Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Super Star Pre-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 children, 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 Super Star Pre-school expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that setting 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 AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Super Star Pre-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 and online and offline communication technologies.

2. I understand that Super Star Pre-school Acceptable Use of Technology Policy (AUP) should be read and followed in line with the setting child protection policy and staff code of conduct.

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

Use of setting devices and systems

4. I will only use the equipment and internet services provided to me by the setting for example setting provided laptops, tablets, mobile phones, and internet access, when working with children.

5. 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 not allowed

6. Where I deliver or support remote/online learning, I will comply with the setting 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 setting systems. (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.)
    - I will protect the devices in my care from unapproved access or theft by not leaving devices visible or unsupervised in public places.

8. I will respect setting 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 Manager.

10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the Manager.

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the setting Information sharing and Record Keeping 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 setting 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 setting.

12. I will not keep documents which contain setting 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 setting learning platform to upload any work documents and files in a password protected environment or setting approved/provided VPN.

13. I will not store any personal information on the setting IT system, including setting laptops or similar device issued to members of staff, that is unrelated to setting activities, such as personal photographs, files or financial information.

14. I will ensure that setting 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 setting.

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 Manager, Sandra Burgess as soon as possible.

17. If I have lost any setting related documents or files, I will report this to the Manager, Sandra Burgess, who is also the setting Data Protection Officer as soon as possible.

18. Any images or videos of children will only be used as stated in the setting camera and image use policy. I understand images of children must always be appropriate and should only be taken with setting provided equipment and only be taken/published where children and/or parent/carers have given explicit written consent.

Classroom practice

19. 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.

20. I have read and understood the setting mobile and smart technology and social media policies.

21. I will promote online safety with the children 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 children 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) (Sandra Burgess) or deputy (Amy Corderoy) as part of planning online safety lessons or activities to ensure support is in place for any children who may be impacted by the content.
- make informed decisions to ensure any online safety resources used with children is appropriate.

22. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the setting child protection policy.

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 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 setting mobile technology policy and the law.

Online communication, including use of social media

25. 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 and staff code of conduct, social media policy and the law.

26. As outlined in the staff code of conduct and setting social media policy:
    - I will take appropriate steps to protect myself and my reputation, and the reputation of the setting, online when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to children, staff, setting business or parents/carers on social media.

27. My electronic communications with current and past children 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 setting approved and/or provided communication channels and systems, such as a setting email address, user account or telephone number.
    - I will not share any personal contact information or details with children, 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 children and/or their parents/carers.
    - If I am approached online by a current or past children or parents/carers, I will not respond and will report the communication to my line manager and (Sandra Burgess) 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 manager.

Policy concerns

28. 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.

29. 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.

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

31. I will report and record any concerns about the welfare, safety or behaviour of children or parents/carers online to the DSL in line with the setting child protection policy.

32. I will report concerns about the welfare, safety, or behaviour of staff online to the manager, in line with setting child protection policy and the allegations against staff policy.

Policy Compliance and Breaches

33. If I have any queries or questions regarding safe and professional practise online, either in the setting or off site, I will raise them with the DSL and/or the manager.

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

35. I understand that if the setting believe that unauthorised and/or inappropriate use of setting systems or devices is taking place, the setting may invoke its disciplinary procedures as outlined in the staff code of conduct.

36. I understand that if the setting believe that unprofessional or inappropriate online activity, including behaviour which could bring the setting into disrepute, is taking place online, the setting may invoke its disciplinary procedures as outlined in the staff code of conduct.

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

Reviewed 23rd July 2024
To be reviewed annually