I have come that they may have life and have it to the full
(John10:10)

STAFF ACCEPTABLE USE POLICY AND AGREEMENT

This policy is taken from the OLHOC Trust Handbook of Statutory policies and should be read in conjunction with the other policies within the document.

Revised Edition September 2023

STAFF ACCEPTABLE USE POLICY AND AGREEMENT

1. Introduction

1.1. This policy is designed to enable acceptable use for staff and governors.

1.2. The Trust provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of staff, governors and students, it is important that all staff and governors follow the guidelines detailed below.

1.3. This policy aims to:

1.3.1. Promote the professional, ethical, lawful and productive use of the Trust's ICT systems and infrastructure.

1.3.2. Define and identify unacceptable use of the Trust's ICT systems and external systems.

1.3.3. Educate users about their data security responsibilities.

1.3.4. Describe why monitoring of the ICT systems may take place.

1.3.5. Define and identify unacceptable use of social networking sites and Trust devices.

1.3.6. Specify the consequences of non-compliance.

1.4. This policy applies to employees, governors, trustees, members and directors along with all users of the Trust's ICT systems, including but not limited to, contractors, consultants, volunteers, casual or agency staff (collectively referred to as "Staff" in this policy. All Staff are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action for employees or other appropriate alternative action for other Staff.

1.5. The use by Staff and monitoring by the Trust of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the Trust's Data Protection Policy for further information. This policy should also be read in conjunction with the Trust's Electronic Information and Communications Systems Policy, Social Media Policy and Whistleblowing Policy.

1.6. If you are in doubt and require clarification on any part of this document, please speak to the CEO / Principal / Head Teacher.

2. Provision of ICT Systems

2.1. All equipment that constitutes the Trust's ICT systems is the sole property of the Trust.

2.2. No personal equipment should be connected to or used with the Trust's ICT systems. Users must not try to download, install or run any software on the ICT systems without permission from the IT Manager. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

2.3. The IT Manager is responsible for purchasing and/or allocating ICT equipment to individuals throughout the Trust. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

2.4. Users are not permitted to make any physical alteration, either internally or externally, to the Trust's computer and network hardware.

3. Network access and security

3.1. All users of the ICT systems at the Trust must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address.

3.2. All passwords should be complex to ensure data and network security. Best practice as recommended by the National Cyber Security Centre is to use three random words. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

3.3. All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to designated members of the IT Support Staff for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to their line manager, the CEO / Principal / Head Teacher or IT Manager as soon as possible.

3.4. Users should only access areas of the Trust's computer systems to which they have authorised access.

3.5. When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the Trust's ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the Trust's ICT systems or cause difficulties for any other users.

3.6. Under no circumstances should a student be allowed to use a Staff computer account, unless being directly supervised by the account owner.

4. Trust E-mail

4.1. Where e-mail is provided, it is for academic and professional use, with no personal use being permitted. The Trust's e-mail system can be accessed from both the Trust's computers, and via the internet from any computer. Wherever possible, all Trust-related communication must be via the Trust's e-mail address.

4.2. The sending or re-sending of e-mails is subject to the following rules:

4.2.1. Language must not include swear words or be offensive or abusive.

4.2.2. E-mails or attachments of a pornographic, illegal, violent, sexist, or racist nature are not permitted.

4.2.3. Sending e-mails or attachments which contain copyright material to which the Trust does not have distribution rights is not permitted.

4.2.4. The use of personal e-mail addresses by Staff for any official Trust business is not permitted.

4.2.5. The forwarding of any chain messages/junk mail or trivial messages etc. which may contribute to system congestion is not permitted. Spam or junk mail will be blocked and reported to the e-mail provider.

4.2.6. Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) or is confidential in nature will only be sent using secure and encrypted e-mail or password protection. Sending such e-mails by unsecure means is prohibited.

4.2.7. E-mails should never contain children's full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible.

4.2.8. Access to Trust/setting e-mail systems will always take place in accordance with data protection legislation and in line with other appropriate Trust/setting policies e.g. confidentiality.

4.2.9. Members of the community must immediately tell a designated employee if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).

4.2.10. Staff will be encouraged to develop an appropriate work life balance when responding to e-mail.

4.2.11. E-mails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on Trust or academy headed paper would be.

4.2.12. Trust -email addresses and other official contact details will not be used for setting up personal social media accounts.

4.2.13. Where possible e-mails must not contain personal opinions about other individuals, e.g. about Staff, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

4.2.14. E-mails selling or advertising goods or services or broadcasting messages about sponsorship or charitable appeals or lost property should not be sent, as other more appropriate forums are available for these purposes.

4.2.15. Staff must not agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained.

4.2.16. The sending of e-mails from another worker's computer under an assumed name is prohibited unless written authorisation has been granted.

5. Internet Access

5.1. Internet access is provided for academic and professional use with no personal use being permitted.

5.2. The Trust's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in an education setting. In this case the website must be reported immediately to the Trust CEO or CEO / Principal / Head Teacher.

5.3. Staff must not therefore access from the Trust's system any web page, or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

5.4. Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

5.4.1. Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;

5.4.2. transmitting a false and/or defamatory statement about any person or organisation;

5.4.3. sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;

5.4.4. transmitting confidential information about the Trust and any of its Staff, students or associated third parties;

5.4.5. transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee, member of Staff or for the Trust);

5.4.6. downloading or disseminating material in breach of copyright;

5.4.7. copying, downloading, storing or running any software with the express prior authorisation of the IT Manager;

5.4.8. engaging in online chat rooms, instant messaging, social networking sites and online gambling;

5.4.9. forwarding electronic chain letters and other materials;

5.4.10. accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child;

5.4.11. accessing sites promoting radicalisation, terrorism etc.

5.5. Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

5.6. Where evidence of misuse is found the Trust may undertake a more detailed investigation in accordance with the Trust's Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

5.7. If necessary, such information may be handed to the police in connection with a criminal investigation.

6. Digital cameras

6.1. The Trust encourages the use of digital cameras and video equipment; however, Staff should be aware of the following guidelines:

6.1.1. Photos should only be named with the student's name if they are to be accessible within the Trust or the academy in which you work only. Photos for the website or press must only include the child's first name.

6.1.2. The use of personal digital cameras within the Trust is not permitted, including those which are integrated into mobile phones, iPads or similar.

6.1.3. All photos should be downloaded to the Trust network as soon as possible.

6.1.4. The use of personal mobile phones /tablets for taking photos, electronic images or audio of students is not permitted.

7. File Storage

7.1. Staff users will have their own personal area on the network, as well as access to shared network drives, if appropriate. Any Trust-related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files.

7.2. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

7.2.1. If information/data has to be transferred it must be saved on an encrypted, password protected, storage device

7.2.2. No Trust data is to be stored on a home computer, or un-encrypted storage device.

7.2.3. No confidential, or Trust data which is subject to the Data Protection Act 2018 should be transferred off site unless it is sent by secure e-mail.

8. Mobile Phones

8.1. Mobile phones are permitted in the Trust, with the following restrictions:

8.1.1. They are not to be used when Staff are directly supervising or working with children. Whilst Staff are working in the classroom mobile phones should be securely stored in a bag/cupboard/locker.

8.1.2. Personal mobile phone cameras are not to be used on school trips organised by the Trust. The Trust provides digital cameras/trip phones for this purpose.

8.1.3. All phone contact with parents regarding Trust issues will be through the Trust's phones where available. Personal mobile numbers should not be given to parents of students of the Trust.

8.1.4. In the event of a trust mobile phone not being available staff may use their personal mobile phones to contact parents but must withhold their number.

9. Social networking

9.1. The Trust has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

9.1.1. Staff have a responsibility to protect the reputation of the Trust, staff and students at all times and that they treat colleagues, students and associates of the Trust with professionalism and respect whilst using social networking sites.

9.1.2. Social networking sites should be used responsibly, and users should ensure that neither their personal or professional reputation and/or the Trust's reputation, nor the reputation of individuals within the Trust are compromised by inappropriate postings.

9.1.3. Use of social networking sites for Trust business is not permitted, unless via an officially recognised Trust site and with the permission of the CEO / Principal / Head Teacher.

9.1.4. Staff will notify the CEO / Principal / Head Teacher if they consider that any content shared or posted via any information and communications technology, including e-mails or social networking sites conflicts with their role in the Trust/setting.

9.1.5. No Trust information, communication, documents, videos and/or images should be posted on any personal social networking sites.

9.1.6. No details or opinions relating to any student are to be published on any website.

9.1.7. Users must not knowingly cause annoyance, inconvenience, or needless anxiety to others (cyber bullying) via social networking sites.

9.1.8. No opinions regarding another member of Staff, which could cause offence, are to be posted.

9.1.9. No photos or videos, which show students of the Trust who are not directly related to the person posting them, should be uploaded to any site other than the Trust's website.

9.1.10. No comment, images or other material may be posted anywhere, by any method that may bring the Trust, its academies or, the profession into disrepute.

9.1.11. Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook).

10. Monitoring of the ICT Systems

10.1. The Trust may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the Trust's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the CEO / Principal / Head Teacher to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

10.2. Other reasons for monitoring the ICT systems include the need to:

10.2.1. ensure operational effectiveness of the services provided;

10.2.2. maintain the systems;

10.2.3. prevent a breach of the law, this policy, or any other Trust policy;

10.2.4. investigate a suspected breach of the law, this policy, or any other Trust policy.

10.3. Please refer to the Trust's Electronic Information Communications and Systems Policy and Monitoring the Use of Information Systems Policy for further information.

11. Failure to Comply with the Policy

11.1. Any failure to comply with this Staff Acceptable use Policy may result in disciplinary action.

11.2. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

11.3. Any unauthorised use of the Trust’s ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the CEO / Principal / Head Teacher considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

11.4. The Trust reserves the right to audit and/or suspend a user’s network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.