STFC Monitoring and Interception Policy

Issue 1.1 (19 March 2015)

This document contains a copy of the STFC policy statements outlining the circumstances when authorised STFC staff may be granted access to Information Communication Technology (ICT) systems and services for the purposes of monitoring and interception available at:

https://staff.stfc.ac.uk/core/security/information/Policy/STFCMonitoringPolicy.pdf

This document should be read in conjunction with the STFC Acceptable Use Policy for ICT systems and services (AUP) available at: https://www.stfc.ac.uk/aup

This document and its contents were formally endorsed by STFC on 27 June 2012 by the Operations Board. It is effective from 27 June 2012 and supersedes earlier versions. Please check the above web site for any changes or updates.

1. PURPOSE

This Policy is designed to:

- help all individuals (e.g. employees, visitors, contractors, Facilities users, Tenants organisations etc.) understand the circumstances in which it is permissible for STFC to grant authorized access to ICT systems and services for the purposes of monitoring and interception;
- help maintain the security, integrity and performance of STFC ICT systems and services;
- help maintain the privacy of communications and data set to and from individuals;
- help ensure that STFC and individuals users demonstrate effective and appropriate compliance with English law.

The Policy, any additional supporting standards, process descriptions, guidance, instructions, frequently asked questions (FAQ) etc. are all are published within the STFC Information Security Policy Framework accessible to STFC staff via in.Focus. Particularly relevant documentation is highlighted in ANNEX A.

2. SCOPE

This Policy applies to all individuals (e.g. employees, visitors, contractors, Facilities users, etc.) and Tenant organisations that make use of STFC ICT systems, services and Facilities. It applies to all user accounts, files, communications and/or other data stored on ICT equipment, including any peripheral devices or hardware, used by individuals that make use of STFC ICT systems and services.

This Policy applies to all ICT systems and facilities provided either directly or indirectly by the STFC whether accessed from an STFC site or remotely.

It also applies to all third party systems which transfer communication and/or other data across STFC provided infrastructures as described in the STFC Network Transit Policy.

For the absence of doubt, this policy applies to "private" and other third party ICT equipment used on STFC networks.

3. PRIVACY AND ACADEMIC FREEDOM

STFC respects the privacy and academic freedom of staff, Tenants and Facilities users. However, STFC may carry out lawful monitoring of ICT systems. Staff, Tenants, Facilities users and any other authorised users should be aware that STFC may access email, telephone and any other electronic communications, whether stored or in transit. This is in order to comply with the English law and applicable regulations and to ensure appropriate use of STFC ICT systems and services. All access and monitoring will comply with UK legislation including, but not limited to, the Regulation of Investigatory Powers Act 2000 (RIPA), the Human Rights Act 1998 (HRA) and the Data Protection Act 1998 (DPA).

4. STFC'S POWERS TO ACCESS COMMUNICATIONS

4.1 AUTHORISED STFC STAFF

1. STFC will put in place processes to identify, train and authorise appropriately trained members of STFC staff so that they implement this policy. Such individuals are known as "authorised STFC staff" within the context of this policy and will be trained in data protection compliance.
2. Where contractors or other third parties are acting on behalf of STFC, they will be required to demonstrate that they have received the same level of training that would be expected of authorised STFC staff. Until such assurances have been verified and they receive written authorisation, contractors or other third parties should not implement this policy. Once appropriately authorised, within the context of this policy, contractors or other third parties are part of "authorised STFC staff".

4.2 POWERS OF ACCESS

1. Authorised STFC staff may access accounts, files and communications, including electronic mail files, stored on any ICT systems, services or facilities owned, managed or maintained (except where the STFC act solely as a service provider for another body) by STFC and may examine the content and relevant traffic data.
2. STFC may access accounts, files and communications for the following reasons:
    - To detect or prevent crime e.g. detecting unauthorised use of systems, protecting against viruses and hackers, fraud investigation etc.;
    - As part of occasional training and quality control exercises e.g. how incoming calls are handled;
    - To assist in maintaining the security, performance, integrity and availability of the ICT systems, services and facilities;

- To provide evidence e.g. of a commercial transaction, to establish regulatory compliance, audit, debt recovery, dispute resolution;
- To fix problems reported to the IT Service Desks or which become apparent during routine system administration;
- To ensure the operational effectiveness of the service. (For example, STFC may take measures to protect the ICT systems from viruses and other threats such as hacking or denial of service attacks.);
- To establish the existence of facts relevant to the business of the STFC. (For example, where a case of suspected plagiarism is being investigated and there is sufficient evidence to warrant authorised STFC staff examining relevant communications and/or files without the individuals consent. Another example may be checking email accounts when staff are absent on holiday or on sick leave to access relevant communications.);
- To ascertain compliance with regulatory or self-regulatory practices or procedures relevant to STFC business (e.g. to ascertain whether STFC is abiding by its own policies.);
- To monitor whether or not communications are relevant to the business of STFC. (For example, to check an email account to ensure that it is not being misused for personal or private purposes but not to look at the contents of the emails unless this is required to confirm the use of the email account.);
- To monitor (but not log) communications to a confidential, free, telephone counselling or support service run by STFC, provided that users are able to remain anonymous if they so choose. This is to enable help-line workers to receive appropriate supervision and support.

STFC will publish monitoring statements bringing these reasons to the attention of users. (See Annex B for the Monitoring statement used in the STFC AUP).

5. THE POWERS OF LAW ENFORCEMENT AUTHORITIES TO ACCESS COMMUNICATIONS

1. A number of non-STFC bodies/persons may be allowed access to user communications in certain circumstances. Where STFC is compelled to provide access to communications by virtue of a Court Order or other competent authority, STFC will disclose information to these non-STFC bodies/persons when required as allowed under the Data Protection Act 1998.

   For example, under the Regulation of Investigatory Powers Act 2000 a warrant may be obtained by a number of law enforcement bodies regarding;

   - issues of national security;
   - the prevention and detection of serious crime;
   - safeguarding the economic well-being of the UK.

   In such circumstances, STFC will provide reasonable assistance with the execution of a lawful warrant. The term “authorised persons” in this policy refers to authorised STFC staff and relevant Law Enforcement Authorities.

6. POLICY ON ACCESS TO COMMUNICATIONS BY OTHERS

1. Individuals who are neither authorised STFC staff (see section 4) or working for Law Enforcement Authorities (see section 5) must not access the accounts, files, and communications of any other individual and must only use STFC's facilities in compliance with the STFC Acceptable Use Policy (available at www.stfc.ac.uk/aup).

7. POLICY ON ACCESS TO COMMUNICATIONS BY INDIVIDUALS

1. Individuals are allowed access to their own accounts, files and communications in compliance with the STFC Acceptable Use Policy (available at www.stfc.ac.uk/aup).

8. POLICY ON ACCESS TO COMMUNICATIONS BY AUTHORISED PERSONS

8.1 STAFF ABSENCE / DEPARTURE

Where a member of staff is absent from work and access is required to that member of staff's account, files or communications for a specific reason (for example to access correspondence in order to complete an item of work), STFC will follow the procedure set out below:

1. If appropriate, the member of staff will be contacted by their line manager and consent sought in writing for access to specific communications and/or files. If given, this consent will passed to authorised STFC staff to facilitate the access.
2. Where consent is not or cannot be given and there is no alternative way to get the required information, permission to access the member (or ex-member) of staff's accounts, files or communications will be sought in writing from authorised STFC staff. Authorisation will only be given for access to specific information and not for general access to the accounts, files or communications in question.
3. The person authorised to access the accounts, files or communications is responsible for ensuring that only the specific information authorised is accessed and that other information is not read or disclosed.
4. After the necessary information has been retrieved, any relevant password to the absent member of staff's account(s) will be reset and the new password will be communicated only to that member of staff.

8.2 SUSPECTED ILLEGAL BEHAVIOUR

1. Where circumstances brought to the attention of the STFC Senior Information Risk Owner (SIRO) or the STFC Information Technology Security Officer (ITSO) constitute grounds for reasonable suspicion that an individual is using STFC's ICT Facilities for the commission or attempted commission of a criminal offence, the SIRO or ITSO will contact the police for advice.
2. Based on that advice, the account(s) and any associated hardware or peripheral devices of the individual may be frozen pending further investigation by STFC or the police.

8.3 SUSPECT BREACH OF TERMS OF CONTRACT OF EMPLOYMENT OR STFC REGULATIONS

1. Where there are reasonable grounds to suspect that a member of staff is using STFC's ICT systems, services or facilities in breach of the terms of their contract of employment or is in breach of STFC regulations, an internal investigation may commence to establish the facts supporting or refuting the potential allegation.
2. All ICT investigations will follow the STFC ICT Investigation process and be carried out by appropriately authorised STFC staff. Based on the outcome of this initial investigation, appropriate disciplinary process may begin.
3. Where appropriate, the member of staff will be contacted to give consent for access to appropriate accounts, files or communications and information relevant to the investigation.
4. Where it is not appropriate, not possible to inform the member of staff, they are not available to give consent or consent is refused or access is required under section 4, authorisation will be requested from the SIRO and ITSO as described in the STFC ICT Investigation process.
5. All access and monitoring will comply with UK legislation including the Regulation of Investigatory Powers Act 2000, the Human Rights Act 1998 and the Data Protection Act 1998.

9. GENERAL GUIDANCE

1. Any authorised access to the accounts, files or communications of an individual will be with as little intrusion and disruption to the communications of third parties that are unconnected to the authorised access as possible.
2. Where possible, access will be granted without the need to share, divulge or reset passwords on user accounts.
3. Any information collected under this Policy will be treated in confidence and will only be examined by those persons who are so authorised.
4. Any information collected under this Policy will only be retained for as long a period as deemed necessary for the specific purpose and in line with STFC's Records Retention Policy.
5. Any information collected under this Policy will be stored securely and will be labelled accordingly depending on the sensitivity of the material in question.
6. Unless any information collected or accessed under this Policy warrants further investigation or ongoing review, the collected information or access to it will be destroyed or revoked after 28 days.
7. Any person collecting or accessing information under this Policy will ensure that they have continued authorisation to implement this policy. Individual authorisations will expire at least annually and on departure from STFC.
8. Where possible, authorised STFC staff collecting or accessing information under this Policy will respect the privacy of files and messages which are marked as 'personal' or 'private' provided it does not impede or frustrate any ICT investigation.

This Policy should be read in conjunction with STFC's Communication Policy and with any other relevant sections of STFC's Rules and Regulations as applicable to Facilities users and relevant terms of STFC's conditions of employment (CEMs) as applicable to members of staff.

10. FURTHER INFORMATION

Individuals should seek guidance about this Policy or its application in their specific circumstances from their local IT Service Desk, your Information Security Group representative or IT Security Officer.

11. REVIEW

This Policy will be reviewed every 2 years or as required and endorsed by the Operations Board.

12. VERSION HISTORY

Version	Date	Comments/Changes
1.0	27/6/12	Approved version
1.1	19/3/15	ISG review amendments added

ANNEX A - Related Policies and Procedures

- STFC Acceptable Use Policy (https://www.stfc.ac.uk/aup)
- STFC Network Transit Policy (http://staff.stfc.ac.uk/core/security/information/Policy/STFCNetworkTransitPolicy.pdf)
- Staff Absence - Process to request access to STFC accounts, files or communications
- STFC ICT Investigation Process
- Requesting authorisation to access communication (Process)
- Granting authorisation to access communication (Process)

ANNEX B – Monitoring statement used in the STFC AUP

The STFC Monitoring Statement can be found at Section 2.1 of the STFC Acceptable Use Policy