FRAYS
Academy Trust

Frays Academy Trust
ICT Usage Policy

Date Ratified: July 2022
Review Date: July 2025

Approval

Signed by Chair of Directors	
Date of Approval/Adoption	July 2022
Date of Review	July 2025

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 the permission of 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.

This policy will be subject to ongoing review and may be amended prior to the scheduled date of the next review in order to reflect changes in legislation, statutory guidance, or best practice (where appropriate).

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

Contents

1 Scope

This policy applies to all employees who are directly employed by the Frays Academy Trust.

This policy also applies to our Directors and Governors. Where the policy refers to employees, this should also be taken to refer to Directors and Governors. Directors and Governors should refer any queries or concerns to the Clerk in the first instance or, for more serious matters, to the relevant Local Governing Body Chair or the Chair of the Board of Directors.

For staff employed centrally, where the policy refers to the Headteacher, this should be replaced with the Chief Operating Officer (COO).

This policy applies to all users of the Trust's network and the use of the Trust'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, Directors and Governors by making clear what is acceptable use of the Trust's ICT facilities;
- Protect the security and integrity of the Trust, its ICT facilities and all personal data.

3 Policy

High standards of conduct and probity are as relevant to the use of the Trust ICT facilities as they are to all other aspects of work, and employees must conduct themselves in line with the Code of Conduct. The policy must be read alongside the Data Protection Policy.

Employees who are in any doubt about what is, or is not, acceptable use of the Trust's ICT facilities must seek advice from their either their line manager, the Headteacher 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 Trust's ICT facilities.

Breach of this policy by staff 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. Directors and Governors should be aware that breaches may result in them being asked to step down from the Board of Directors or the Governing Body.

Directors, Governors and employees are required to sign a statement agreeing to the terms and conditions of this policy (Appendix 1).

The Headteacher/line manager must ensure that employees have the relevant skills to use the Trust's ICT facilities.

The Trust will purchase all hardware and software through approved suppliers.

At all times desktop/laptop/tablets will be password protected and screens not left open. Screens must be left locked by pressing ctrl/alt/delete.

Memory sticks/removable drives will not be used within Frays Academy Trust as all schools have Wi-Fi access, Office 365 and remote access arrangements. For the sharing of information, schools will use Office 365 with appropriate permissions in place or use networked drives with password protection/ appropriate permissions.

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

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

4 Access

The Trust provides access to ICT to enable employees to undertake their duties.

The Headteacher, Chief Operating Officer or another designated senior person has authority to obtain access to an employee's data and documents.

5 Monitoring

Each employee will be required to sign the Statement of Acceptance of the Terms and Conditions of the ICT Usage Policy.

The Trust'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 Trust's network or equipment can be inspected, at any time, without notice.

6 Personal use

Employees can use the Trust'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 Trust's systems or reputation.

7 Inappropriate Use

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

- Send or access messages that are, or perceived to be, libellous, 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 Trust. 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 Trust's computer facilities.
- Download, use or distribute software including entertainment software or games.
- Download video and audio streaming for personal purposes.
- Use their Trust e-mail address for the purchase of personal goods or financial transactions.

8 Authority to Express Views

Employees using the Trust's ICT facilities must communicate the Trust's views 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 Trust or its name to endorse any non-Trust 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 UK General Data Protection Regulation and Data Protection Act 2018.

Security measures are in place to ensure the confidentiality of data held by the Trust 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.
- Employees must carefully address e-mails to avoid sending sensitive information to the wrong recipient.
- 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 or ensure that the screens are locked by pressing ctrl/alt/delete.
- Governors and Directors should only use their designated Trust email account for all matters concerning Trust business.
- Laptops/tablets/phones provided by the Trust for work purposes should only be used by the employee who has been assigned the equipment. The employee must at all times use all reasonable efforts to keep the equipment secure off site.

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 Trust 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 Headteacher or the designated authorised ICT person. Downloaded software becomes the Trust'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 Trust or data owned or licensed by the Trust without authorisation from the Headteacher/Chief Operating Officer or the designated ICT person.

- The use of ICT 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 any ICT facility must be treated in the same way as transactions on the Trust's headed paper.

11 Network Efficiency

Employees must regularly delete or archive files no longer required or needed for immediate access. Further information on records retention and destruction can be found in the Record Management Policy and the Records Retention Schedule.

The Trust'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 Trust.
- All software must be procured by the Trust 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 Frays Academy Trust's ICT Usage Policy.

I will use the Trust'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 the Headteacher or the designated authorised ICT person.

I agree to report any misuse of the Trust's ICT network to the Headteacher or the designated authorised ICT person.

I also agree to report any websites that are available on the Trust Internet that contain inappropriate material to the Headteacher or the designated authorised ICT person.

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: _____

Signature: _____

Date: _____