SEPT 2022

ICT ACCEPTABLE USE FOR STAFF POLICY

DOCUMENT CONTROL	
ISSUED	CHANGES FROM PREVIOUS VERSION
Date reviewed: Sept 2022 Date of next review: Sept 2023 Reviewer: Executive Headteacher (Dr. Kim Taylor), Acting Head of School – RMA (Andrew Armstrong) Date of ratification by Governing Board: TBC	Wording added to section 'Personal Use' **Personal ICT equipment, including mobile phones and computers, should never be used to contact students, parents or guardians, nor take photographs or engage in email or social media without prior authorisation from the Headteacher due to potential safeguarding issues and GDPR security.** **Staff members found to have such devices on their person, or using devices for photographs may be subject to misconduct procedures due to not following the safeguarding and acceptable use of ICT policies** Wording added to section 'Access to employee communications and files' **5. The school reserves the right, at its discretion, to review anyone's electronic files and messages of any employee to the extent necessary to ensure business continuity in the event of long term absence or resignation.** Section added called 'Mobile Phones' **The use of personal mobile phones is prohibited in areas of the school that can be accessed by students and access to such devices should be limited to before and after school, and when on a scheduled break. At all other times phones should be locked away in personal lockers or left in another secure location.**

Introduction

Staff must accept that any computer used or laptop loaned by the school is provided solely to support their professional responsibilities. They must only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head Teacher.

Data Protection

Data protection law require that any information seen by individuals with regard to staff or pupils which is held within the school's management information system must be kept private and confidential, EXCEPT when required by law to disclose such information to an appropriate authority.

Staff must ensure all documents; data etc. are saved, accessed and deleted in accordance with the school's data security and confidentiality protocols.

Login passwords which allow access to work stations, information systems or email must be in accordance with guidelines and must not be divulged to anyone except when requested by Senior Management or for reasons of technical support.

Prohibited Use

Electronic media cannot be used for knowingly viewing, transmitting, retrieving, or storing anything that is:

1. discriminatory or harassing
2. derogatory to any individual or group
3. obscene, sexually explicit or pornographic
4. defamatory or threatening
5. in violation of any license governing the use of software
6. engaged in any purpose that is illegal or contrary to the school policy or interests or reputation.

Personal Use

The computers, electronic media and services provided by the school are for educational use to assist staff in the performance of their job. Limited, occasional, or incidental use of electronic media for personal purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the system's use for their educational purposes and outside school contact hours.

Personal ICT equipment, including mobile phones and computers, should never be used to contact students, parents or guardians, nor take photographs or engage in email or social media without prior authorisation from the Headteacher due to potential safeguarding issues and GDPR security.

Staff members found to have such devices on their person, or using devices for photographs may be subject to misconduct procedures due to not following the safeguarding and acceptable use of ICT policies.

However, accessing social networking sites (such as Facebook or Twitter) is **not** permitted on school site using the school's internet connection, including non-timetabled periods and break or lunch times.

In addition, no reference should EVER be made to Horizons Education Trust or it's associated schools on any social networking site.

Access to employee communications and files

Generally, electronic information created and/or communicated by staff using email, word processing, spreadsheets, internet and similar electronic media is not reviewed by the school. However, the following conditions should be noted:

1. The school can gather logs of electronic activities and monitor use for detecting patterns which indicate individuals are violating school policies or engaging in illegal activity.
2. The school reserves the right, at its discretion, to review anyone's electronic files and messages of any employee to the extent necessary to ensure electronic media and services are being used in compliance with the law and this and other school policies.
3. Staff should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit to an address outside the springcommon.cambs.sch.uk domain, they should use other means.
4. As far as possible pupil named data should not be transmitted over the Internet or email. Senior Management should be consulted in order to ensure that information sharing guidelines are followed.
5. The school reserves the right, at its discretion, to review anyone's electronic files and messages of any employee to the extent necessary to ensure business continuity in the event of long term absence or resignation.

Software

To prevent breach of licensing regulations, only software registered through the school may be installed onto school owned equipment. Before downloading or installing any software you must seek advice and permission from the Head Teacher. Any violations by members of staff may be subject to disciplinary action.

Security and responsibility

All employees have a responsibility to maintain the security of school equipment and should:

1. Ensure laptops are physically secure at the end of the school day.
2. Report any loss or damage to equipment immediately to the Head Teacher.
3. Not divulged their login details to anyone and not log anyone else on as them.
4. Never leave their computer unattended whilst logged in – always lock your computer.
5. Always logout and shutdown at the end of each day
6. Never allow pupils to access devices when logged on as a member of staff
7. Not allow pupils to use designated administration machines, as they could gain access to privileged information and therefore contravene the Data Protection Act.

Any violations by members of staff may be subject to staff disciplinary procedures.

Appropriate Use

Staff should only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

Except in extreme cases in which explicit authorisation granted by the Head Teacher no employees can engage in:

1. monitoring or intercepting the files or electronic communications of other staff or third parties.
2. hacking or obtaining access to systems or accounts they are not authorised to use.
3. breaching, testing, or monitoring computer or network security measures.
4. send email or other electronic communications which attempt to hide the identity of the sender or represent the sender as someone else.
5. copying, retrieving, modifying or forwarding copyrighted materials except as permitted by the copyright owner.
6. Represent views about the school, its staff, volunteers, trustees, parents or pupils

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password protected and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

External storage devices with photos or data relating to pupils or staff must not be taken off site.

Participation in online activity

Although we cannot dictate whether or not staff participate with online social networking in their own time, the school strongly advises that staff do not participate in such activities (including, but not limited to, Facebook, Twitter and Instagram).

If staff or volunteers decide to involve themselves in social networking, the consequences of inappropriate updates (including text, images and videos) become their sole responsibility. Be aware that should any inappropriate text, images or video comes into the public domain, staff will be in breach of this agreement and it will lead to disciplinary investigation and therefore open to disciplinary action which could include dismissal.

School guidelines on appropriate use and security settings must be adhered to as any violation by members of staff or volunteers approved by the school may be subject to disciplinary action.

In addition, staff must ensure that any private blogs, bulletin boards, websites etc. that they create or actively contribute to do not compromise and are not confused with their professional role. There is no circumstance when staff may represent the school online through any medium without specific agreement from the Head Teacher.

Staff must ensure that any engagement in any online activities does not compromise their professional responsibilities.

Services:

The school will not accept responsibility for damage or loss for use of the network system.

Mobile Phones:

The use of personal mobile phones is prohibited in areas of the school that can be accessed by students and access to such devices should be limited to before and after school, and when on a scheduled break. At all other times phones should be locked away in personal lockers or left in another secure location.

Media publications:

Written permission is obtained from parents before photographs or names of pupils can be published. Students work may not be published in any form without consent of the Head Teacher and appropriate agreement from parents. All photographs, images or written text from school is the property of the school and appropriate permission from the Head Teacher or Trustees is a requirement to protect the privacy of pupils and staff.

This policy links to:

- All personnel policies for staff approved by trustees.
- Safeguarding and child protection policies
- 'Keeping Children safe in Education'
- Working together to safeguard children
- Whistle blowing Policy
- PREVENT training
- Equalities Policy
- E- Safety Policy
- Data Protection Policy

All terms and conditions for this policy must be accepted using the agreement form enclosed. Staff and volunteers must sign to agree and understand this policy within 5 working days of issue.

Acceptable use of ICT 2020 – Horizons Education Trust

Employee acceptance form:

Name of employee:

Date issued:

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of Horizons Education Trust's computers, networks and telecommunications equipment and services. I understand that I have no expectation of privacy when I use any of the equipment or services. I am aware that violations of this guideline may subject me to disciplinary action, including termination of employment, legal action and criminal liability.

I further understand that my use of email and the Internet may reflect on the image of Spring Common Academy to our pupils, parents, trustees and suppliers and that I have responsibility to maintain a positive representation of the school at all times. Furthermore, I understand that this policy can be amended at any time.

I agree to the following set of rules for the implementation of this Acceptable use Policy as follows:

1. I will not create, transmit, display or publish any material that is likely to: harass, cause offence , inconvenience or needless anxiety to any other person or bring the reputation of the school into disrepute.
2. I will use appropriate language and remember that I am a representative of the school on a global public system. I accept illegal activities of any kind are forbidden.
3. I will not use language that could be calculated to incite against ethnic, religious or any minority group.
4. I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have usage monitored.
5. Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details0 of other users to any unauthorised person. I will not reveal personal information to pupils past or present or parents.
6. I will not trespass into other users files or folders.

7. I will ensure my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
8. I will ensure that if I think someone has learned my password then I will change it immediately and contact the Head Teacher to advise.
9. I will ensure I log off after my network session has finished.
10. If I find an unattended machine logged on under another users name I will not continue using this machine. I will log off immediately.
11. I will not use personal use personal digital cameras or camera phones for creating or transferring images of children, young people or vulnerable adults without express permission of the Head Teacher.
12. I am aware that e- mail is not guaranteed to be private. Messages relating to or in support of illegal activities or that bring the school into disrepute will be reported to the authorities. Anonymous messages are not permitted by staff or others.
13. I will not use the network in any way that would disrupt use of the network by others.
14. I will report any accidental access, receipt of inappropriate materials or filtering breaches, unsuitable websites to the Head Teacher.
15. I will not use USB drives, portable hard drives, tablets or personal laptops on the network without having them approved by the school and checked for viruses.
16. I will not attempt to visit websites that might be considered inappropriate or illegal or incite others to do this particularly children in my care. I am aware that downloading material is illegal in school and the police or other authorities may be called to investigate such use.
17. I will not download any unapproved software, system utilities or resources from the internet that may compromise the network or are not adequately licensed.
18. I will not accept invitations from children, young people or vulnerable adults past or present in school to add me as a friend to any social networking site, nor will I invite them to be friends on mine.
19. Damage to professional reputation can be caused by quite innocent postings or images. I will also take great care and accept responsibility for anyone who can access on to my pages through friends or friends of friends. I will take care that no images or text can be shared with school parents or their children past or present, especially in connection with my professional role or duties.
20. I will ensure that any private social networking sites / blogs or other social media that I create or actively contribute to, are not confused or lead to my professional role.
21. I will not retain images of children for personal use or post on social media sites.
22. I will not retain images of staff at work for personal use or for social media sites.
23. I will not publish material that violates data protection Act or breach the security this act requires for personal data, including data held in SIMS or on the SIMS products.
24. I will not receive, send or publish material that violates copyright law. This includes materials sent / received using video conference or web broadcasting or similar.

25. I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
26. I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used and accept this responsibility.
27. I will ensure that any personal data Where the data protection Act applies) that is sent over the internet (or taken offsite in any other way) will be encrypted or otherwise secured.

Policy agreed on: ……

Signed …….