Policy			**Ref: XXX**
Brief Description & Purpose:	Call recording was introduced to Northumbria University in 2018. Since this time, it has proved invaluable in training Northumbria University staff to improve their Customer Service and has also helped resolve some issues and complaints between customers and the university. Both Inbound and outbound calls are recorded automatically for All Services, with the exception of the following: - IT Service Desk - Direct Calls to and from the individual extension or mobile of a University member of staff - Calls that are transferred to an individual extension or mobile number of a university member of staff		
Applicable to (list cohorts):	**Staff:** All staff, including Governors and co-opted Board Committee Members	**Students:** All students when using University Telephony Software	**Third Parties:** All who are in a formal relationship with the University
Effective From:	22.09.2021	**Last Review Date:**	07.11.2022
Approval Authority:	Employment and Finance	**Approved:**	22.9.21
Executive Owner:	Executive Director of SLAS	**Business Owner:**	Director of Student Engagement
Next Review Date:	07.11.2025	**Publication External Y/N**	Y

1. Introduction

The purpose of this policy is to govern the procedures for telephone call recording within Northumbria University ("we") and the management of access to and use of the recordings. The policy aims to minimise intrusion by restricting the recording of calls and access to and use of these recordings to limited and specific purposes.

2. Legislative, Regulatory and Strategic Context

The recording and monitoring of telephone calls is affected by several items of legislation, in particular:

- Article 8 of the Human Rights Act
- Data Protection Act 1998 Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBP Regulations)

The recording of employee's telephone calls has also been the subject of guidance from the Information Commissioner within the ICO's

Employment Practices Code and Supplementary Guidance which has been incorporated into this policy.

If it is likely that conversations that include data relating to a customer's credit card, debit card or bank account details will be recorded, advice must be sought from IT Security to ensure compliance with Payment Card Industry Data Security Standard (PCI DSS), and a record of the advice retained.

3. Policy Detail

3.1. Implementing Call Recording

Before a service area commences call recording, for an existing University system a business case must be made to their Head of
Service for appropriate licences to be issued and for permission to use Call Recording for their Service. This must include:

a. A clear and valid reason for recording calls.
b. Confirmation from the IT Security Manager that the service's call recording system and processes are compliant with PCI DSS and IT Security Standards.
c. Confirmation that the that a Data Privacy Impact Assessment (DPIA) has been completed and the call recording is compliant with corporate information governance policies.
d. Confirmation from the HR Manager that call recording is compliant with HR policies and that recognised Trade Union(s) and staff have been properly consulted.
e. Details of the levels of access that various staff groups or individual staff would have to recordings. Only the corporate Call Recording System may be used to record telephone calls. If an alternative system is being considered, this must be discussed with and agreed by IT Services, and then points "a" to "d" above followed.

Upon receipt of all the above permission, then a ticket should be raised with IT requesting the licences.

3.2. Staff Issues

Where staff are using a telephone system that could allow their telephone conversations to be recorded the following actions must be
taken:

a. All reasonable efforts must be made to ensure that staff are aware that calls may be recorded. (These recordings occur when Horizon is used to make and receive calls, regardless of the device used and anywhere that the member of staff is working) To achieve this staff using the system for the first time must be told that calls may be recorded, and they should be reminded every 12 months.
b. Staff must be made aware of why calls are being recorded, how the recordings may be used and the retention policy for those recordings.
c. 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 or to cancel the recording facility (e.g. to receive urgent family calls, to make calls to staff representatives or to have a confidential discussion with a line manager).
d. Staff who are likely to use an extension that is recorded must be made reminded that only business calls may be made on that extension.

3.3. Customers

If it is likely that a call to or from a customer will be recorded, then all reasonable efforts must be made to ensure that callers are aware of this fact. Whenever possible this will be achieved by placing relevant notifications on the “Contact Us” corporate website for Northumbria University and by ensuring that a notification of recording is given at the start of the call. If this is not operationally feasible, we 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.

When telephoning customers from a recorded extension they must be informed that the call is being recorded at the beginning of the call.

If a customer is abusive during a telephone call on a recorded extension, they must be reminded that the call is being recorded and that its 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.

Where a customer is providing confidential information, there must be a facility to pause recording and the customer advised when:

1. Call recording has been paused; and
2. When the recording is restarted

3.4. Use of Call Recording

3.4.1. Which calls are recorded?

Both inbound and outbound calls that are routed through the horizon software

3.4.2. Which calls are not recorded?

Calls to and from any of the following Services:

- IT Services
- Direct to the individual extension or mobile of a university member of staff

- Calls that are transferred to an individual extension or mobile number of a university member of staff

3.4.3. Why do we record calls?

We use call recording for the following reasons:

- To monitor the quality of call handling and customer service
- Staff training, coaching and support
- The verification of what was said if there is a dispute or complaint
- To protect staff from the abusive behaviour
- To verify the agreement during certain requests such as Clearing Offers
- To improve First Contact Resolution by directing callers to the best Service to answer their query
- To support any request from the Emergency Services and/or Northumbria's own Security Department

Release of any information would be subject to appropriate permissions being received – *as detailed in the Access Matrix at the foot of this document*

Call recording system must have security features that control access to recordings, with only nominated staff able to download, copy, share or delete recordings.

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.

3.5. General Call Recording Storage

3.5.1. Supplier

Call recordings are held by Northumbria's third-party supplier, Gamma. The recordings are encrypted before they are saved to disk, with AES256-bit encryption. They are decrypted as they are streamed for playback or downloaded. At no time are they permanently stored unencrypted on disk. This ensures compliance to BS10008.

BS10008 compliance, means customers' recordings are admissible in a UK court of law.

The service platform is ISO20000, ISO27001 and ISO22301 compliant, Cyber Essentials certified, listed on the Cloud Security Alliance STAR Registry and featured on the VISA Europe Merchant Agent list for the secure storage of PCI DSS sensitive call recordings.

These calls will be automatically deleted after 6 months (or earlier in the case of calls into Security

3.5.2. Other Call Recording storage

Call recordings are retrieved for the following reasons:

- To support investigation into an issue/complaint from a caller
- At the request of the Police or other Regulatory Body
- For training and monitoring
- At the request of the person who handled the call, who wishes to gain further clarity on how they handled the call.

These call recordings will be stored separately in files pertaining to the reason for the retrieval, and will be deleted within 6 months unless:

- They can be deleted sooner
- They are deleted within one month of any investigation being fully completed and authorisation for the deletion has been obtained from the Assistant Director of the Service to which they relate

3.6. Access to Call Recordings

Call recordings can be accessed by Line Managers for training and quality assurances purposes.

Personal requests for call recordings from individuals are handled through a Data Subject Access Request (SAR) and such requests must be made in writing to the Data Protection Officer. Please refer to the Subject Access Guidance for further information.

Specific call recordings may be accessed by Line Managers and Human Resource Managers *(subject to the permissions in the Access Matrix shown at the foot of this document)* as part of the investigation into a potential staff management matter and where appropriate, used as evidence. In these cases, requests for access (made in writing) may only be granted by the HR Manager in consultation with the Data Protection Officer.

Call recordings may be used outside of the Service Area they belong to for an agreed purpose to deal with issues arising from the original call with the permission of one of the following:

- Manager of Service Area (nominated by Head of Service)
- Senior Information Risk Officer
- Head of Legal Services
- Data Protection Officer
- Member of the University Executive

Recordings released to other Service Areas must be kept securely and in compliance with this policy. Once the recording has been used for the agreed purpose it must be deleted.

If a service area wishes to use a recording for a purpose other than those identified in above or for a purpose unrelated to the reason for the call, advice must be sought from the Data Protection Officer.

3.7. Disclosure of calls to third parties

Copies of calls requested in relation to Subject Access Requests, Fraud Investigations and Complaints must be approved by the Data Protection Officer in line with internal guidance.

Call recordings may only be released to an external agency such as the police or law enforcement or to any third parties with the permission of one of the following:

- Data Protection Officer
- Head of Security
- Senior Information Risk Owner

For the release to third parties, the following must be recorded:

- The purpose for which it is being released
- The person requesting the recording
- The date/time of the recording
- Who authorised the release?

3.8. Retention of Calls

3.8.1. Retention

- Call recordings are retained for 6 months (maximum) at which point they are automatically deleted.
- Any call recording can be deleted at the request of the Caller at any time.
- The University can take up to one month to delete a recording as specified under GDPR (Right to Erasure)
- Call Recordings that are held for longer than 6 months (due to an on-going investigation or complaint), will be deleted when the investigation or event has been finalised.

3.8.2. How to delete a Call recording

- The caller requests suspension of the recording during the call.
- Or: The caller requests that it is deleted after the call has been made, and the Data Protection Officer will ensure that your request is completed.
  Please note, a deleted Call Recording will remain in Advanced Comms for 7 days, after which it can never be retrieved.

4. Escalation Routes Where Breach in Policy Occurs

All staff are responsible for reporting breaches within the Call recording policy due to the Breach Reporting Policy. Within the policy, breaches may occur from the following (please note this list is not exhaustive):

- Failure to comply with deletion procedures.
- Sharing of calls to those who do not have access.
- Call recordings being stored for more than 6 months.

Breaches of the Call Recording Policy may be treated as a disciplinary matter and a breach of the Code of Conduct, particularly where the breach has exposed the University or its staff to actual or potential risk, damage, or loss.

5. Key Roles and Responsibilities

Key owners of the Call Recording System are outlined below. Please view the Access Matrix below for full roles and responsibilities.

Role	Responsibility
Current operational Owner of Call Recordings (with permission from the Deputy Director GMB)	The Operational Owner listens to and assesses call recordings (except for Security), across the University to determine improvements to be made, to support University Projects, improve processes, develop training and to improve the Customer Experience
Nominated Telecomms Analyst	The Telecomms Analyst is responsible for deleting call recording when requested by a customer/caller (Via authorisation from the Operational Owner of Call Recording and the Data Protection Officer)

Call Recording Access Matrix

Call Recording - Access Matrix for Managers										
Who	**Access to MyInbound to manage their own IVR**	**Access to Advanced Comms to listen to calls of their own Service**	**Listen to calls (or part thereof) transferred to another Service**	**Listen to calls for training and monitoring purposes**	**Listen to calls where a complaint has been received or a Fraud Investigation needs to be completed**	**Listen to all calls across any Service (Except Security)**	**Delete Call Recordings**	**Lisen to all calls to support an investigation**	**Share call recordings with a Third Party including the caller**	**Share calls with External Agencies**
Accommodation	No	Yes	No	Yes	Must be approved by the Data Protection Officer	With permission of one of the following: Head of Service, Senior Information Risk Officer, Head of Legal, Data Protection Officer, Member of University Executive	Submit request by email to Data Protection Officer and Operational Owner of Call Recordings. Operational Owner of call recordings then deletes the recording.	With permission of one of the following: Head of Service, Senior Information Risk Officer, Head of Legal, Data Protection Officer, Member of University Executive	After obtaining a Subject Access Request	With permission of one of the following: Senior Information Risk Officer, Data Protection Officer, Head of Security
Ask4Help/StudentLifeandWellbeing	Yes	Yes	No	Yes						
Switchboard	Yes	Yes	No	Yes						
Campus Helpdesk	No	Yes	No	Yes						
Finance	No	Yes	No	Yes						
Business Growth	No	Yes	No	Yes						
Placements and Internships	No	Yes	No	Yes						
Human Resources	No	Yes	No	Yes						
IT Service Desk	No	Yes	No	Yes						
London Campus	No	Yes	No	Yes						
The below roles are subject to the same rules as detailed above										
Assistant Directors/Head of Service	N/A	N/A	No	Yes	Yes	Yes	No	Yes	Subject to SAR	No
Human Resources Managers	N/A	N/A	Yes	Yes	Yes	Yes	No	Yes	Subject to SAR	No
Operational Owner of Call Recordings	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Subject to SAR	No
IT Telecomms Analyst	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	No

6. Related Policies, Procedures and Other Resources

Gamma is the third-party supplier to Northumbria for the four systems pertaining to Call Handling:

- Horizon – an App used to answer calls (found in Northumbria's Software Centre)
- Advanced Comms – a system where recorded inbound and outbound calls can be retrieved - https://advancedcomms.co.uk/
- My Inbound – a system where Interactive Voice Response (IVR) messages can be amended - https://www.myinbound.com/#!/app/welcome
- Akixi – a reporting portal - https://gamma.akixi.com

8. Version

Version No.	Reviewer	Date	Changes
1.0	University Executive, E&F Committee	22.9.22	*Pre-2022 guidance version*
1.1	Jill Dunn	07.01.22	*Minor design changes, updating links/names etc*
1.2	Jill Dunn	07.11.22	*Minor design changes, updating links/names etc*