Frays Academy Trust
IT Acceptable Use Agreement

Date Ratified: May 2024
Review Date: May 2026

Approval

Signed by Chair of Directors	
Date of Approval/Adoption	May 2024
Date of Review	**May 2026**

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.

Frays Academy Trust IT Acceptable Use Agreement

This agreement applies to all users of the Frays Academy Trust's network and the use of the Trust's IT facilities, (including telephones, hardware, software, e-mail, internet etc.) used anywhere, for professional or personal purposes whether in working time or in the user's own time.

'Users' include all staff (including temporary staff and contractors), third parties, Directors and Governors and anyone else granted access to the Trust's network and IT facilities.

Unless otherwise stated the use of 'Trust' (meaning Frays Academy Trust) throughout this agreement should be considered synonymous with 'school' (meaning those individual schools which make up the Trust) and compliance requirements should be considered to apply equally.

All authorised users of Frays Academy Trust's network, systems, information and communications equipment, devices (and the data and information they process) must comply with the Child Protection Policy, the Information Security Policy, this IT Acceptable Use Agreement, related policies, and associated guidance.

It is your responsibility to read, understand, and adhere to the contents of these policies and guidance. If you are not clear about any policy requirements or guidance you must seek advice from your line manager or the Headteacher.

All Frays network, systems and services including Internet, email, and messaging activity is logged for audit and monitoring purposes, including performance monitoring and to identify inappropriate use. You are responsible for all activity logged against your access credentials.

All users should be aware that there can be no expectation of privacy on the Frays network, systems and services. By using Frays networks, systems and services including email and messaging services, and by using Frays' data and information, users are agreeing to abide by the contents of the Information Security Policy and the Acceptable Use Agreement.

You are responsible for the security of Frays Academy Trust's data and information wherever and however you are accessing it.

Purpose

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This IT Acceptable Use Agreement is intended to ensure:

- that staff and volunteers will be safe and responsible users of the internet and other digital technologies,
- that school IT systems and users are protected from accidental or deliberate misuse.

Agreement

- I understand that I must use school IT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the IT systems and other users. I will, where possible, educate the young people in my care in the safe use of IT and embed e-safety in my work with young people.
- I understand that the school's information systems including, but not limited to, the MIS and Safeguarding systems contain sensitive data and information pertinent to the functioning of the school; I will only access these systems, browse, search or query data with the appropriate permissions and for legitimate school-related purposes.
- I understand that if I have enhanced user permissions or privileged access to Trust or school systems I must comply with any additional security measures required for that role.

For my professional and personal safety:

- I understand that the school will monitor my use of IT systems, including email and other digital communications technologies. This may include but not be limited to the following circumstances:
  - With software to monitor 'trigger' words or phrases for safeguarding and to ensure acceptable, professional use of IT.
  - When staff leave or are on long-term absence for retrieval or redirection of messages.
  - When a member of staff is under investigation or suspected of illegal, fraudulent, inappropriate or safeguarding activity.
  - To collect and review information contained in any electronic system for documented purposes and authorised by Headteacher or COO, for example, to complete a Subject Access Request or similar.
- I understand that information and resources stored on the organisation's equipment and drives should be considered to be controlled and accessible only by the school and authorised staff.
- I understand that this agreement also apply to use of school IT systems out of school (e.g. laptops, email, etc.). This includes my personal or work mobile phone or tablet if it contains my work email or work-related materials.
- I understand that the school IT systems are primarily intended for educational use and I will only use the systems for personal or recreational use within the policies and rules set down in this agreement and any further requirements made by the school. Users may use IT 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 systems or Frays' reputation.
- I will keep my usernames and passwords private and will not share them or use anyone else's username and password.
- I will only use school / Trust systems and personal data for legitimate and authorised purposes.
- I will not disclose or discuss any personal, confidential or sensitive data which I have access to with any unauthorised person(s).
- I will not attempt to access any school service or platform once I have left my employment with a school/ Trust.
- I will return all school-owned IT equipment and delete all school data from my personal devices when I leave my employment.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the Headteacher or other person appointed by the Headteacher/COO.
- I will immediately report any IT security incident or potential IT security incident (including data breaches) to the IT provider and Headteacher without delay. The Headteacher will notify the Data Protection Officer (DPO).

I will be professional in my communications and actions when using school IT systems:

- I will not access, copy, delete or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner.

- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's Agreement.
- I will not use my personal equipment to record these images, unless I have permission from the Headteacher to do so and I will immediately transfer images to a school-based system, delete and not store on my device.
- Where these images are published (e.g. on the school website) I will ensure that it will not be possible to identify pupils by name or other personal information.
- I will not use chat and social networking sites during work time.
- I will only communicate with children and parents/ carers using official school systems and in a professional manner. I will not share any personal information with a pupil or parent/ carer (including personal phone numbers or email address). Nor will I request or respond to any personal information from a child unless it is appropriate as part of my professional role.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure that I do not display or allow my screen to be viewed by staff or external persons whilst accessing/ processing personal data.
- I will lock my screen (by pressing ctrl, alt and delete keys together) or shutdown my computer should I leave it unattended.
- I will ensure that I log out of information systems after each session.
- I will not allow a third party (including family members) to access my work emails or work materials on my mobile phone, tablet or other device.
- I will not leave any IT device unattended when on public transport such as laptop bags in luggage racks.
- If it is necessary to work on a laptop whilst travelling on public transport I will ensure my screen cannot be observed by other passengers.
- If it is necessary to discuss a pupil (or other confidential or sensitive school business) over the phone whilst on public transport I will stop the conversation and wait until I cannot be overheard.

The Trust has the responsibility to provide safe and secure access to technologies and information systems:

- All devices, applications and information systems I use must be secured with an appropriate password/ pin/ biometric protection. Multi-factor authentication (MFA) should be used, where enabled, when accessing information systems to ensure the highest level of security. I will seek advice from the IT provider if required.
- I will delete personal data according to the Trust's Record Retention Schedule. I will seek advice from my school office team if required.
- I will not use personal email addresses for work-related purposes.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will immediately inform the IT provider if I receive any suspected phishing email.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not use any programmes or software that might allow me to bypass the filtering/ security systems intended to prevent access to such materials.
- I will not install or attempt to install programmes of any type on school systems, nor will alter computer settings, unless this has been authorised.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy. Where personal data is electronically transferred outside the secure school network, it must be encrypted.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

Use of Personal Devices

- When I use my personal handheld / external devices in school (PDAs/ laptops/ mobile phones), I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also

follow any additional rules set by the school about such use. As far as I am able, I will ensure that when connecting these devices to school IT systems, they are using up to date Operating Systems (e.g. latest versions of Android/ iOS) and protected by up to date anti-virus software where applicable.

- I will not save any personal data to my personal computer.
- I will only use the recommended apps on my personal device for accessing data/emails via Microsoft 365.
- I will enable encryption on my personal device where possible if I use it to access school personal data or Microsoft 365. If encryption is not available, a personal device should not be used to access or process personal data.
- I will inform the Headteacher or other person appointed by the Headteacher/COO if my personal device (e.g. phone or tablet) is lost or stolen should it contain any school personal data.

When using the Internet:

- I will not engage in any online activity that may compromise my professional responsibilities or bring the Trust and its academies into disrepute.
- I will not attempt to access internet sites/ content which I know to be blocked.
- I will not upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (e.g. child sexual abuse images, racist material, adult pornography etc.).
- I will immediately report to the Designated Safeguarding Lead (DSL) any Internet content that is not filtered that I suspect could be inappropriate.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Intellectual property:

- I understand that material I create in the course of my duties is the intellectual property of the Trust.
- I will not use any information obtained in the course of my work for personal gain, or pass it on to others who might use it in such a way, or for any purpose for which it was not originally intended.

Use of Electronic Whiteboards and Screensharing:

- I understand that electronic whiteboards should be used in a manner that upholds the school's standards of professionalism and respect.
- I will ensure that any content displayed or written on electronic whiteboards during lessons or meetings is appropriate for the intended audience.
- I will not save or store sensitive information displayed on the whiteboard without the necessary permissions or safeguards in place.
- When using interactive features, I will ensure that pupil data and privacy are protected at all times.
- When sharing the screen of my device (laptop, tablet, work phone etc.) to the electronic whiteboard, I will ensure that only the necessary applications or windows are visible to avoid unintentionally sharing sensitive or personal information. This also applies to screensharing during online remote lessons or meetings.
- I will be vigilant and ensure that any notifications or pop-ups that may contain personal or sensitive information are disabled before sharing my screen to the electronic whiteboard. This also applies to screensharing during online remote lessons or meetings.
- I will ensure that any shared content displayed on the electronic whiteboard or shared during online remote lessons or meetings, upholds the school's standards of professionalism and respect.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment outside school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

I have read and understood the IT Acceptable Use Agreement and agree to use the school IT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

School: ……..

Signed: …… Print name: ……..

Date: ……