The Aspire Academy Trust

Staff IT Acceptable Usage Agreement

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the academy and trust systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. Academy owned information systems must be used 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.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will not remove any IT equipment from the academy without prior authorisation from the trust IT team, or Academy leadership team.

4. I will respect system security and I will not disclose any password or security information and will use a 'strong' password (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 and is changed regularly or when required by the academy trust. Mobile devices will be protected with a passcode or using an approved biometric system. This will be in line with the measures set out in the IT Technical Security Policy.

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the trust IT team. Apps installed on tablet and mobile devices should be for educational purposes and are monitored by the trust IT team.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that 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 (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN).

7. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Where possible, I will use the Office

365 platform as a means of accessing and sharing data remotely. Any images or videos of pupils will only be taken and used as stated in the Trust image use policy and will always take into account parental consent. Please refer to the Trust Data Protection policy for further guidance. I will respect copyright and intellectual property rights.

8. Unencrypted memory sticks and removable storage should not be used within the school environment due to the associated risks that the carry for data protection and IT system security.

9. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, tablets, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the Office 365 platform to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft. When using a personal device for work purposes, I will abide by the Trust Bring Your Own Device (BYOD) guidance.

10. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, audio and video files or financial information.

11. I have read and understood the school Digital Safeguarding policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

12. I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Child Protection Coordinator and/or the IT Manager as soon as possible.

13. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the trust IT team as soon as possible.

14. 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 at all times. No personal contact information will be provided to pupils and parents and all communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with a Senior Leader.

15. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not

undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

16. I will ensure that my online activity, both in school and outside school, will not bring the academy or trust, my professional role, or that of others into disrepute.

17. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the academy, or the Aspire Academy Trust, into disrepute.

18. I will access my work e-mails on a regular basis during each working week. I understand that email should be used carefully and appropriately and it should be understood that an email can be classed as a legally binding document.

19. 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 in line with the trust Digital Safeguarding policy.

20. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Child Protection Coordinator and/or the IT Manager or the Academy leadership team.

21. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The Trust may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy, the Digital Safeguarding Policy and the Trust's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the Trust will invoke its disciplinary procedure. If the Trust suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: …….. Print Name: …… Date: ……

Accepted by: ……. Print Name: ……