Scottish Funding Council

ICT Monitoring Policy

Contents

Purpose

1. This policy describes how we will monitor the use of our Information and Communication Technology (ICT) systems.

Introduction

2. Our ICT systems support the work of the Scottish Funding Council (SFC) and are intended for business use. However, we also recognise that there are benefits to be gained by allowing staff to make limited personal use of our ICT services. All usage of our ICT services should be consistent with our Acceptable Use Policy.

3. We reserve the right to monitor the use of our ICT services, and access any information stored on our ICT infrastructure, but will do so in ways that are consistent with relevant legislation and guidance the Information Commissioner's Officer and the European Data Protection Board. We will undertake such monitoring to:

    - Comply with our regulatory and statutory obligations.
    - Assess compliance with our Information Security and Acceptable Use Policy
    - Maintain effective ICT systems
    - Prevent and detect unauthorised use or other threats to our ICT systems.
    - Evaluate staff training.
    - Monitor system performance.

4. Such monitoring may include email, internet, telephone, mobile telephone and electronic file storage usage. Such monitoring is not, in general, person specific; however, it may be unavoidable personal data may be accessed as part of this policy.

5. Monitoring will only take place where strictly necessary and only in ways that are consistent with data protection law and good corporate governance. Such monitoring is defined as **systematic monitoring** in terms of the UK Information Commissioner's Office (ICO) Employment Practices Code

6. The existence or otherwise of monitoring procedures does not diminish the responsibility on SFC staff to comply with the Acceptable Use Policy.

Scope

7. This policy specifies:

    - Our approach to monitoring usage of ICT devices, services and software, including printer usage and electronic door access logs.
    - Intercepting communications on our ICT systems.

- The information we gather during usage logging.
- How we control content inspection.
- How staff and other users of our ICT systems are made aware of this policy.

Communication of this policy

8. We shall make users aware of this policy by:

    - Highlighting the policy in the staff privacy notice.
    - Ensuring new members of staff are informed of the policy at their induction.
    - Informing staff of the terms of this policy by logging onto our ICT infrastructure.
    - Reminding users at regular intervals, e.g. at the point of log on, of the existence of the policy and any updates to it, and where to find it.

Privacy

9. Our policy aims to provide an appropriate balance between respecting your privacy and allowing the necessary monitoring required to meet our business needs and legal obligations.

10. We recognise that staff have legitimate expectations that they should be able to keep their personal lives private and that they are entitled to a degree of privacy in the work environment. Our monitoring policy will therefore be undertaken in ways that are consistent with relevant legislation and good corporate governance, including the Data Protection Act 2018, the UK Information Commissioner's Office (ICO) Employment Practices Code, and The Human Rights Act 1998.

11. We will also act in accordance with our obligations under the Telecommunications (Lawful Business Practice) (Interpretation of Communications) Regulations 2000 and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA).

Monitoring definitions

12. This policy makes a distinction between:

    - Usage logging: collecting data, usually from log files, about how and when a person used our ICT systems.
    - Content inspection: viewing information held within, for example, business or personal files or emails, or viewing of information on a VDU screen.

Usage logging

13. We carry out 'usage logging' on a regular basis to ensure or improve the performance of our ICT services and to help identify and investigate potential

misuse or prohibited use of our ICT systems (e.g. where a complaint or concern has been raised). This is 'systematic monitoring' as defined by the UK ICO.

14. None of this data contains the content of the communication or the file – only information about the electronic activity. The 'usage logging' does not therefore allow SFC to monitor or record 'sensitive personal data' as defined by the Data Protection Act.

15. The data logged automatically by our ICT infrastructure is given in Appendix 1. This represents monitoring, but not recording within the context of RIPSA. This information is restricted to the team(s) identified in the appendix for the day to day administration of our infrastructure.

Content inspection and authorised access

16. SFC has the right to inspect the content in our ICT systems:

- To fulfil SFC business, (for example, when a user is unexpectedly absent or is on leave).
- To satisfy Data Protection subject access and Freedom of Information requests.
- Where we have reason to believe that a breach of our information security and information management policies is occurring, or has occurred (for example, where a complaint or concern has been raised.)
- At the request of law enforcement officers.

17. Content inspection involves viewing information contained within:

- Business files and documents.
- Printer usage and door access logs.
- Business-related email messages, telephone calls, videoconference sessions, chat sessions or any other ICT-based communications including internet usage logs.
- Business information displayed on a VDU screen.

18. We will only carry out content inspection after permission has been granted by the Head of Human Resources or the Assistant Director for Human Resources and Organisational Development. If the request to conduct a content inspection originates from HR, or it is not appropriate for HR to grant permission, permission will be granted by the Chief Operating Officer or Chief Executive.

19. Requests for access to the email account or restricted folders of a member of staff must be made using the content inspection request form, detailing the reason for the request and the information to be viewed. The request form should be submitted to either the Head of Human Resources or the Assistant

Director for Human resources and Organisational Development. If the request to conduct a content inspection originates from HR, or it is not appropriate for HR to grant permission, permission will be granted by the Chief Operating Officer or Chief Executive. The form is then passed to ICT for action.

20. The request should only be approved providing it meets the criteria set out in this policy.

21. Upon receipt of the approved form, a member of ICT will undertake a content inspection. Following the inspection, the member of ICT will record:

    - What information was inspected.
    - The computer on which the monitoring took place.
    - The start and end date and time of the monitoring.
    - The identity of the person(s) performing the inspection.

22. This record will be kept securely and in accordance with the SFC Retention Schedule. In order to respond to the criteria in this policy, the record may be shared with the line manager, the individual, the Head of Human Resources or Assistant Director for Human Resources and Organisational Development, or the Information Management and Governance Officer (IMGO), only in so far as necessary.

23. In certain circumstances, investigation of misuse or prohibited use may require taking a copy of material which would normally be prohibited from being stored on our ICT systems: for example, pornographic images. As well as requiring the above approval, the investigating person must record and inform at least one other member of staff where this material is being stored and why. As soon as the process is complete, this material must be destroyed by the two members of staff involved in its retention. The date of the destruction should be recorded. Destruction will be delayed if the material is illegal and SFC is requested to retain the material by law enforcement officers.

24. We will regard any attempt to conduct a content inspection that is not in accordance with this policy as gross misconduct.

Web monitoring, filtering and blocking

25. The prevention of inappropriate use of the internet is aided by the use of the web filtering software. This enables blocking of inappropriate websites. Due to the nature of certain technologies, for example the wireless network, stricter criteria will at times need to be applied, meaning where web filtering software cannot determine whether a website is appropriate or not, it will be blocked. Staff requesting the unblocking of web sites for legitimate business use must obtain consent from their line manager before contacting the head of ICT.

26. Web filtering software is used for the reduction and prevention of Spam emails, but also blocks potential system threats such as virus or Trojan horse malware in emails or attachments. Web filtering software is also able to detect and block pornographic images being sent externally or being received from an outside source. All these functions identify the time, workstation and user receiving or sending such emails.

Misuse

27. Where our systematic monitoring suggests that a member of staff may be misusing our ICT systems, the Head of Human Resources or Assistant Director for Human Resources and Organisational Development may raise the matter with the individual concerned and/or their line manager. We may conclude that the individual's use of our ICT system needs to be monitored more closely. In this case, we will notify the individual in writing as soon as reasonably possible of:

    - The reasons for the monitoring.
    - The nature and extent of the monitoring.
    - The timeframe of the monitoring.

28. This monitoring is defined as **occasional monitoring** in terms of the Information Commissioner's Office (ICO) Employment Practices Code.

29. Only the Head of Human Resources or Assistant Director for Human Resources and Organisational Development may authorise occasional monitoring. The record of the monitoring may only be viewed by the individual's line manager, the Head of Human Resources or Assistant Director for Human Resources and Organisational Development.

30. Any occasional monitoring must be proportionate and in accordance with the reasonable privacy expectations of the individual. If the individual has any concerns about the nature of the occasional monitoring, they can ask the Information Management and Governance Officer for advice.

Prohibited use

31. Where we have good reason to suspect that a member of staff is engaging in a prohibited use of our ICT systems – as set out in the Council's ICT Acceptable Use Policy – we may, in very exceptional circumstances, introduce covert monitoring of the individual.

32. We will only undertake such covert monitoring where there are strong grounds for suspecting criminal activity or equivalent malpractice, and where notifying an individual about the monitoring would prejudice its prevention or detection. Covert monitoring will be strictly targeted at obtaining evidence within a set timeframe and will not continue after an investigation has been completed.

33. Covert monitoring may only be authorised by the Chief Executive or Chief Operating Officer. The record of the monitoring may only be viewed by the individual's line manager, the Head of Human Resources or Assistant Director for Human Resources and Organisational Development.

Monitoring of Social Media

34. SFC does not carry out routine monitoring of staff or other individuals' social media accounts. This includes the social media accounts of prospective employees.

35. However, where SFC has been informed of alleged misuse of SFC business information, occasional monitoring of social media accounts may be carried out. Monitoring in these circumstances will be limited to publicly available information. However, an investigation into any misuse may collect available information which is not publicly available where necessary.

36. For example, if an employee was accused of revealing personal information of colleagues on their social media profile, SFC may collect a screen shot of the information provided by a fellow colleague. Such information will only be collected where necessary and relevant.

Document control

Title	SFC Monitoring Policy
Prepared By	Information Management and Governance Officer
Approved Internally By	Chief Operating Officer
Date of Approval	20 March 2019
Review Frequency	Annually
Date of Next Review	March 2020

Version Control

Version Control	Date	Control Reason	Author
1.0	01/05/2010	General review no change. S. Macauley.	-
1.2	01/05/2011	General review no change. S. Macauley.	-
1.3	25/05/2012	Additional reference to monitoring on printers and door access. S. Macauley.	-
1.4	09/04/2014	General Review - Changes Communicated J Murphy	-
1.5	27/07/2016	General Review - no changes S. Macauley	-
2.0	14/08/2018	Review for GDPR	C Morrison

Appendix A: Automatic data logging

System	Data logged	Access restricted to
Network and network application accounts	Login and logoff date/time (AD logs and EventLog Analyzer)	IS
	Volume of disk storage space used by My Documents and Desktop.	
	File access, modifications and deletions (LINKS)	
	File print date/time, printer used and user (MS & Konica Print Server)	
Microsoft Outlook Email accounts	Sender	IS
	Recipient	
	Date/time	
	Email traffic	
	Email volume	
	Flag of any blocked messages	
Internet	User identity and IP address of PC from which request was made	IS
	Date/time of request	
	Full url details of accessed web pages	
	Individual usage is automatically recorded including time spent on each website, volume of downloaded or streamed data and details of any websites blocked by the Sophos Web Appliance.	
	Extension or mobile making call	
Skype for business	Current user activity status	Available to all users on the system
	Time last active on PC/Laptop	
Telephones (landline, or Council owned mobile or Blackberry)	Number called	IS
	Duration of call	
	Cost of call	
	Date/time logging in and out	
Pi	Clock in and Clock out times	HR
	Rule violations	
Door entry system	Date/time of named door opening	
	Card ID	Facilities
GoToMyPC	Login date, time, duration and username for each remote session.	

SunSystems	userID, date/time logged against transaction entry and modifications	IS and Sun/ Q&A users
Q&A Budget Management	Login date/time and worksheet creation, modifications and deletions (Budget Management)	IS and budget management users
Q&A	Q&A application module, user ID, computer name, and date/time for login, logoff, error and security events	IS

SunSystem 5 data audit plan

Any addition, modifications or deletions to any of the data items below are logged in the SFC Data Plan against user ID, date and time. The log data is retained for 2 years. It can be accessed by IS and senior staff in Finance.

Data Audit
SSDA_MTCE_PLAN
SSDA_DDR
Accounts (ACNT)
Address (ADDR)
Analysis Dimensions (ANL_CAT)
Analysis Codes (ANL_CODE)
Bank Details (BANK_DETAILS)
Customer (CUST)
Journal Types (JNL_DEFN)
Number Stream
NUM_STREAM
NUM_STREAM_HDR
Purchases
PURCH_BUS_DEFN
PURCH_DEFN
Payment Terms
PYMT_TERMS
PYMT_TERMS_GRP
Supplier (SUPP)
Value Labels (VLAB)
Data Access Groups (DAG)

Appendix B: Overview of Procedure for Web Monitoring

Purpose

1. In keeping with Information and Communications Technology Acceptable Use Policy ["Acceptable Use Policy"] and the Information and Communication Technology Monitoring Policy, this procedure will be put in place to clarify what routine and ad-hoc monitoring of web usage may to be conducted by Information Services, HR and line managers. An impact assessment has been conducted as suggested by the Information Commissioner's Office.

Background

2. Information Services have the capacity to pull various reports to monitor Internet usage by employees.
3. Of key concern to the Scottish Funding Council (SFC) is the prevention of misuse and prohibited use of ICT systems as outlined in the Acceptable Use Policy.
4. This procedure is designed to enable SFC to conduct reasonable monitoring of Internet use by staff members to prevent inappropriate use of ICT.

Available reports

5. The reports below relate to activity that will be regularly monitored by Information Services and HR:
6. Browse Time

    - *Simple browse time reports* list users' browse time and the categories of website they spent most of their time on.
    - *Detailed browse time reports* can be pulled on an individual user. This will break browse time down into the time spent on each category of website and the web address (but not the individual pages) visited.

7. Website Categories

    - Reports can be pulled on the category of website visited e.g. search engines, shopping etc. Some of these categories will be recognised as in violation of policy, e.g., adult/sexually explicit , gambling. Some website will not yet have been assigned a category – these are "uncategorised". These reports can break the categories down to understand the web address (but not the individual pages) visited by a staff member.

8. The reports below relate to activity that will not be regularly monitored but may require to be monitored on an ad-hoc basis:

    - Types of files downloaded (e.g. video.flv, doc.pdf).
    - Bandwidth Use – reports the amount of information downloaded/uploaded and which web addresses information was downloaded from or uploaded to.

Standard Monitoring

Browse Time

- Information Services will routinely provide HR with reports outlining browse time and the categories of website accessed by staff. HR will identify which staff members are accounting for the most browse time, taking their working hours into account. In general, the top 10 users in terms of the proportion of working hours spent online will be sufficient to give an indication of which, if any user's browse time is unusually high.
- Information Services will then supply HR with a report for each individual identified with a breakdown of their browse time in terms of categories of website and domain [homepage] addresses. This will aid HR to understand if there is a reason for unusually high browse time – e.g. whether websites accessed appear to be work-related, whether a page has been left open but idle on a user's computer. It may be necessary to refer to the user's bandwidth use to clarify this.
- HR will highlight to line managers users whose personal browse time still appears to be excessive. They will be provided with the individual users usage report, redacted as necessary (i.e. line managers will not see the homepages accessed unless necessary).
- Line managers will discuss usage with the staff member and document the conversation, supported by HR where necessary. These staff members may be subject to individual monitoring for a set period of time, and will be notified in keeping with the Monitoring Policy.
- Continued excessive personal use may result in disciplinary action. Please refer to the Disciplinary Policy for more information.

Website Categories

- Information Services will routinely pull reports to identify where staff members have accessed website categories that are illegal or are classed as prohibited according to the Acceptable Use Policy. It is recognised that these sites can be accessed by accident, Information Services will generally be able to discern this where the length of time or amount of activity on the website is minimal, and so the Head of Information Services will review the reports and flag concerning behaviour to HR to act upon as necessary.

- Some websites will appear on the report as “Uncategorized”. Information Services will need to access these websites in order to ascertain that the Acceptable Use Policy has not been breached and that the website contains no illegal content.
- Where a website is not illegal or expressly prohibited under the Acceptable Use Policy, the Assistant Director of Human Resources and the Head of Information Services will together decide if the content could still be deemed inappropriate or offensive. This will be flagged to the member of staff concerned as necessary, detailing why the content is considered inappropriate, and access to the site may be blocked pending a review of the Acceptable Use Policy.