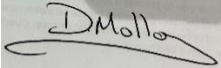
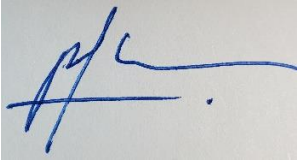




First **Star** Scholars **UK**

Acceptable IT Use Policy

Date of Last Review	29/10/2024
Review Cycle	Annually
Date (Month/Year) of Next Review	10/2025
Date Policy was Ratified	29/10/2024
Named Lead for Writing/Review	Emily Hollis MBE
Signed: CEO 	Date 29/10/24
FSSUK Board of Trustees – Chair 	

Introduction

As a professional organisation with responsibility for safeguarding, all members of staff (including volunteers) are expected to use First Star Scholars UK's (the charity) IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and social media platforms, they are asked to read and sign the Acceptable IT Use Policy.

We do not intend to unduly limit the ways in which members of staff use technology and social media professionally, or indeed how they use the internet personally, however the policy will help ensure that all staff understand the charity's expectations regarding safe and responsible technology use and can manage the potential risks posed. This policy will also help to ensure that the charity's systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy scope

I understand that this policy applies to my use of technology systems and services provided to me or accessed as part of my role within the charity both professionally and personally, both on and offsite, and whilst on residential or trips and visits. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, online and offline communication technologies.

I understand that this policy should be read and followed in line with the charity's Safeguarding Policy and Code of Conduct. I am aware that this policy does not provide an exhaustive list; all staff should ensure that technology use is consistent with the charity's ethos, all associated policies and the law.

Use of devices and systems

I will only use the equipment and internet services provided to me by the charity, for example laptops, tablets, mobile phones, and internet access, when working for the charity. I understand that any equipment and internet services provided by my workplace is intended for work purposes and/or professional use and should only be accessed by members of staff or client contracts (by agreement). Personal use of IT systems and/or devices by staff is not allowed.

Data and system security

To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

I will use a 'strong' password to access charity systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. This password should be changed every 6 months.

I will protect the devices in my care from unapproved access or theft, for example not leaving devices visible or unsupervised in public places or in a car overnight.

I will respect charity system security and will not disclose my password or security information to others.

I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the Director of Operations.

I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the Director of Operations.

I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the charity's policies. All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. Any data such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the charity.

I will not keep documents which contain charity related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones, but instead will use charity provided devices such as encrypted pen drives.

I will not store any personal information on the charity IT system, including laptops or similar device issued to members of staff, that is unrelated to charity activities, such as personal photographs, files or financial information.

I will ensure that charity owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences:

- to gain unauthorised access to computer material;
- to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

I will not attempt to bypass any filtering and/or security systems put in place by the charity.

If I suspect a computer, pen drive or system has been damaged or affected by a virus or other malware, I will report this to the Director of Operations as soon as possible.

If I have lost any charity related documents or files, I will report this to the charity Data Protection Officer as soon as possible. Further information can be found in the Data Protection Policy.

Any images or videos of children/vulnerable adults will only be used as stated in the Safeguarding Policy. I understand images of children/scholars must always be appropriate and should only be taken with charity provided equipment and only be taken/published where children/vulnerable adult and/or parent/carers have given explicit written consent.

Mobile devices and smart technology

I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the Safeguarding Policy, Code of Conduct and the law.

Online communications including use of social media

I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the Safeguarding Policy, Code of Conduct and the law.

I will take appropriate steps to protect myself and my reputation, and the reputation of the charity, online when using communication technology, including the use of social media.

I will not discuss or share data or information relating to children/vulnerable adults, staff, charity business, parents/carers or any clients on social media.

My electronic communications with any charity clients will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

I will ensure that all electronic communications take place in a professional manner via charity approved and/or provided communication channels and systems, such as a charity email address, user account or telephone number.

I will not share any personal contact information or details with clients, such as my personal email address or phone number.

I will not add or accept friend requests or communications on personal social media with current or past children/vulnerable adults and/or their parents/carers who are involved in the charity in any way (either directly or indirectly).

If I am approached online by current or past children/vulnerable adults or parents/carers, I will not respond and will report the communication to the Director of Operations and Designated Safeguarding Lead (DSL).

Any pre-existing relationships or situations that compromise my ability to comply with this policy or other relevant policies will be discussed with the Director of Operations and DSL.

Management of the charity social media platforms is the responsibility of the CEO, Director of Operations and Assistant Director. Only they and the charity Trustees have permission to post to and from the charity social media accounts.

Policy concerns

I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the charity into disrepute.

I will report and record any concerns about the welfare, safety or behaviour of service users online to the DSL in line with the charity Safeguarding Policy.

I will report concerns about the welfare, safety, or behaviour of staff online to the CEO, in line with the charity Safeguarding and Whistleblowing policies. If the concern is regarding the CEO, I will report the concern to the Chair of Trustees.

Policy compliance and breaches

If I have any queries or questions regarding safe and professional practise online, either at the charity or off site, I will raise them with the CEO/DSL.

I understand that the charity may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure safety. This includes monitoring all charity provided devices and systems and networks including charity provided internet and SharePoint access, and may include the interception of messages and emails sent or received via charity provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

I understand that if the charity believe that unauthorised and/or inappropriate use of charity systems/networks or devices is taking place, the charity may invoke its disciplinary procedures as outlined in the charity Disciplinary Policy and Code of Conduct.

I understand that if the charity believe that unprofessional or inappropriate online activity, including behaviour which could bring the charity into disrepute, is taking place online, the charity may invoke its disciplinary procedures as outlined in the charity Disciplinary Policy and Code of Conduct.

I understand that if the charity suspects criminal offences have occurred, the police will be informed.

Other documentation

This policy should be read in conjunction with:

- Code of Conduct
- Whistleblowing Policy
- Disciplinary Policy
- Safer Recruitment Policy
- Safeguarding Policy
- Data Protection Policy

Version Control - Approval and Review

Version No.	Approved by	Approval Date	Main Change	Review Period
1.0	Diarmuid Molloy	29 October 2024	New policy format approved	Annually

Acceptable IT Use Policy Acknowledgement

I have read, understood and agreed to comply with First Star Scholars UK's Acceptable IT Use Policy.

Name	
Signed	
Date	