Safeguarding Policy which covers the requirements for safe ICT use, including using appropriate devices and supervision of pupils within the classroom and other working spaces.

13. I will report all incidents of concern regarding children's online safety to my school's Designated Safeguarding Lead as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to my school's Designated Safeguarding Lead and the Digital Safeguarding Coordinator, (Sarah Luff), as soon as possible.

14. I will not attempt to bypass any filtering and/or security systems put in place by the school/trust. If I suspect a computer or system has been damaged, or affected by a virus or other malware, or if I have lost any school/trust related documents or files, I will report this to the Trust IT team and the Data Protection Officer (DPO) as soon as possible.

15. Any electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. No personal contact information will be provided to pupils and parents and all communication will take place via school/trust approved communication channels e.g. via a school/trust provided email address, ClassDojo, via telephone or a virtual parents' consultation platform and not via personal communication channels, e.g., personal email or social networking. Any pre-existing relationships that may compromise this expectation, should be discussed with a Senior Leader.

16. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school/trust or personal systems. This includes the use of email, text, social media/networking, gaming video conferencing and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the points made in this policy, and the law.

17. I will ensure that my online activity, both in school and outside school, will not bring the Trust, my professional role, or that of others into disrepute.

18. I will not create, transmit, display, 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 Rainbow Multi Academy Trust, into disrepute.

19. During any ongoing need for remote learning, I will continue to act professionally and appropriately, in accordance with the Trust's and school's related policies and procedures. This applies to my interactions with pupils and parents.

20. Live video and or audio streaming can be used for the purposes of remote learning, in line with the expectation of the online safeguarding protocols document, and alongside a personalised school risk assessment.

21. I will access and stay up-to-date with relevant and statutory online training and child safeguarding updates.

22. I will not create, transmit, display, publish or forward any materials that fall under the government's Prevent Duty guidance; i.e. radicalisation, terrorism and extremism.

23. I will access my work e-mails on a regular basis, as stipulated in the communication protocol. I understand that email should be used carefully and appropriately and it should be understood that an email can be classed as a legally binding document.

24. I will promote online safety 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 in line with the Trust's Digital Safeguarding policy.

25. If I have any queries or questions regarding safe and professional practice online, either in school or off site, then I will raise them with the Designated Safeguarding Lead and/or the Digital Safeguarding Coordinator.

I understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance.

The Trust 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 Digital Safeguarding 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 Trust will invoke its disciplinary procedure. If the Trust 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.

2.0 Procedures for staff/visitor/governor use of mobile phones in school

The following section outlines the acceptable use of mobile phones by staff, volunteers and governors in all Rainbow Multi Academy Trust schools; we keep the safeguarding of pupils, and staff, at the forefront of our considerations, recognising the vulnerability and potential for exploitation and abuse through the inappropriate use of mobile phones. **All staff, including supply teachers, contactors, volunteers and visitors to school sites** should take every step to adhere to the following acceptable use protocols.

Staff/volunteers/governors may bring mobile phones onto the school site, providing the device is:

- used only in a designated meeting room/classroom, outside of the school gate, or in office spaces where no pupils are present.
- switched off and out of sight of pupils, in a locked cupboard or locker where possible.
- only used during break or lunch times and at either end of the school day in the spaces outlined above.
- when attending an off-site visit or trip, designated members of staff will have a mobile phone available for emergency contact with the school/ with each other/ to make emergency calls. In this context, phones will not be used to make or receive personal calls, send messages or use social media.
- Personal mobile phones **must not** be used to take photos of pupils. School cameras/school mobile phone should be used for this purpose.
- Mobile phone numbers should not be exchanged with parents, unless a pre-existing relationship is held. Parents should not contact you on personal devices about school matters and should be redirected to use the school secretary's email address to make contact.
- Visitors/new staff will receive this information during their school induction. An information leaflet should be shared that provides a summary of the school's expectations.

  It is the responsibility of all staff/ volunteers/governors to exercise vigilance at all times and to raise concerns about misuse and non-adherence to this policy by reporting the incident to the school's Designated Safeguarding Lead.

3.0 Procedures for social media use

Rainbow Multi Academy Trust is aware and acknowledges that an increasing number of adults and children are using social networking sites, including Instagram, Facebook and Twitter, amongst many others. The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and

services effectively and flexibly. However, it is also important to ensure that we balance this with the up keeping of school and Trust reputation.

This policy, and associated guidance, is to protect staff and advise school/trust leaders on how to deal with potential inappropriate use of social networking sites. For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. The policy requirements, in this document, aim to provide this balance, to support innovation whilst providing a framework of good practice.

The purpose of this section of the policy is to ensure:
- That the school/trust is not exposed to legal risks
- That the reputation of the school and trust is not adversely affected
- That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the school/trust.

A reminder that Facebook is targeted at older teenagers and adults. They have a 'no under 13' registration policy and recommend parental guidance for 13 to 16 year olds.

This policy covers the use of social networking applications by all school/trust stakeholders, including, employees, governors, visitors and Directors. The requirements of this section of the policy apply to all uses of social networking applications (which are used for any school/trust related purpose) and regardless of whether the school/trust representatives are contributing in an official capacity to social networking applications provided by external organisations. Social networking applications include, but are not limited to: Blogs, online discussion forums, collaborative spaces, such as Facebook, media sharing services (You Tube and Twitter, for example). All school/trust representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with Rainbow Multi- Academy Trust Equality and Diversity Policy.

Use of social networking applications in work time, for personal use, is not permitted from school devices.

All proposals for using social networking applications as part of a school/trust service (whether they are hosted by the school or by a third party) must be approved by the Head of School/CEO first.

School/trust representatives must adhere to the following Terms of Use which apply to all uses of social networking applications; this includes public facing applications such as open discussion forums and blogs, whether they are hosted on the school/trust network or not. Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.

Terms of Use:

- Social media must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes material of an illegal, sexual or offensive nature that may bring the school/trust into disrepute.
- Social media must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns
- It must not be used in an abusive or hateful manner
- It must not be used for actions that would put school/trust representatives in breach of school/trust codes of conduct or policies relating to staff.
- Should not breach other Trust policies like the equal opportunities policy.
- Social media must not be used to discuss or advise on any matters relating to school/trust matters, staff, pupils or parents
- No staff member should have a pupil, or former pupil under the age of 18, as a 'friend' to share information with
- Employees should not identify themselves as a representative of the school/trust

- References should not be made to any staff member, pupil, parent or school/trust activity / event unless prior permission has been obtained and agreed with the Head of School/CEO
- Staff should be aware that, if their out-of-work activity causes potential embarrassment for the employer, or detrimentally effects the employer's reputation, then the employer is entitled to take disciplinary action.
- Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to, and including, termination of employment.

Guidance & protection for staff on using social networking:

• No member of staff should interact with any pupil in the school/trust on social networking sites
• No member of staff should interact with any ex-pupil in the school/trust on social networking sites who is under the age of 18
• This means that no member of the school/trust staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
• Where family and friends have pupils in school and there are legitimate family links, please inform the Head of School.
• It is illegal for an adult to network, giving their age and status as a child.
• If you have any evidence of pupils or adults using social networking sites in the working day, please contact the named Designated Safeguarding Lead in school.
• No pupil under 13 should be accessing social networking sites. This is the guidance from Facebook. There is a mechanism on Facebook where pupils can be reported via the Help screen.
• No pupil may access social networking sites during the school working day
• All pupil mobile phones must be securely stored in accordance with the individual school's protocol. The internet capability should never be linked to the school's wifi.
• If pupils attempt to add staff members on social media, the member of staff is to inform the Head of School. Parents will be informed if this happens
• No school/trust computers are to be used to access social networking sites at any time of day, unless for direct school use (posting school information on the school Facebook page.)

Child protection guidance

If a Head of School receives a disclosure that an adult employed by the school is using a social networking site in an inappropriate manner, as detailed above, they should:
• Record the disclosure in line with their child protection policy.
• Refer the matter to the LADO who may investigate with the Police Child Protection Team. If a disclosure comes from a member of staff, confidentiality should be upheld.
• Seek advice from the LADO who will advise whether the member of staff should be suspended pending investigation after contact with the police. It is not recommended that action is taken until advice has been given.
• If disclosure is from a child, follow your normal process in your child protection policy until the police investigation has been carried out.

4 Virtual Attendance during face to face Board or governor meetings:

Where a Trustee or governor member wishes to attend a meeting by telephone, or by a virtual forum, the Chair of the SMC/ Chair of the Committee/ Chair of the Board and the Clerk or Secretary taking minutes must be notified at least 48 hours in advance of the meeting to ensure that appropriate arrangements can be made to include the individual. The individual will be asked their reasons for not attending the meeting in person and their attendance, virtually, will be subject to the approval of the Chair. Where approval is withheld, the reason for this will be provided to the Director/governor member.

Trustees/governor members attending the meeting, either by telephone or video conference, will be entitled to vote on any issue providing they have been 'present' for the whole agenda item which the vote relates to. Where a secret ballot is required, this will be facilitated, where possible, (e.g. by taking a telephone call off speaker phone and the Trustee sharing their vote verbally with the Clerk). Within an online forum, the individual will be asked to message the Clerk directly through the 'chat' function to cast their vote. Where voting confidentially is not possible, the Trustee/SMC member will be required to vote publicly, or abstain from voting.

Trustees/governors members attending the meeting, virtually, will contribute to the quorum. If the technological link is lost, they will cease to contribute to the quorum, but this will not prevent the meeting continuing in their absence, unless it has become inquorate.

If, after all reasonable efforts, it does not prove possible for a Trustee/governor member to participate by telephone or virtual forum, the meeting may still proceed with its business provided it is otherwise quorate.

NB: Directors and governor members may wish to agree an established pattern of meetings, some of which may be stipulated as face to face meetings and others as virtual meetings. A schedule may be agreed as an internal procedure, with all Committee/Board/Governor members in agreeance.

Where a meeting is taking place virtually, the usual statutory notice arrangements will apply and all papers to be considered will be circulated at least five days in advance of the meeting, except where the Chair has exercised his/her right to waive the usual notice, in an emergency.

Virtual meetings will be minuted in the same way as other meetings, either by the Clerk or School Secretary who will be present either virtually or physically at the meeting. Minutes will be sent and shared following each meeting and ratified at the next meeting of the Board/Committee/Governors.

Virtual meetings should not be video or audio recorded by any Trustee, Clerk or Secretary without the approval of Trustees and, if agreed, should be for a specified purpose.

5.0 Declaration

In signing this policy, I agree and understand that:

1) this Acceptable Use Policy applies not only to my work and use of digital technology equipment in school, but also applies to my use of school/trust systems and equipment off the premises and my use of personal equipment on the premises, or in situations related to my employment by the school/Trust.
2) If I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. I have read and understand the above and agree to use the school/trust digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school/trust) within these guidelines.