THE UNIVERSITY of EDINBURGH

Use of Operational Data
Policy

Overview

1. Whilst accessing University services, systems or data, some user activity is recorded in log files that are stored to allow subsequent analysis for a number of operational reasons. Where such data contains personal information, it is collected and processed in line with published privacy statements and against a confirmed legal basis for doing so. Data collected varies depending upon the service or system involved but could include date/time of access, IP addresses, UUN, identity of access points (wired or wireless).

2. The uses to which this data is put are widespread and cover day to day operational requirements, such as fault resolution; service capacity planning and provision of enhanced services, such as estate capacity management. There are also other uses that require a higher level of oversight and they are subject to additional scrutiny before access is granted – this would include HR/student investigations, or cases where personal safety was at risk. In some, limited instances, there may be a requirement to correlate operational data with other existing data sets (HR records, student systems, IDM, door access records etc) held by the University to add context and turn this data into actionable information. Finally, there may also be some use cases where University research might benefit by accessing anonymised extracts of operational data. Whatever type of access is required, all access will be proportional and limited to strictly necessary activity.

3. Benefiting from the use of operational data is not without limitations, so access to the log data cannot necessarily address every scenario or use case. This is particularly of note in cases where Type 2 access is involved. For example, whilst it may be possible to identify an individual user has accessed a particular wireless access point (WAP), it may not be possible to be certain that the actual person linked to that identity was present as their account or device may have been compromised; the device may have been left in the location or borrowed by someone else. All that could be confirmed would be a device registered against a WAP at a specific time. Similarly, it may not be possible to identify individuals if there are multiple people connected to the same access point at the same time. It should also be noted that the use of log data for evidential purposes may be problematic as maintaining a demonstrable chain of custody for the data would be challenging. Although access to the log data is strictly limited, there is still a possibility that the log data could be altered prior to being copied.

Purpose

4. The University provides authorised users access to network connection services to enable them to carry out their work, studies or other approved activity which supports the overall objectives and operations of the University by connecting their end user devices to University systems, services and data. Whilst using network connection services, user activity generates log data that is stored for predefined times and uses. This data can be utilized for a number of operational purposes, including those detailed in this document.

Scope

5. This policy applies to all users of University of Edinburgh network connection services, including staff, students, visitors, Alumni or contractors and covers all operational log data, whether hosted locally within University premises or at third party sites.

6. Out of Scope: This policy does not include the management of CCTV systems and data as that is covered by a dedicated CCTV Policy approved via the Estates Committee (CCTV Policy)

Definitions

7. *'Operational Data'* is defined, for the purposes of this policy, as activity log data generated automatically as a result of anyone in scope of this policy interacting with University systems, services or data via any University 'Digital Service'. The data logged by a service is typically pre-determined by the software supplied by the manufacturer, though in some circumstances this may be configurable. It includes data such as user unique identification, IP address details, time and location of network access points, security card access usage and logging related to the specific activity undertaken – e.g. that a user has changed their password or an email had been sent.

8. '*Digital Service'* includes any online service or infrastructure which the University provides, whether operated by the University directly, or on behalf of the University. It includes network connection services that link computing facilities and end user devices; technical services which provide underpinning technologies such as authentication and authorization; and end user services such as email or calendar services.

9. *'End user device'* is defined as any electronic device used to facilitate a connection between an authorised user in scope of this policy and University systems, services or data, irrespective of ownership of the device.

Use Cases

10. The collection and subsequent use of operational data is required for a number of purposes, some of which occur on a day-to-day basis (type 1 access) and some of which are less frequent and more focused (type 2 access). These uses include the following:

    10.1 **Network Capacity Planning (Type 1 access)**. . Details of device connections are logged and analysed to ensure the University has sufficient capacity to support current operations and allow for anticipated expansion.

    10.2 **Fault Resolution (Type 1 access):** To allow support teams to identify and rectify faults with digital services

    10.3 **Information Security Incident Management (Type 1 access):** Log data containing details of user access is utilised to support the resolution of information security incidents such as phishing email campaigns, malware infections, DDoS attacks.

    10.4 **Estate Capacity Management (Type 1 access):** To support the management of the University estate, for example main library occupancy levels, data is collected from user interaction with the network. This data is anonymised as part of the collection and analysis process, and no personal data is made available to published dashboards.

10.5 **Information Security/HR/Student Investigations (Type 2 access):** Log data including user identity details, network access points, timings etc can, in exceptional circumstances be used a part of information security, or formal HR or Student investigations. Operational data may also be combined with other University owned data to provide actionable information.

10.6 **Personal Safety (Type 2 access):** Where a risk to individual or group safety is identified, operational data may be used to help manage that risk. Whilst care to obtain prior approval, outlined above will be sought, in extreme circumstances, approval may need to be retrospective.

10.7 **Personal/Group Health (Type 2 access):** Where a risk to individual or group health is identified, operational data may be used to help manage that risk, for example via Scottish Government Test & Protect requirements. Whilst care to obtain prior approval, outlined above will be sought, in extreme circumstances, approval may need to be retrospective.

10.8 **Use of Operational Data for Research purposes (Type 3 access**). Where it can be demonstrated there are material benefits to researchers accessing anonymised extracts of operational data, such access may be approved.

Procedures

11. Type 1 access covers routine day to day use of operational data and is driven by the needs of the University. Access is linked to specific individual roles and approval for regular access is deemed by default as part of the role approval process. No further access approvals are required.

12. Where exceptional Type 2 access is required; requests must be made via the appropriate Head of College or Professional Services Group, Head of HR, Director of Legal Services or Deputy Secretary, Student Experience. Where ISG maintain the log data, the request for the data will be reviewed and authorised by Director ITI/CISO. Where specific personal information is being sought, there may also be a requirement to consult with the University DPO and the AI and Data Ethics Advisory Board. Where operational data is managed locally within Schools or Colleges, a similar level of access approval should be implemented, especially where Type 2 data is involved.

13. Requests for approval for Type3 access must follow local research sign off routes and be accompanied by a DPIA, risk assessment and ethical review. It is anticipated that access to operational data for research purposes will only be approved if the data has been anonymised prior to release to the research team. All requests must therefore outline how this will be achieved. Access to ISG maintained log data will be subject to final approval by the Director of ITI and CISO.

Exemptions

14. Any requests for an exemption to this policy must be sought from the Vice-Principal and CIO in the first instance.

Policy Effective date

15. The policy will be effective from November 2020.

Review of Policy

16. The policy will be reviewed by the Vice Principal and CIO and any amendments will be approved by the University Executive.

17. The schedule for policy review is as follows

Review	Year
Review 1	November 2021
Review 2	November 2022
Review 3	2025 – moving to a 3 year review cycle

This is the first version of this Policy:–

Policy Version	Amendment Made	Amended by/Date	Approved by	Approval Date
Draft version 0.1	First Draft	CISO	N/a	N/a
Draft version 0.2	Incorporating comments from Director ITI	CISO 07/09/2020		
Version 1	Updated following discussion at University Executive	CISO 11/11/2020	CIO	

Related Governance

Information Security Policy

Computing Regulations

Code of Student Conduct

Regulation of Investigatory Powers

University of Edinburgh Privacy Notices