Visitor and Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology.

This AUP will help Shipbourne School ensure that all visitors and volunteers understand the School's expectations regarding safe and responsible technology use.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within Shipbourne School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies**.**

2. I understand that Shipbourne School AUP should be read and followed in line with the School staff behaviour policy/code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the School ethos, School staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Data and Image Use

4. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

5. I understand that I am not allowed to take images or videos of learners.

Classroom Practice

6. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners.

7. Where I deliver or support remote learning, I will comply with the School remote learning AUP.

8. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.

9. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) (Terri Daters) in line with the School child protection policy.

10. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, or distribute or use it.

Use of Social Media and Mobile Technology

11. I have read and understood the School policy which covers expectations regarding staff use of social media and mobile technology.

12. I will ensure that my online reputation and use of technology and is compatible with my role within the School. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the online safety/social media policy.
    - I will not discuss or share data or information relating to learners, staff, School business or parents/carers on social media.
    - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the School code of conduct and the law.

13. My electronic communications with learners, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via School approved communication channels such as via a School provided email address, account or telephone number.
    - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the DSL and/or Head of School.

14. If I have any queries or questions regarding safe and professional practice online either in School or off site, I will raise them with the Designated Safeguarding Lead and/or Head of School.

15. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

16. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

17. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the School into disrepute.

Policy Compliance, Breaches or Concerns

18. I understand that the School may exercise its right to monitor the use of School information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

19. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead in line with the School child protection policy.

20. I will report concerns about the welfare, safety, or behaviour of staff to the Head of School, in line with the allegations against staff policy.

21. I understand that if the School believes that if unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the School may invoke its disciplinary procedures.

22. I understand that if the School suspects criminal offences have occurred, the police will be informed.

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the School community are fully aware of the School boundaries and requirements when using the School 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 School community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. The School provides Wi-Fi for the School community and allows access for education and school-based communication, allowing for reasonable personal use outside of teaching sessions.

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

3. The use of technology falls under Shipbourne School Acceptable Use of Technology Policy (AUP), child protection policy, online safety policy, positive behaviour policy, staff code of conduct, data protection policy and mobile devices/social media policy which all learners/staff/visitors and volunteers must agree to and comply with.

4. The School 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. School 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 School service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. Use of the School 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. The School accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the School 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 the School 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 the School security and filtering systems or download any unauthorised software or applications.

11. My use of School Wi-Fi will be safe and responsible and will always be in accordance with the School 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 the School into disrepute.

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

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead and/or the Head of School.

15. I understand that my use of the School Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the School suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the School may terminate or restrict usage. If the School 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.