WHINLESS DOWN ACADEMY
Staff Acceptable Use Policy
November 2023

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Whinless Down Academy Trust 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).

It 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 the Whinless Down Academy Trust expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that 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 school/Trust or accessed by me as part of my role within The Whinless Down Academy Trust, 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 the AUP should be read and followed in line with the Trust Child Protection & Safeguarding, online safety 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 Trust ethos, code of conduct and safeguarding policies, national education and child protection guidance, and the law.

Use of school/Trust devices and systems

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

5. I understand that any equipment and internet services provided by the Trust is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of Trust IT systems and/or devices by staff is not allowed.

6. I will not connect my own personal device e.g., phone or laptop to the school wifi.

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 locking access.

- I will follow the Whinless Down Password Policy. Passwords must comply with the expectation set out in the policy.
- I will protect the devices in my care from unapproved access or theft. I will not leave devices visible or unsupervised in public places.
- I will respect school/Trust system security and will not disclose my password or security information to others.

8. I will not open any hyperlinks or attachments in emails, even if it looks like it is from a trusted source. If I have any concerns or suspicion at all about email content sent to me, I will report them to the IT Technician immediately.

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT Technician or Headteacher.

10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the Trust 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 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 Trust.

11. I will not keep documents which contain school or Trust 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 WDAT trusted platforms, such as Onedrive, network drives or Teams, to upload any work documents and files.

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

13. I will ensure that the Trust 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.

14. I will not attempt to bypass any filtering and/or security systems put in place by the Trust.

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT technician or my line manager as soon as possible. If I have lost any Trust related documents or files, I will report this to the Headteacher as soon as possible.

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

<u>Classroom practice</u>

17. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by the Whinless Down Academy Trust, as detailed in the child protection/safeguarding and online safety policies, and in annual staff safeguarding training.

18. 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, in line with the Trust child protection and safeguarding policy.

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 children protection and safeguarding policies. I will ensure children are always supervised when accessing the internet.

20. 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.
- Informing the DSL and/or ICT technician 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 children are appropriate.

21. 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

22. I have read and ensure I meet the expectations of the Trust mobile and smart technology and social media policies which addresses use by children and staff.

Online communication, including use of social media

23. 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 safeguarding, online safety, and social media policies, the staff code of conduct and the law.

24. As outlined in the staff code of conduct and the Trust social media policy:

- I will take appropriate steps to protect myself and my reputation, and the reputation of the Trust, online when using communication technology, including the use of social media.
- I will not discuss or share data or information relating to children, staff, Trust/school business or parents/carers on social media.

25. 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 Trust approved and/or provided communication channels and systems, such as a school 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 Lead Designated Safeguarding Lead (DSL).
- Any pre-existing relationships/friendships/situations that compromise my ability to comply with the AUP will be disclosed on the Disclosure of Friends document at induction.

Policy concerns

26. 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.

27. 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.

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

29. 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 Trust child protection and safeguarding policy.

30. I will report concerns about the welfare, safety, or behaviour of staff online to the Headteacher, in line with Trust child protection and safeguarding policy and the allegations against staff policy.

Policy Compliance and Breaches

31. If I have any queries or questions regarding safe and professional practise online, either in school or off site, I will raise them with the Headteacher.

32. I understand that the school may exercise its right to monitor the use of its devices and information systems to monitor policy compliance and to ensure the safety of children and staff. This includes monitoring all school provided devices and school systems and networks, including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via 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.

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

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

I have read, understood and agree to comply with the Whinless Down Academy Staff Acceptable Use of Technology Policy when using Whinless Down devices and the internet and other associated technologies, both on and off site.

Name of staff member: ……

Signed: …….....

Date (DDMMYY)……...