Kingsmead Academy T/A Kingsmead School	**POLICY TITLE:**	**Staff and Volunteer Acceptable Use Policy**
		Deputy Headteacher: Well-Being & Diversity Well-Being & Diversity sub committee
Date Approved by Governing Body:		September 2022
Date of Last Review:		Term 6 – 2022/23
Next Review Due:		Term 6 – 2023/24

1. Introduction

This Acceptable Use Policy reflects the school Online Safety, Cyber Security and Data Protection & Freedom of Information policies. The school will ensure that staff and volunteers will have access to technology to enable efficient and effective working enabling learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

2. Scope of Policy

This Acceptable User Policy (AUP) policy applies to staff and volunteers who have access to and are users of school technology systems, school related use of technology systems outside of school, and make use of social networks personally and professionally.

3. My responsibilities

3.1. I agree to read, understand, sign and act in accordance with the school Online Safety Policy

3.2. I agree to report any suspected misuse or concerns to the Online Safety Leader / Designated Safeguarding Lead

3.3. I agree to monitor technology activity in lessons, extracurricular and extended school activities, including awareness of any access to extremist views

3.4. I agree to model the safe and effective use of technology

3.5. I agree to demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies especially at the time of a Critical Incident

4. Education

4.1. I agree to provide age-appropriate online safety learning opportunities as part of a progressive online safety curriculum; and reinforce the learning throughout the school's curriculum

4.2. I agree to respect copyright and educate the pupils to respect it as well

4.3. I agree to teach about the need for using responsible and caring language when communicating with others

5. Training

5.1. I agree to participate in Cyber Security, GDPR and Online Safety training

5.2. I agree to request training if I identify an opportunity to improve my professional abilities

6. Online Bullying

6.1. I agree to support the school's zero tolerance of bullying. In this context, online bullying is seen as no different to other types of bullying

6.2. I agree to report any incidents of bullying in accordance with school procedures

7. Sexting

7.1. I will secure and switch off any device discovered with a sexting image and report immediately to the Designated Safeguarding Lead.

7.2. I will not investigate, delete, or resend the image.

8. Prevent

8.1. I will continually develop children's ability to evaluate information accessed online.

8.2. I will follow the agreed reporting procedure where children are purposefully searching for inappropriate sites or inadvertently accessing inappropriate sites.

9. Technical Infrastructure

9.1. I understand that the school will monitor my use of computing devices and the internet. Unless I have permission, I will not try to by-pass any of the technical security measures that have been put in place by the school which include:

a) the proxy or firewall settings of the school network
b) not having the rights to install software on a computer
c) not using removable media e.g. memory sticks

10. Password Security

10.1. I will follow the password requirements within the Cyber Security Policy

10.2. I will only use my own passwords

10.3. I will never share my passwords

10.4. I will never log another user onto the system using my login

10.5. I will not leave my device unsupervised and unlocked.

11. Filtering

11.1. I will not try to bypass the filtering system used by the school.

11.2. If I am granted special access to sites that are normally filtered, I will not leave my device unsupervised

11.3. I will report any filtering issues immediately

12. Data Protection

12.1. I understand my responsibilities towards the data protection regulations and will ensure the safe keeping of personal and sensitive personal data at all times.

12.2. I will ensure that all data held in personal folders is regularly backed up and kept secure.

12.3. If I believe there has been a loss of personal or sensitive data, I will immediately report it to the Data Protection Lead in the school.

13. Use of digital images, video and sound

13.1. I will follow the school's policy on using digital images, video and sound, especially in making sure that only those pupils whose parental permission has been given are published.

13.2. I will not use personal devices for taking or sharing digital images or sound.

14. Communication

14.1. I will be professional in all my communications and actions when using school technology systems.

14.2. I understand that I need to be open and transparent in all my communications.

15. Email

15.1. I will use the school provided email for all business matters.

15.2. I will follow the school agreed email protocols:

a) **Confidential**
- Apply the correct sensitivity marker – confidential (internal) or encrypt (external)

b) **Courtesy**
- No expectation whilst teaching or after 5:30pm
- Set a reasonable time scale for action
- Reply within 2 working days

c) **Common sense**
- Use BCC and avoid Reply All
- Write professionally – a third party may see your message!
- Avoid large recipient groups if you can – especially regarding individual students
- Use 'FAO' (for attention of) when using BCC with larger groups of recipients
- Use a person's initials in the subject line
- Use your correct email signature (which may not be set on personal devices)

d) **Check it**
- **CHECK:** Correct recipients in the correct places?
- **CHECK:** Have your proofread it?
- **CHECK:** Are you emailing outside of working hours? (Consider using 'send later')

15.3. I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs

16. Social Media and Personal Publishing

16.1. I will ask permission before I use social media e.g. blogs, social networks or online communication tools with pupils or for other school related work, this must be using a Kingsmead email address.

16.2. I will check with the Data Protection Lead before I use sites/apps with learner logins to ensure that any pupil personal data is being held securely. The site/apps must have a Privacy Impact Assessment (PIA) completed and the system will be recorded on the school's Data Asset Audit.

16.3. I will follow the online safety policy concerning the personal use of social media, never publishing disparaging or harmful comments or expressing extreme views. These are considered to bring the school into disrepute.

16.4. I will not post any comments about the school, any pupil, employer or colleagues on any personal social networking and publishing accounts.

16.5. When there is a Critical Incident, I will not post any comments online.

17. Personal Devices

17.1. I will not use personal devices during contact time with pupils. They will be turned off at other times.

17.2. I will check that any personal devices I have in school are pin code or fingerprint protected and not discoverable by third parties.

17.3. I will not use my personal devices to contact pupils or parents.

17.4. I am responsible for any use of my own 3G/4G data during agreed times and ensuring that my use complies with the school's online safety policy.

17.5. I will only use the school WiFi for work related matters when using personal devices.

17.6. I will use Company Portal on my personal device to access work data.

17.7. I will not download any school data on my personal device.

18. Reporting Incidents

18.1. I will report and record any incidents relating to online safety to the Online Safety Leader / Designated Safeguarding Lead and check actions taken have been recorded

18.2. I understand that in some cases the Police may need to be informed.

19. Sanctions and Disciplinary procedures

19.1. I understand that there are regulations in place when pupils use technology and will apply sanctions if they do not follow the rules.

19.2. I understand that if I misuse the School technology systems in any way then there are disciplinary procedures that will be followed by the school.

Staff and Volunteer Acceptable Use Policy Agreement

I have read and understand the full School online safety policy and agree to use the school technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in a responsible and professional manner as outlined in that document.

Staff/Volunteer Name	
Signature	
Date	