IT Policy:
Use of IT Facilities provided by the Woolf Institute

1. Scope

The policy applies to all staff, students and visitors using IT facilities provided by the Woolf Institute.

This includes personal devices used to access the Institute's network and systems. The Institute's network also falls under the supervision of the University Computing Service and all users are subject to its rules and guidelines. The Institute uses the Virtual Learning Environment which is hosted by the Cambridge Theological Federation and all users are subject also to its rules and guidelines.

This document provides an overview of what is considered misuse of Woolf Institute IT resources, and applies to individuals using resources and/or networks provided by the Institute and/or its partner bodies, whether using Institute owned equipment or a personal device.

2. Definitions of Misuse

Information Technology is an essential part of the Institute's life and business. Misuse can damage the Institute's business and reputation and may infringe the law. Examples of such misuse include, but are not limited to:

- Accessing or downloading material that encourages terrorism or may lead to radicalisation
- Disrupting the Institute's systems by inappropriate downloads or e-mailing
- Harming the Institute's reputation by downloading potentially offensive material in a public space or making inappropriate posts on social networking sites
- Unauthorised access to and theft or loss of Institute data
- Decreased efficiency by prolonged inappropriate use during working hours
- Illegal downloading, file sharing or support for other illegal activities

3. Monitoring and Access by the Institute

The Institute does not routinely monitor accounts and will do so only in exceptional circumstances. For monitoring to take place, authorisation of the Founder Director will be required.

The Institute may require emergency access to accounts of staff, students or visitors if the account holder is away in unforeseen circumstances. Every effort will be made to seek the account holder's consent but operational need may override this. Folders relating to Institute business should be clearly marked as such and kept separately from personal and academic work to facilitate this and protect users' privacy.

Monitoring will only be authorised when there is clear and justifiable suspicion of sustained misuse, where network performance is adversely affected or where criminal activity is suspected.

4. Usage of Institute Systems

It is unacceptable for staff, students and visitors to use Institute systems:

For unauthorised commercial purposes

To bully, harass or cause distress to others

To view obscene or offensive websites in public or access websites supporting illegal activities

The Institute supports Freedom of Expression. However using Institute systems to promote extreme views inciting violence and/or hatred of others because of their race, religion, sexual orientation or political affiliations is never acceptable and may constitute a criminal offence.

All users posting to social networks on their own devices should be aware that posts may not be private and may be shared by others. Users are responsible for their own security settings and for preventing posts that may harm the Institute.

Users must not imply that a page, account or blog is an official site if it is not. Official sites should be registered as such with the Institute.

5. Email

Electronic communication has become the principal medium for information flow within the Institute and more widely. However, the norms applying to electronic mail communication have dramatically modified traditional styles of writing. Brevity and spontaneity have become the operating principles, which sometimes add considerably to the risk of poor communication. Risks include spelling mistakes, lack of punctuation, and such extreme brevity that the message is not understandable to the receiver (or those copied into the message). This medium also seems to offer the opportunity for less than constructive feedback, particularly ill-considered expressions of feelings that might never take place in face to face circumstances.

Email etiquette: the Institute's staff, students and visitors engaged in validated programmes of study should familiarise themselves with and adhere to the policies on electronic communication at the institution which validates their programme of study:

Anglia Ruskin University: http://web.anglia.ac.uk/it/support/staff/needhelp/email/outlook/Anglia%20Practice%20and%20Good%20Practice%20at%20Anglia2.doc and http://web.anglia.ac.uk/it/standards/Email%20Policy%20and%20Practice%20September%202009.pdf

University of Cambridge: http://www.cam.ac.uk/cs/email/etiquette.html

Durham University: https://www.dur.ac.uk/cis/policy/

American University in Washington:
http://www.american.edu/loader.cfm?csModule=security/getfile&pageid=4252664
and
http://www.american.edu/loader.cfm?csModule=security/getfile&pageid=2452105

6. Consequence of misuse of IT resources provided by the Institute

Consequences of misuse may include, but are not limited to:

Immediate suspension of the email account
Barring from Institute computer networks
Notification of suspicious activity to the police
Fines
Recuperation of costs incurred by the Institute
Expulsion from the Institute.

An appropriate process will be held before any of these consequences are implemented, having due regard to the particular circumstances of the case and the need for urgency, confidentiality and the maintenance of security.

Woolf Institute
Cambridge 25 July 2016