The Auriga Academy Trust

Staff ICT Usage Policy

CONTENTS

APPENDICES

1. Scope

The ICT Usage Policy ("this Policy") applies to employees who are directly employed by schools within the Trust.

It applies to all users of the school's network and the use of the school's ICT facilities, (including telephones, hardware, software, e-mail, internet etc) used anywhere, for professional or personal purposes whether in working time or in the employee's own time.

Please refer to the Social Media Policy for further guidance on the use of social networking sites and other technology.

2. Purpose

The purpose of this policy is to protect employees by making clear what is acceptable use of the school's ICT facilities. Protect the security and integrity of the school and its ICT facilities and all personal data.

3. Policy

High standards of conduct and probity are as relevant to the use of the school ICT facilities as they are to all other aspects of work, and employees must conduct themselves in line with the school's code of conduct and disciplinary code.

Employees who are in any doubt about what is, or is not, acceptable use of the school's ICT facilities must seek advice from their manager or the designated ICT person in advance of the use.

Employees must conduct themselves honestly, appropriately and in accordance with the law and this policy when using the school's ICT facilities.

Breach of this policy may lead to disciplinary action and result in withdrawal of access to some or all ICT facilities. Serious breaches may be regarded as gross misconduct and may lead to dismissal.

Employees are required to sign a statement agreeing to the terms and conditions of this policy (Appendix 1). Managers must ensure that employees have the relevant skills to use the school's ICT facilities.

The school will co-operate with any law enforcement activity.

4. Access

The school provides access to ICT to enable employees to undertake their duties as specified by their job description. Access to ICT through school is not intended for personal use, please see paragraph 6 for further information. On this basis, the Headteacher, or another designated senior person, has authority to obtain access to an employee's data and documents, including emails.

Employee's wishing to use school ICT equipment (e.g. laptop / chrome book) at home must seek permission from their line manager and sign the relevant documentation accepting responsibility for loss or damage. Please see **Appendix 2: School Equipment Agreement.**

Employees are permitted to use their own ICT equipment during breaks. However, personal ICT equipment can only be used in a place not accessible to students.

5. Monitoring

Each employee will be required to sign the Statement of Acceptance of the Terms and Conditions of the ICT Usage Policy (**Appendix 1**). The school's ICT facilities will be monitored to ensure this policy is adhered to and that these facilities are used properly.

Any information (including personal emails, documents, etc) within the school's network or equipment can be inspected, at any time, without notice.

6. Personal Use

Employees can use the school's ICT facilities for occasional personal use provided it:

- Does not interfere with the performance of their duties;
- Is appropriate;
- Is on an occasional, rather than a regular or substantial basis;
- Does not compromise the security of the school's systems or reputation.

7. Inappropriate Use

Employees must **not** use the school's ICT facilities to:

- Send or access messages that are, or perceived to be, libelous, harassing or defamatory, or cause offence to the dignity of an individual or group.
- Access inappropriate internet sites or material. These may include pornographic, racist or any other sites not appropriate for a school. In the case of accidental access, the employee must immediately disconnect and inform their manager.
- Store, view, print or redistribute any inappropriate material.
- Access chat rooms, social networking sites or newsgroups for personal use.
- Advertise or send personal messages to large groups internally or externally unless through a specified facility or with the permission of an authorised person.
- Spread harmful programs that may damage the school's computer facilities; download, use or distribute software including entertainment software or games; download video and audio streaming for personal purposes.
- Use their school e-mail address for the purchase of personal goods or financial transactions.

8. Authority to Express Views

Employees using the school's ICT facilities must communicate the school's, and not their personal, views.

Employees must not participate in newsgroups / chat rooms / social networking sites, unless in a professional capacity relevant to their duties and with prior agreement from their manager or the designated authorised person.

Employees must not use the school or its name to endorse any commercial product or service.

9. Confidentiality and Security of Data

The school is legally responsible for all information stored or transmitted by its computer systems and for any improper disclosure. Disclosure of data, even unintentionally, can breach the General Data Protection Regulations 2018 and the Data Protection Act 2018.

Security measures are in place to ensure the confidentiality of data held by the school and employees are accountable for breaches of security or confidentiality.

- Employees must not attempt to disable or evade any security facility.
- User IDs and passwords must be kept secure and confidential, and passwords changed if an unauthorised person may be aware of them. It is recommended that passwords are automatically updated every 3 months.

- Employees must carefully address e-mails to avoid sending sensitive information to the wrong recipient. In addition, attachments and links to files should be double checked before an email is sent. In the event an email is sent to the wrong person, or with the wrong attachment or link, a data breach MUST be logged.
- Employees must ensure that data they are storing, updating or transmitting is accurate, and must not amend or alter e-mails they receive.
- To ensure security, it may be necessary to prevent equipment with sensitive data from connecting to the internet or restrict usage of file transfers.
- Employees must use the appropriate system/method e.g., password-protected screen saver, if leaving their computer for short periods and switch computers off at the end of the working day.
- Governors and Trustees should only use their designated school email account for all matters concerning school business.
- Laptops/tablets/phones provided by the school for work purposes should only be used by the employee who has been assigned the equipment. The employee must at all time use all reasonable efforts to keep the equipment secure off site.
- USB sticks should not be used under any circumstances.

10. Copyright

Downloading and copying data and software or sending the work of others to third parties without permission can infringe copyright. The Trust retains the copyright to all materials produced by an employee in the course of their duties, including any original ICT based material produced.

- Copyright should be checked and appropriate permissions sought. In the case of subscription services the appropriate licenses must be obtained.
- Software can only be downloaded with permission from the Headteacher or the designated authorised ICT person. Downloaded software becomes the school's property and must be used only under the terms of its license.
- Employees must arrange to license and register such software, where required. Software downloaded without permission must be deleted.
- Employees must not transfer any software licensed to the school or data owned or licensed by the school without authorisation from the Headteacher or the designated ICT person.
- The use of ICT facilities can lead to contractual obligations in the same way as verbal or written transactions. Employees must not exceed their delegated authority to enter into contracts or authorise expenditure.
- Records of computer transactions must take place through archiving or backup. Where appropriate, confirmation of receipt of important e-mails must be gained which may be disclosed in litigation.
- Transactions through any ICT facility must be treated in the same way as transactions on the school's headed paper.

11. Network Efficiency

Employees must regularly delete or archive files no longer required or needed for immediate access. The school's ICT unit will scan all files for viruses.

Wherever possible intensive operations such as large file transfers, video downloads, mass e-mailing should be scheduled during off-peak hours.

Video and audio streaming and downloading must be for work purposes only.

12. Software

The school must ensure all software is legally licensed and is responsible for managing and maintaining the register of software and for holding licenses and the original media.

- No software can be loaded onto or used on any computer owned or leased unless approved by and licensed to the school.
- All software must be procured by the school and installed by the designated authorised ICT person.
- Software must not be copied or distributed by any means without prior approval from the Headteacher or the designated authorised ICT person.

Appendix 1

Statement of Acceptance of the Terms and Conditions of the ICT Usage Policy

I agree to follow the rules set out in the ICT Usage Policy.

I will use the school's ICT network in a responsible way and observe all the restrictions explained in the Policy. If I am in any doubt I will consult _____ *(name of Headteacher)*.

I agree to report any misuse of the school's ICT network to _____ *(name of headteacher)*.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to _____ *(name of Headteacher)*.

I understand that any breaches of the Policy may result in loss of access to the ICT facilities and will be subject to disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Name of Employee: _____

Signature of Employee: _____

Date:_____

Appendix 2

SCHOOL EQUIPMENT AGREEMENT

EQUIPMENT ASSIGNED:

Item: (e.g. laptop, Ipad):

Serial Number:

I assume responsibility for the equipment assigned to me and will adhere to the following -

The equipment is:

- used appropriately and only for school use
- NOT used to access any information that would put out pupils in danger or our school into disrepute
- NOT used to access any social medial platforms, e.g. Instagram and face book
- NOT lent to anyone outside of school
- stored securely and I recognise I am responsible for the equipment whilst travelling. I accept personal liability for this equipment and acknowledge that I will bear the cost of the equipment in the event of damage or loss due to theft or otherwise.
- I will report any defects, faults, accidents, damage or loss immediately to school including reporting to the police if appropriate.

Receiving:

Signature: _____Date: _____

Issuing Staff:

Signature: _____Date: _____

Returned by:

Signature: _____Date: _____

Received by:

Signature: _____Date: _____