Chilton Academy

Adult/Staff Acceptable Use Policy (2019/20)

IT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in the academy. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs. A. Pybus (Headteacher) or Fiona Brady (Online Safety co-ordinator).

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 academy'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 school 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 academy ethos, other appropriate policies 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 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.

Mobile Phones

a) Staff are responsible for their own mobile phones. These must be stored away during the school day and remain on silent. Mobile phones may only be used before/after school or during break times when children are not present.

b) Staff mobile phones will never be used for any reason when children are present.

c) Cameras on personal phones or tablets will not be used to take pictures of children in any circumstances.

d) Staff mobile phones are allowed in the academy, but are not allowed to be used in sensitive areas (EYFS, cloak rooms, toilets, when children are changing, swimming). Mobile phones should only be used for communication when not working with children and there are no children present.

e) In the unlikely event of needing to contact a parent directly an academy mobile phone will be issued to the member of staff concerned.

4) I understand that any device or hardware provided for by the academy is to be mainly used to complete official academy work. Use of any device for personal use, outside of academy hours, is permitted, providing any actions/activities are lawful and in keeping with the ethos of the academy.

5) Personal use of academy ICT systems and connectivity is only permitted outside of the academy day and only permitted when children are not present.

6) 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.

7) I will respect system security and I will not disclose any password or security information. I 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).

8) I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

9) Data Protection - School should have a separate Data Protection Policy

a) I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. 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) or accessed remotely. Any personal data which is being removed from the academy site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the academy. Secure means of transporting data are encrypted laptop / encrypted USB memory / encrypted HDD /Google Drive.

b) If I choose to use a portable device (Phone, Tablet etc…) to collect my work e-mail I will ensure that the device is locked by a pin code or password and will be wiped when I dispose of the device.

Chilton Academy

c) I will not transfer sensitive personal information from my academy e-mail account (e.g. Support Plans, Safeguarding Reports, Medical Information) UNLESS the information is encrypted.

d) I will not keep professional documents which contain academy-related personal information (including images, files, videos etc.) on any personally owned devices (such as laptops, digital cameras, mobile phones).

e) Digital Images or videos of pupils will NOT be taken away from the academy premises OR only taken from the academy premises using encrypted memory OR alternative secure transport method.

f) I will not use unapproved cloud storage systems (Dropbox, icloud etc) for storing personal data of staff or pupils.

10) I will not store any personal information on the academy computer system that is unrelated to academy activities, such as personal photographs, files or financial information.

11) I will respect copyright and intellectual property rights.

12) <u>Social Media</u>

a) I have read and understood the Academy Online Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media.

b) I will not communicate with parents, pupils or ex-pupils under the age of 18 using any personal social media account. Any communication with parents must be completed through the official Chilton Academy Twitter account (see point 'e').

c) If any request is made by pupils or parents, staff should take a photo/screen shot and report this to Online Safety Co-ordinator / Headteacher (Mrs. A. Pybus/F. Brady). Parents will then be informed and a discussion will take place with parents about the appropriate use of social media. This will then be logged in the online safety incident record.

d) My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via academy twitter, an academy provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team. This would include any relatives of current pupils that are my "friends" on a social media site.

Chilton Academy

e) My use of ICT and information systems will always be compatible with my professional role, whether using academy or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

f) 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 County Council, into disrepute. This would include any comment made, even in the belief that it is private on social media.

13) I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator (Mrs. A. Pybus) and the Online Safety Coordinator (Ms. F. Brady) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Online Safety Coordinator the designated lead for filtering as soon as possible.

14) I will not attempt to bypass any filtering and/or security systems put in place by the academy. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any academy-related documents or files, then I will report this to the Eden Learning trust ICT Support as soon as possible.

15) I will promote e-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.

16) If I have any queries or questions regarding safe and professional practise online either in academy or off site, then I will raise them with the Online Safety Coordinator or the Head Teacher.

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

The Academy 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 and the Academy'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 Academy will invoke its disciplinary procedure. If the Academy 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.

Chilton Academy

I have read and understood and agree to comply with the **Adult/Staff ICT Acceptable Use Policy.**

Signed: ………………………….. Print Name: ……………………… Date: ………

Accepted by: ………………………….. Print Name: ………………………….