Call Recording Policy

Version 1.0

Effective from: 06/02/2024

1.0 Purpose & Scope

The purpose of this document is to:

1. define policy on call recording on University managed telephony systems.
2. ensure that recording of the calls, storage, access to and retention of the recordings is consistent and in accordance with relevant legislation and University Policy (see section 4.0 Related Documentation), including:
    a. GDPR 2016 and Data Protection Act 2018
    b. Human Rights Act 1998
    c. University Records Retention Schedule.
3. define that any monitoring of recorded calls may only be carried out to the extent permitted or as required by law under the Data Protection Act 2018 and the Investigatory Powers (Interception by Businesses, etc. for Monitoring and Record-keeping Purposes) Regulations 2018.

This Telephony & Call Recording Policy is subsidiary to the IT Acceptable Use Policy which outlines rules for the use of University IT facilities and services.

2.0 Policy Statements

2.1 Justification for call recording

Each service area that requires calls to be recorded must ensure that call recording is justified and proportionate and will be handled in accordance with this Policy.

The IT Services department is responsible for providing the corporate telephony and call recording system. Establishment of any other telephony services must be subject to assessment and discussion and formal approval with the Director of IT Services and the Director of People & Services.

The University telephony systems are used by service areas across the University. In a limited number of customer facing areas telephone calls are recorded and are subject to monitoring for the purposes of:

- Monitoring the quality of call handling and customer service, and ensuring University compliance with regulatory procedures
- Facilitating staff training
- Verifying customer agreements during specific service requests
- Verifying what was said in the event of a dispute or complaint
- Protecting staff from abusive behaviour.

2.2 New Requests for call recording

New requests for call recording must be directed to the Network Services Manager (with responsibility for telephony services), outlining the service area, clear business reasons for call recording and outline of the levels of access that staff within the service area would need to access and review the call recordings. Such requests may be for a time limited period.

The requester must discuss the scope of their call recording request with the Data Protection Officer (DPO). The requester should complete a Data Protection Impact Assessment (DPIA). The outcome of the DPIA and advice from the DPO should be included in the request to the Network Services Manager. The request should establish how long the recording should be retained, in line with the requirements in section 2.5 below.

If new requests for call recording, include service areas where sensitive personal data (special category data), validation of identity or payment card data is to be provided, e.g. fundraising or marketing campaigns or for a specific research project, the requester should also discuss the request with the IT Services Security team and the Finance PCI DSS team, to ensure that appropriate mitigations are included. The requester must be mindful of the relevant legislation or University policy that relates to their request. This includes (but is not limited to): Research Ethics and Integrity (research projects) or Privacy & Electronic Communications Regulations (marketing campaigns).

2.3 Notification of call recording: Staff

Staff in the relevant service areas must be informed that their telephone calls are recorded. This should include: why the calls are recorded; how the recordings will be used; and how long the recordings are retained before deletion (see section 2.5 Retention).

This notification should be part of new staff induction in the service area, as well as a regular notification (annually) that calls are recorded.

Where possible, extensions that are recorded should be marked/labelled to inform users of that fact.

Staff who are likely to use an extension that is recorded must be reminded that only business calls should be made on that extension.

Where staff are using an extension that is constantly recorded, they must have access to an extension that is not recorded to allow them to make or receive confidential calls (e.g. to receive urgent family calls, to make calls to staff representatives or to have a confidential discussion with a line manager).

Staff in other service areas that frequently talk to staff using recorded extensions must be informed that calls to these extensions are recorded.

2.4 Notification of call recording: Customers

Customers must be notified that their telephone call is being recorded.

This must be notified at the beginning of **every** call, outlining the purposes for call recording. Each business or service area can record their notification message (in line with this policy). The notification will be applied by IT Services Networks & Unified Communications team. If an automated notification is not operationally feasible the business or service area will make all reasonable efforts to ensure callers are aware of call recording in advance and that a record of these actions must be recorded.

If a customer is rude or abusive during a telephone call on a recorded extension, they should be reminded that the call is being recorded and the contents may be reviewed.

Where there is a need to verify a decision of the caller (e.g. that the information they have provided in support of an application is true and accurate) they must be reminded that the conversation is being recorded to verify their decision.

2.5 Retention of enquiries including recording of calls

Recordings of calls should be held within IT services centrally IT facilities and services, where they are secure and accessible if required.

Call recordings should be retained for a maximum of 12 months, with individual areas of the University implementing a locally agreed retention period within this maximum timeframe that reflects business need.

If specific call recordings become relevant to a long-term query, for example an investigation, disciplinary or legal query, (see section 3.0 Compliance), these call recordings may be extracted from the system and stored securely in a separate location. These recordings will then become a record of the query and will be retained in line with the retention period appropriate to that record type.

3.0 Policy Compliance

3.1 Access to and security of call recording systems

Call recording systems must have security features that control access to recordings, with only nominated staff able to download, copy, share or delete recordings. This level of Privileged access should be reviewed and confirmed on a regular basis, at least annually.

Call recordings should only be retrieved and reviewed for the following specified purposes:

a) To monitor the quality of call handling and customer service, and ensuring University compliance with regulatory procedures,

b) Facilitating staff training, coaching and support,

c) To verify the customers agreement during certain service requests,

d) The verification of what was said if there is a dispute or complaint,

e) To protect staff from abusive behaviour.

Call recordings can be played back from the system for use within the Service Area for the agreed purposes by staff who have an operational need to do so. The area supervisor should maintain a record of these instances and ensure that access is proportionate.

3.2 Investigation requests

In accordance with the IT Acceptable Use Policy (section 3.2), where there is a concern or request to investigate an individual's use of IT facilities and services, an IT activity investigation request form must be completed. IT activity investigations should only be initiated where there is a specific and justified need concerning an allegation of misuse or policy breach, an IT security incident, or a formal request from the Police or other regulatory or law enforcement body. Guidance and forms relating to IT Activity Investigations Requests or Subject Access Requests are listed below. Monitoring the effective function of the call recording facility i.e., reasons outlined in section 3.1 above does not fall within the scope of an investigation.

4.0 Related Documentation

Policies

This section lists policies that are directly relevant to the scope of this policy.

University Records Retention Schedule

Data Protection Policy

IT Acceptable Use Policy

Guidance and Forms

- IT activity Investigation Request forms are part of the Information Access Catalog located within the IT Services self-service portal: https://servicedesk.liverpool.ac.uk >Requests> Information Access forms

- Data Protection Impact Assessment template Data Protection Impact Assessments - Legal & Governance Intranet - University of Liverpool
- Under the UK GDPR, all individuals have the right to request a copy of the personal data that the University holds about them. This is called a Subject Access Request (SAR) – Advice is provided here at https://www.liverpool.ac.uk/legal/data_protection/subject-access-request/
- IT Services webpages: https://www.liverpool.ac.uk/it/

5.0 Document Control

Policy version Control			
Author	Summary of change	Version	Authorised & Date
Information Security Officer	New Policy	V1.0	IT Services SMT: 08/01/2024 IGC: 31/01/2024
Policy Management & responsibilities			
Owner	This policy is owned by the Director of IT Services (Chief Digital Information Officer). The CDIO has authority to issue and communicate policy on IT facilities and services – this includes telephony services and call recording.		
Service owner	The CDIO has delegated responsibility for the day-to-day implementation and communication of the policy to the Network Services manager and the Unified Communications Team leader.		
Policy Enquiries	Please direct any queries about this policy to the IT Services self-service portal https://servicedesk.liverpool.ac.uk for the attention of the Networks team		
Policy Review			
Review Due	Annually by January 2025		
Document Location	IT Services webpages https://www.liverpool.ac.uk/it/regulations/		
** The Service Owner is responsible for publicising this policy document. **			