Frays Academy Trust
ICT Usage Policy

Date Ratified: May 2018
Review Date: May 2021

Approval

Signed by Chair of Directors	
Date of Approval/Adoption	May 2018
Date of Review	May 2021

Notes on Document

This document is the property of the Frays Academy Trust and its contents are confidential. It must not be reproduced, loaned or passed to a third party without prior permission from the Chief Executive.

It is controlled within the Frays Academy Trust admin server where the electronic master is held and can be accessed on a read only basis, subject to security permissions.

Paper or electronic copies may be taken for remote working etc. However, all paper copies not held within the admin server are uncontrolled. Hence the footer 'DOCUMENT UNCONTROLLED WHEN PRINTED' which must not be changed.

Once issued, as a minimum this document shall be reviewed every three years or as necessary by the originating team/committee.

To enable continuous improvement, all readers are encouraged to notify the author of errors, omissions and any other form of feedback.

Version	Status and Purpose	Policy Author	Changes Overview
1 April 2011	Policy Creation	Chief Executive	Policy Creation
2 May 2018	Policy Review	Chief Operating Officer	Policy updated to reflect new GDPR guidance. Section 2 "Policy Purpose" updated to include the following:- • Protect the security and integrity of the Trust personal data and computer systems. Section 3 "Policy" updated to include the following:- • At all times desktop/laptop/tablets will be password protected and screens not left open. • Hard drives will only be used under the agreement of the Head of School/CEO where an Apple-Mac computer has been issued by the school. It shall be the responsibility of the Head of School/CEO to ensure the hard drives are password protected. • Memory sticks will not be used within Frays Trust Schools, as all schools have wi-fi access and Staff/Directors/Governors can use remote access systems. Section 9 "Confidentiality and Security of Data" updated to include the following:- • Laptops/tablets/phones provided for work use by the school/Trust should only be used by Trust/school employees. • Laptops/tablets/phones will be kept securely by employees, for example not leaving these in a car overnight or in view in your car. • Directors and Governors will be issued email addresses through the LGFL system which ensures security of data. • No data should be saved on personal desktop/laptops. • Remote access is to be used for access to school/Trust systems from personal devices as this is key to maintaining security of data. • Staff/Governors/Directors using their own desktop/laptops/tablets/phones must not save any school/Trust data on their own devices.

Contents

1. Scope

This policy applies to all Directors/Governors and school based employees who are directly employed by Frays Academy Trust. It applies to all users of the School's network, and the use of the school's computer facilities, (including telephony, hardware, software, e-mail, internet, etc) used anywhere, for professional or personal purposes whether in working time or in the employee's own time.

2. Purpose

The purpose of this policy is to:

- Protect Directors/Governors and employees, by making clear what acceptable use of the school's computer facilities is.
- Protect the security and integrity of the Trust, personal data and computer facilities.

3. Policy

High standards of conduct and probity are as relevant to the use of the school computer facilities as they are to all other aspects of work, Directors/Governors must conduct themselves in line with the Code of Conduct for Directors and Governors. Employees must conduct themselves in line with the school's Code of Conduct and Disciplinary Code. All must read this alongside the Data Protection Policy.

Directors/Governors and employees who are in any doubt about what is, or is not, acceptable use of the school's computer facilities must seek advice from either the Executive Headteacher/ manager or the designated ICT person in advance of the use.

Directors/Governors and employees must conduct themselves honestly, appropriately and in accordance with the law and this policy when using the school's computer facilities.

Breach of this policy may lead to disciplinary action and result in withdrawal of access to some or all computer facilities. Serious breaches may be regarded as gross misconduct and may lead to dismissal. Directors/Governors and employees are required to sign a statement agreeing to the terms and conditions of this Policy (Appendix 1).

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

The Executive Head/Head of School /Managers must ensure that Directors/Governors and employees have the skills to use the school's computer facilities. The school will purchase all hardware and software through approved suppliers.

At all times desktop/laptop/tablets will be password protected and screens not left open.

Memory sticks will not be used within Frays Trust Schools as all schools have wi-fi access and staff/Directors/Governors can remote access systems.

Hard drives will only be used under the agreement of the Head of School/CEO where an Apple-Mac computer has been issued by the school. It shall be the responsibility of the Head of School/CEO to ensure the hard drives are password protected.

Any documents circulated via email which contains personal data will be password protected.

4. Access

The school provides access to ICT to enable Directors/Governors and employees to undertake their duties.

The Executive Headteacher, Head of School or another designated senior person has authority to obtain access to an employee's data and documents.

5. Monitoring

Directors/Governors and employees will be required to sign the Statement of Acceptance of the Terms and Conditions of the ICT Usage Policy.

The school's computer 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

Directors/Governors and employees can use the school's computer facilities for reasonable 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

Directors/Governors and employees must not use the school's computer 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 programmes 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

Directors/Governors and employees using school computer facilities must communicate the schools, and not their personal, views.

Directors/Governors and 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.

Directors/Governors and employees must not use the school or its name to endorse any non-school commercial product or service.

9. Confidentiality and Security of Data

The Trust 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 Data Protection Act. Security measures are in place to ensure the confidentiality of data held by the school and Directors/Governors and employees are accountable for breaches of security or confidentiality.

- Directors/Governors and 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.
- Directors/Governors and employees must carefully address e-mails to avoid sending sensitive information to the wrong recipient.
- Directors/Governors and 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 machines with sensitive data from connecting to the internet, or restrict usage of file transfers.
- Directors/Governors and 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.
- Laptops/tablets/phones provided for work use by the school/Trust should only be used by Trust/school employees.
- Laptops/tablets/phones will be kept securely by employees, for example not leaving these in a car overnight or in view in your car.
- Directors and Governors will be issued email addresses through the LGFL system which ensures security of data.
- No data should be saved on personal desktop/laptops.
- Remote access is to be used for access to school/Trust systems from personal devices as this is key to maintaining security of data.
- Staff/governors/Directors using their own desktop/laptops/tablets/phones must not save any school/Trust data on their own devices.

10. Copyright, Legal and Contractual Issues

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

- 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 Executive Headteacher/Head of School or the designated authorised ICT person. Downloaded software becomes the school's property and must be used only under the terms of its license. Directors/Governors and employees must arrange to license and register such software, where required. Software downloaded without permission must be deleted.
- Directors/Governors and employees must not transfer any software licensed to the school or data owned or licensed by the school without authorisation from the Executive Headteacher/Head of School or the designated ICT person.
- The use of computer facilities can lead to contractual obligations in the same way as verbal or written transactions. Directors/Governors and 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 computer facilities must be treated in the same way as transactions on the schools headed paper.

11. Network Efficiency

Directors/Governors and 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 Trust 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 Executive Headteacher/ Head of School 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 network in a responsible way and observe all the restrictions explained in the Policy. If I am in any doubt I will consult (the Executive Headteacher/Head of School/designated authorised ICT person).

I agree to report any misuse of the school's ICT network to (the Executive Headteacher/ Head of School/designated authorised ICT person).

I also agree to report any websites that are available on the school Internet that contain inappropriate material to (the Executive Headteacher/ Head of School/designated authorised ICT person).

I understand that any breaches of the Policy may result in loss of access to the ICT resources and can 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 Director/Governor/Employee: _____

Signature of Director/Governor/Employee: _____

Date: _____