

# Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Shipbourne School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for pupils, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Shipbourne School expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that Shipbourne School systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

## Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the Shipbourne School or accessed by me as part of my role within Shipbourne School professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email, data and data storage, remote learning systems and communication technologies.
2. I understand that Shipbourne School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the Shipbourne School child protection policy, staff code of conduct and remote/online learning AUP.
3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the Shipbourne School ethos, Shipbourne School staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

## Use of Shipbourne School devices and systems

4. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed during non-contact time.
5. Personal devices may be used in school but school wifi must be used to ensure full filtering is in place and no phones should be used in classrooms when pupils are present.
6. Where I deliver or support remote/online learning, I will comply with the Shipbourne School remote/online learning AUP.

## Data and system security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
  - I will use a 'strong' password to access Shipbourne School systems.
  - I will protect the devices in my care from unapproved access or theft.
8. I will respect Shipbourne School system security and will not disclose my password or security information to others.
9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager and/or head teacher.
10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.
11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the Shipbourne School information security policies.
  - 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 or accessed remotely.
  - Any data being removed from the Shipbourne School site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.
12. I will not keep documents which contain Shipbourne School related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the Shipbourne School Microsoft 365 account to upload any work documents and files in a password protected environment.
13. I will not store any personal information on the Shipbourne School IT system, including Shipbourne School laptops or similar device issued to members of staff that is unrelated to Shipbourne School activities, such as personal photographs, files or financial information.
14. I will ensure that Shipbourne School owned information systems are used lawfully and 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.
15. I will not attempt to bypass any filtering and/or security systems put in place by the school.
16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider and/or head teacher as soon as possible.

17. If I have lost any Shipbourne School related documents or files, I will report this to the head teacher and Shipbourne School Data Protection Officer (GDPRiS) as soon as possible.
18. Any images or videos of pupils will only be used as stated in the Shipbourne School camera and image use policy. I understand images of pupils must always be appropriate and should only be taken with Shipbourne School provided equipment and only be taken/published where pupils and/or parent/carers have given explicit written consent.

## **Classroom practice**

19. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Shipbourne School as detailed in the Child Protection Policy, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.
20. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider, in line with the Shipbourne School child protection policy. IT breach forms are held in Staff Share; safeguarding. Reports should also be made via Safeguard.software if a specific pupil is affected.
21. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the Child Protection policy, Staff Code of Conduct, Smart Technology and Mobile Phone policy and associated AUPs.
22. 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 by:
  - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
  - creating a safe environment where pupils feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
  - involving the Designated Safeguarding Lead (DSL) (Terri Daters) or a deputy (Alison Holmes/Julie Harvey) as part of planning online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
  - Informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
  - make informed decisions to ensure any online safety resources used with pupils is appropriate.
23. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

## **Mobile devices and smart technology**

24. I have read and understood the Shipbourne School mobile and smart technology and social media policies which addresses use by pupils and staff.
25. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff/code of conduct and the Shipbourne School mobile technology policy and the law.

## **Online communication, including use of social media**

26. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the child protection policy, staff behaviour code of conduct, social media policy and the law.
27. As outlined in the staff code of conduct and Shipbourne School social media policy:
- I will take appropriate steps to protect myself and my reputation, and the reputation of the school, online when using communication technology, including the use of social media.
  - I will not discuss or share data or information relating to pupils, staff, Shipbourne School business or parents/carers on social media.
28. My electronic communications with current and past pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
- I will ensure that all electronic communications take place in a professional manner via Shipbourne School approved and/or provided communication channels and systems, such as a Shipbourne School email address, user account or telephone number.
  - I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
  - I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers.
  - If I am approached online by a current or past pupils or parents/carers, I will not respond and will report the communication to my Head teacher and/or Designated Safeguarding Lead (DSL).
  - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or headteacher.

## **Policy concerns**

29. 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.

30. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
31. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the Shipbourne School into disrepute.
32. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the Shipbourne School child protection policy.
33. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with Shipbourne School child protection policy and/or the allegations against staff policy.

## **Policy Compliance and Breaches**

34. If I have any queries or questions regarding safe and professional practise online, either in Shipbourne School or off site, I will raise them with the DSL and/or the headteacher.
35. I understand that the Shipbourne School may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of pupils and staff. This includes monitoring all Shipbourne School provided devices and Shipbourne School systems and networks including Shipbourne School provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via Shipbourne School provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
36. I understand that if the Shipbourne School believe that unauthorised and/or inappropriate use of Shipbourne School devices, systems or networks is taking place, the Shipbourne School may invoke its disciplinary procedures as outlined in the staff code of conduct and disciplinary policy.
37. I understand that if the Shipbourne School believe that unprofessional or inappropriate online activity, including behaviour which could bring the Shipbourne School into disrepute, is taking place online, the Shipbourne School may invoke its disciplinary procedures as outlined in the staff code of conduct and disciplinary policy.
38. I understand that if the Shipbourne School suspects criminal offences have occurred, the police will be informed with the DBS notified where applicable.

# Visitor and Volunteer Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of our behaviour expectations and their professional responsibilities when using technology. This AUP will help Shipbourne School ensure that all visitors and volunteers understand the school 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, either provided to me by the Shipbourne School or accessed by me as part of my role within Shipbourne School, professionally and personally. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email, 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 Shipbourne 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 Shipbourne School ethos, Shipbourne School staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.
4. 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.
5. 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.
6. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the Shipbourne School into disrepute.

## Data and image use

7. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including UK GDPR.
8. I understand that I am not allowed to take images or videos of pupils.

## Classroom practice

9. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of pupils in line with the Curriculum, Teaching and Learning Policy, Positive Relationships Policy and Volunteer Policy.
10. I will support and reinforce safe behaviour whenever technology is used on site and I will promote online safety with the pupils in my care.
11. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the Shipbourne School community, I will report this to the DSL (Terri Daters), in line with the Shipbourne School child protection policy.
12. 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 mobile devices and smart technology**

13. In line with the Shipbourne School mobile and smart technology policy, I understand that mobile phones are not permitted in classrooms and should not be used where pupils are present.

### **Online communication, including the use of social media**

14. 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 child protection and social media policy.
  - I will not discuss or share data or information relating to pupils, staff, Shipbourne 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 Shipbourne School code of conduct/behaviour policy and the law.
15. My 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.
  - All communication will take place via Shipbourne School approved communication channels such as via a Shipbourne 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 my ability to comply with this will be discussed with the DSL (Terri Daters).

## Policy compliance, breaches or concerns

- 16. If I have any queries or questions regarding safe and professional practice online either in Shipbourne School or off site, I will raise them with the Designated Safeguarding Lead (Terri Daters).
- 17. I understand that the Shipbourne School may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of pupils and staff. This includes monitoring all Shipbourne School provided devices and Shipbourne School systems and networks including Shipbourne School provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via Shipbourne School provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
- 18. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers online to the Designated Safeguarding Lead (Terri Daters) in line with the Shipbourne School child protection policy.
- 19. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with the allegations against staff policy.
- 20. I understand that if the Shipbourne School believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the Shipbourne School may invoke its disciplinary procedures.
- 21. I understand that if the Shipbourne School suspects criminal offences have occurred, the police will be informed.

**I have read, understood and agreed to comply with Shipbourne School visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.**

Name of visitor/volunteer: .....

Signed: .....

Date (DDMMYY).....



# Wi-Fi Acceptable Use Policy

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

1. The Shipbourne School provides Wi-Fi for the Shipbourne School community and allows access for education purposes and personal communication purpose where it does not impact the wellbeing or education of pupils.
2. I am aware that the Shipbourne School will not be liable for any damages or claims of any kind arising from the use of the wireless service. The Shipbourne School takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the Shipbourne School premises that is not the property of the school/setting.
3. The use of technology falls under the Shipbourne School Acceptable Use of Technology Policy (AUP), child protection policy, social media and smart technology policy, staff code of conduct and positive relationships policy which all pupils/staff/visitors and volunteers must agree to and comply with.
4. The Shipbourne 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. Shipbourne 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 Shipbourne School service is adequately secure, such as up-to-date anti-virus software, systems updates.
7. The Shipbourne School wireless service is not fully secure, and the Shipbourne School cannot guarantee the safety of traffic across it. Use of the Shipbourne 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 Shipbourne School accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the Shipbourne 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 Shipbourne 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 Shipbourne School security and filtering systems or download any unauthorised software or applications.
- 11. My use of Shipbourne School Wi-Fi will be safe and responsible and will always be in accordance with the Shipbourne 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 Shipbourne School into disrepute.
- 13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Terri Daters) as soon as possible.
- 14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Terri Daters) or the headteacher.
- 15. I understand that my use of the Shipbourne School Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the Shipbourne School suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the Shipbourne School may terminate or restrict usage. If the Shipbourne 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.

**I have read, understood and agreed to comply with Shipbourne School Wi-Fi Acceptable Use Policy.**

Name .....

Signed: .....Date (DDMMYY).....