



Frank Field Education Trust

10.7a ICT Acceptable Use Policy

Date prepared	September 2022
Implementation	Immediate
Frequency of Review	Annually
Review Date	September 2023

Social Justice through Excellence in Education

Contents

Introduction and General Principles	3
Acceptable Use by Staff	3
Acceptable Use by Pupils	5
Data Protection.....	6
Laptop Use.....	6
Monitoring, Evaluation and Review	7
Appendix 1	8
Staff ICT Acceptable Use Agreement.....	8
Staff Acceptable Use Agreement Form	10
Appendix 2.....	11
Pupil Acceptable Use Agreement	11
For my own personal safety	11
I understand that everyone has equal rights to use technology as a resource and.....	11
When using the internet for research or recreation, I recognise that.....	12
I understand that I am responsible for my actions, both in and out of the Academy	12
Pupil Acceptable Use Agreement Form	14
Appendix 3.....	15
STAFF LAPTOP USE AGREEMENT.....	15
GENERAL TERMS OF USE	16
DATA PROTECTION AND NETWORK SECURITY.....	17
SOFTWARE	17
HOME USE	17
TECHNICAL SUPPORT	18
INSURANCE	19

Introduction and General Principles

This policy covers the use of digital technologies in all academies within the Trust: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems. The policy applies to all staff and pupils and has been drawn up to protect all parties.

All systems and equipment are owned by the Trust and may be used by pupils to further their education and by staff to enhance their professional activities including teaching, research, administration and management. This may take place within or outside of academies and will not be limited to the school day.

Staff and pupils (secondary) will be required to sign statements confirming agreement to and understanding of the requirements of this policy. (See Appendices 1 and 2)

This policy should be read on conjunction with the Trust's e-Safety policy, Data Protection Policy and Social Media Policy.

Acceptable Use by Staff

- Trust computer and Internet use must be appropriate to staff professional activity;
- Access should only be made via the authorised account and password, which must not be given to any other person;
- If a password is compromised, the user must ensure that it is changed;
- Users must not use anyone else's password. If it is revealed they must advise the colleague to change it.
- Users must not allow unauthorised individuals to access email / Internet / intranet / network, or other Trust systems
- Users are responsible for all E-mail sent and for contacts made that may result in E-mail being received;
- E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property;
- Only approved Trust email, or other Trust approved communication systems must be used with pupils or parents/carers, and communication must only relate to appropriate Academy business. (This may include appropriate access to professional association websites and other legitimate business) .
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;

- Copyright and intellectual property rights must be respected;
- Anonymous messages and chain letters must not be sent;
- The use of public chat rooms is not allowed;
- The Trust ICT systems may not be used for private purposes, unless the Principal has given permission for that use;
- Use of the network to access inappropriate materials such as pornographic, racist or illegal material is forbidden; There may be circumstances where access to some material is necessary to inform teaching and learning, in these circumstances prior written permission to use such material should be obtained from the Principal.
- The security of Trust ICT systems must not be compromised, whether through devices owned by the Trust or by other organisations or individuals;
- Accidental access to, or receipt of inappropriate materials, or a filtering breach must be reported to the appropriate line manager;
- Users must not download any software or resources from the Internet that can compromise the Trust network, or are not adequately licensed;
- Computers, laptops or other devices (including USB flash drives) must not be connected to the network / Internet that do not have up-to-date anti-virus software, and 'loaned' equipment must be kept up-to-date, using the Trust's recommended anti-virus, firewall and other ICT 'defence' systems;
- Personal digital cameras or camera phones must not be used for taking and transferring images of pupils or staff without permission of parent/carer and or individual, equally images must not be stored without permission of parent/carer or individual.
- Staff must ensure that any private social networking sites / blogs etc. created or actively contributed to are not confused with their professional role;
- Staff must agree and accept that any computer or laptop loaned by the Trust, is provided solely to support professional responsibilities and that staff must notify their Academy of any "significant personal use" as defined by HM Revenue & Customs;
- Teaching staff must embed the Trust's e-safety curriculum into their teaching;
- Staff must only use FFET systems in accordance with any corporate policies.
- All Internet usage / and network usage can be logged and this information could be made

available to a manager on request.

- Failure to comply with this agreement could lead to disciplinary action.

Acceptable Use by Pupils

- Pupils must use Trust ICT systems in a responsible way, to ensure that there is no risk to their own safety or to the safety and security of the ICT systems and other users;
- The Trust will monitor pupils' use of the ICT systems, email and other digital communications;
- Passwords must not be shared, nor must pupils try to use any other person's username and password;
- Irresponsible use, both within academies and outside of the school day, may result in the loss of Internet access or sanctions as identified in the Trust Behaviour policy for pupils;
- Accidental access to, or receipt of inappropriate materials, or a filtering breach must be reported to a member of staff;
- Trust ICT systems are primarily intended for educational use and not to be used for personal or recreational use unless pupils have permission to do so.
- Large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work must not be performed without permission;
- Trust ICT systems must not be used for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), without permission from a member of staff.
- Pupils are expected to respect others' work and property and not to access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission;
- Pupils must be polite and responsible when communicating with others electronically and not use strong, aggressive or inappropriate language;
- Taking or distributing images of anyone without their permission is not allowed; Permission must be obtained before use of personal hand held/external devices (mobile phones/USB devices etc.) in academies and use of said devices must follow the rules set out in this agreement, in the same way as use of Trust equipment.
- Pupils must not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor use any programmes or software that might bypass the filtering/security systems in place to prevent access to such materials.

- Pupils must immediately report any damage or faults involving equipment or software, however this may have happened.
- Pupils must not open any attachments to emails, unless they know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes;
- Pupils must not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor alter computer settings;
- Chat and social networking sites may only be used with permissions and at the times that are allowed;
- Permission to use the original work of others in pupils' own work must be obtained before use;
- Where work is protected by copyright, pupils must not try to download copies (including music and videos).

Data Protection

Staff must ensure that any confidential data transported from one location to another is protected by encryption and that Trust data security protocols are followed when using any such data at any location.

Staff must ensure that any information seen by them with regard to staff or pupil information, held within the Trust's information management system, is kept private and confidential, EXCEPT when it is deemed necessary that they are required by law to disclose such information to an appropriate authority.

All users must ensure that all documents, data etc., are saved, accessed and deleted in accordance with the Trust's network and data security and confidentiality protocols

Laptop Use

The member of staff is responsible for the security of an issued laptop at all times, and for the security of data accessed through this device.

Laptops must not be left unattended & logged on to the network as unauthorised persons could gain access to personal information of pupils/staff/carers

Information relating to an individual to a third party must not be divulged.

Laptops must always be locked whenever left unattended and not left in vehicles on display or overnight.

All data must be saved to the network drive. Data saved to C: drive is at the users' own risk. Staff must not save files to the desktop, as they are not backed up and will slow down log in times.

Staff members will be required to sign a Laptop agreement (see Appendix 3)

Monitoring, Evaluation and Review

The Trust ICT/Communications team may exercise its right by electronic means to monitor the use of the Trust's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the Trust's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

The Board will review this policy at least every two years and assess its implementation and effectiveness through the Chief Operating Officer. The policy will be promoted and implemented throughout the Trust.

Appendix 1

Staff ICT Acceptable Use Agreement

- I will only use the Academy's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other Academy / FFET systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the Academy's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any Academy business.
- I will only use the approved Academy email, or other Academy approved communication systems with students or parents/carers, and only communicate with them on appropriate Academy business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / Academy named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the Academy's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of students or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.

- I agree and accept that any computer or laptop loaned to me by the Academy, is provided solely to support my professional responsibilities and that I will notify the Academy of any “significant personal use” as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow Academy data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or student information, held within the Academy’s information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the Academy’s e-safety curriculum into my teaching.
- I will only use FFET systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Staff Acceptable Use Agreement Form

This form relates to the Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Trust Acceptable Use Policy. If you do not sign and return this agreement, access will not be granted to Academy ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the Academy ICT systems and equipment (both in and out of school).
- I use my own equipment in school (when allowed) e.g. mobile phones, PDAs, cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this Academy e.g. communicating with other members of the Academy, accessing Academy email, learning platform, website etc.

Name: _____

Signature: _____

Date: _____

Appendix 2

Pupil Acceptable Use Agreement

I understand that I must use Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the Academy will monitor my use of the ICT systems, email and other digital communications.
- I will not share my password, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating online.
- I will not disclose or share personal information about myself or others when online.
- If I arrange to meet people that I have only communicated with online, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Academy ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the Academy ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission from a member of staff to do so.
- I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the Academy.

- I will only use my personal hand held/external devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use chat and social networking sites with permission and at the times that I am allowed.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of the Academy:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the Academy community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy network/internet, detentions, and suspensions and contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy Agreement. If you do not sign and return this agreement, access will not be granted to Academy ICT systems.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy Agreement. If you do not sign and return this agreement, access will not be granted to Academy ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the Academy ICT systems and equipment (both in and out of school).
- I use my own equipment in school (when allowed) e.g. mobile phones, PDAs, cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this Academy e.g. communicating with other members of the Academy, accessing Academy email, learning platform, website etc.

Pupil's Name:

Signature:

Form Group:

Date:

Appendix 3

STAFF LAPTOP USE AGREEMENT

Between _____ and Birches Head Academy

It is important that you read the following information carefully and sign to acknowledge that you understand and consent to the guidelines below. Please sign 2 copies, returning one to ICT Support and retaining one copy for your reference.

GENERAL TERMS OF USE

1. This computer is provided to assist you in your professional duties including lesson planning & preparation, teaching, internal and external communications and electronic registration.
2. The laptop must be made available to ICT Support on request.
3. The laptop is the property of FFET and it holds the right to allocate and transfer custody of the laptop and installed software.
4. You must take due care in the handling and use of the laptop and return it in good condition if your employment with FFET is terminated.
5. The following activities are prohibited – they may invalidate the warranty and/or insurance:

Performing upgrades or enhancements which require you to access the interior of the laptop
e.g. memory upgrades etc.
6. You must follow the usage guidelines in the technical documentation supplied with the laptop.

DATA PROTECTION AND NETWORK SECURITY

1. You are responsible for the security of your laptop at all times, you are also responsible for the security of data you have access to on your laptop.
 -] **DO NOT** – Leave your laptop unattended & logged on to the network as unauthorised persons could gain access to personal information of students/staff/carers
 -] **DO NOT** – Give out any information relating to an individual to a third party
 -] **DO** – Always lock your laptop whenever you leave your laptop unattended
2. You may use the laptop to print to network printers and to save files on authorised Academy drives only. You may use the network to access email and intranet/internet services. You may not access or attempt to access any other part of the network without authorisation.
3. You may run applications from the network if they have been provided for you by ICT support.
4. You must not divulge your network or laptop username and password to anyone.
5. All data should be saved to a network drive. Data saved to C: drive is at the users' own risk. You must not save files to the desktop, as they are not backed up and will slow your laptop down when logging in.

SOFTWARE

1. The installed software is licensed to FFET and may not be removed, transferred, modified or copied.
2. In the event of a technical fault, ICT Support reserves the right to erase the hard disk drive and stored data.
3. You may install software on the laptop, provided that you hold a current license. ICT Support will need to see a copy of the license.

HOME USE

1. You may use the laptop computer at home for professional or lawful personal purposes.
2. You may connect peripherals that belong to you such as printers, digital cameras etc. ICT Support does not provide extra cables to enable such connections.
3. You must **NOT** install iTunes on your laptop under any circumstances unless authorised by ICT Support.
4. Any work you do at home will synchronise when you come back into school however very occasionally this will fail so always make sure you back up your work.

TECHNICAL SUPPORT

1. FFET will provide support in the event of hardware faults or software faults, provided that the software has been licensed to FFET and installed by ICT Support.
2. Support requests should be made by logging a request via the “ICT Support” link on your desktop
3. Lost/Stolen/Broken chargers will be replaced but will be charged to your department.
4. In-school use while connected to the school network takes priority over other forms of usage.
5. Peripherals not owned by FFET will not be supported.

INSURANCE

Your laptop is covered by an insurance policy both in school and off premises. The insurance is limited and has key exclusions including theft from a vehicle and theft whilst left unattended. You are responsible for any uninsured risk. Full details of the policy cover can be inspected at your Academy.

Any loss, theft or accidental damage MUST be reported *immediately* to ICT Support at your FFET Academy.

Any loss, theft or damage arising from a criminal offence should be reported to the Police and a crime number obtained. The crime number should then be given to ICT Support within 48 hours of the incident even if this happens in school holiday time any longer and it will invalidate the insurance.

Signed _____ Date