Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members and visitors of the TechCommsMedia community are fully aware of the TechCommsMedia boundaries and requirements when using the TechCommsMedia Wi-Fi systems and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list, and all members of the TechCommsMedia community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. TechCommsMedia provides Wi-Fi for the TechCommsMedia community and allows access for (state purpose, for example education use only). Settings should include any include information about time limits, passwords, and security.

2. I am aware that the TechCommsMedia will not be liable for any damages or claims of any kind arising from the use of the wireless service. TechCommsMedia takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the TechCommsMedia premises that is not the property of the TechCommsMedia.

3. The use of technology falls under TechCommsMedia Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy (any other relevant policies such as data security, safeguarding/child protection) which all staff and visitors must agree to and comply with.

4. The TechCommsMedia reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. TechCommsMedia owned information systems, including Wi-Fi, must be used lawfully; 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.

6. I will take all practical steps necessary to make sure that any equipment connected to the TechCommsMedia service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The TechCommsMedia wireless service is not secure, and TechCommsMedia cannot guarantee the safety of traffic across it. Use of the TechCommsMedia wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. TechCommsMedia accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the TechCommsMedia wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless TechCommsMedia from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

10. I will not attempt to bypass any of TechCommsMedia security and filtering systems or download any unauthorised software or applications.

11. My use of TechCommsMedia Wi-Fi will be safe and responsible and will always be in accordance with the TechCommsMedia AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring TechCommsMedia into disrepute.

13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead Mr. Adam Benjamin as soon as possible.

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead Mr. Adam Benjamin or the manager.

15. I understand that my use of the TechCommsMedia Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If TechCommsMedia suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then TechCommsMedia may terminate or restrict usage. If TechCommsMedia suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.