Corporate Policy and Resources Committee	
Thursday, 11 April 2019	

Subject: Recording of telephone calls

Report by:	Executive Director of Operations
Contact Officer:	Lyn Marlow Customer Strategy and Services Manager lyn.marlow@west-lindsey.gov.uk
Purpose / Summary:	Approve updated policy for call recording of customer telephone calls

RECOMMENDATION(S):

a) Members approve the amended policy for formal adoption;

b) Delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policy in future, in consultation with the chairman of the Corporate Policy & Resources committee and chairman of JSCC

IMPLICATIONS

Legal: N/A

Financial: There are no financial implications resulting from this report

FIN REF: FIN224/19

Staffing: HR086-2-19

Equality and Diversity including Human Rights: N/A

Risk Assessment: N/A

Climate Related Risks and Opportunities: N/A

Title and Location of any Background Papers used in the preparation of this report:

Telephone recording policy 2009 at appendix 1 of this report.

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)	**Yes**		**No**	**X**

Key Decision:

A matter which affects two or more wards, or has significant financial implications	**Yes**		**No**	**X**

1. Background

1.1 The Council created a call recording policy in 2009 and a copy of this can be found at Appendix 1 of this report.

1.2 Following an upgrade to our telephone system and requirements to adhere to new legislation and compliance the policy requires a refresh. The new policies can be found at Appendix 2 (internal and 3 (external) of this report.

2. Changes of note

2.1 The new policy now reflects the need to adhere to Information Security (GDPR)

2.2 The policy now advises that recorded calls will be retained for 6 months rather than the previous 12 months.

2.3 Call recording will now take place for the Revenues and Housing Benefits teams whereas previously it was calls to Customer Services only.

2.4 It is now possible to use manual intervention to record calls made to other extensions, outside of the contact centre, during periods of service monitoring.

2.5 The policy reflects that the Council has implemented a mid-call solution in order to comply with Payment Card Industry Security Standards (PCiDSS) which was not previously a compliance requirement.

2.6 Customers are advised that they can opt out of call recording by terminating their telephone call

2.7 Authorisation is now given to the POD manager to be able to use/listen to calls as a result of evidence gathering for a disciplinary investigation or hearing

2.8 Customers can ask to have a copy of their recorded calls emailed to them on an audio file

2.9 A telephone extension will be identified that staff can use to make a private calls to a trade union for example, that will be excluded from call recording.

2.10 Our GDPR obligations are set out in the policy.

2.11 A separate (external) customer policy has been created reflecting all of the above where appropriate

3. Benefits of call recording

3.1 **Compliance:** We are PCiDSS compliant and able to demonstrate this.

3.2 **Dispute Resolution:** Call recording provides an accurate version of events

3.3 **Training & Improved Customer experience:** Call recording is great tool for training staff, can be utilised for quality monitoring, allows for continued development and identification of change to improve the customer experience.

Appendix 1 – call recording policy 2009

Call recording policy Jan 2009

Purpose

The purpose of this policy is to govern the procedures for call recording within West Lindsey District Council and the management of access and use of telephone call recordings.
The implementation of recording of telephone calls was agreed in order to support effective training, performance monitoring and delivery of excellent customer services, across the whole council, and to enable the council to deal efficiently with internal or external complaints.

Scope

The policy aims to minimise instruction by restricting access to and use of recording to limited and specified purposes only.
This policy outlines:

- Recorded information
- Purposes of call recording
- Access and availability
- Data Protection
- Monitoring and review

Recorded Information

All calls received by the contact centre will be recorded and stored securely for up to 12 months
Call to and from other officers within the council are not currently recorded.

Purposes of call recording

The purpose of call recording is to provide an exact record of the call which can:

- help protect officers from abusive or nuisance calls
- establish the facts in the event of a complaint either by a customer or a member of staff and to assist in resolving it
- help identify officer training needs and to support training new and existing officers; and

Internal access and availability

Access and playback of recordings will be carefully controlled as per the requirements of Data Protection
Only those with the appropriate authority can access calls.
Access to calls may be for a number of reasons. We anticipate the three main reasons will be for;

- Checking accuracy
- Answering complaints
- Training to improve services and skills

An individual officer may request to hear call recordings in which they are personally involved, and any Head of Service may request to hear call recordings which involve a member of their team. They should make a request detailing the reason for hearing the recording to Lyn Marlow or Alan Robinson

Every caller to 676676 is notified that the call may be recorded. This is done through a pre-recorded message within the council's telephone welcome message before a connection is made to an officer.

Appendix 2 Call Recording Policy – Internal

Internal Call recording policy

Document Control	
Organisation	West Lindsey District Council
Title	Call Recording Policy
Version	1.0
Author	Lyn Marlow, Customer Services Manager
Filename	Call Recording Policy
Subject	Management of information
Review Date	January 2019

Revision History/date	**Reviser**	**Previous version**	**Description of revision**

Internal Telephone Call Recording Policy

1: Purpose

1.1 The purpose of this policy is to govern the procedures for telephone call recording within West Lindsey District Council and the management of access and use of telephone call recordings.

1. 2 The implementation of recording of telephone calls was agreed in order to support effective training, performance monitoring and delivery of excellent customer services, across the whole council, and to enable the council to deal efficiently with internal or external complaints, implementation of customer standards and training of staff in the delivery of excellent customer service.

2: Scope

2.1 The policy aims to minimise intrusion by restricting access to and use of recording to limited and specified purposes only.

2.2 This policy outlines:

- Recorded information
- Purposes of call recording
- Access and availability
- Information Security (GDPR)
- Monitoring and review

3: Recorded Information

3.1 All calls received or made from nominated extensions will be recorded using the Councils Red Box call recording system and will be stored securely for up to 6 months and will then be automatically deleted, unless highlighted for the purposes of evidence gathering.

3.2 Telephone calls currently included in the call recording scope are the following services:

- Customer Services
- Revenues and Benefits

3.3 Call recording will apply to all calls made and received and will include both external and internal calls

3.4 Calls to and from other officers within the council will not routinely be recorded but may be recorded during periods of mystery shopping events

3.5 Calls where the caller provides details of a payment card will be subject to a mid-call solution in order to comply with Payment Card Industry Security Standards (PCiDSS), ensuring that the Council will not hold any credit/debit card data.

4: Purposes of call recording

4.1 The purpose of call recording is to provide an exact record of the call which can:

4.a help protect officers from abusive or nuisance calls

4.b establish the facts in the event of a complaint either by a customer or a member of staff and to assist in resolving it

4.c help identify officer training needs and to support training new and existing officers; and

4.d assist the council's quality control to identify any issues in council processes, with a view to improving them

4.2 In addition, recordings may provide evidence for crime prevention purposes or internal investigations.

5: Internal access and availability

5.1 Access and playback of recordings will be carefully controlled as per the requirements of GDPR

5.2 Only those with the appropriate authority can access calls. (See below)

5.3 Access to calls may be for a number of reasons. We anticipate the six main reasons will be for;

5.a Checking accuracy
5.b Answering complaints
5.c Training to improve services and skills
5.d Mystery shopping events
5.e Internal investigations
5. f Maintenance of the call recording system by the ICT team

5.4 An individual officer may request to hear call recordings in which they are personally involved but must do this via their team manager, who will submit a request via request it option on Minerva.

5.5 Any team manager or above may request to hear call recordings which involves a member of their team. They should make a request detailing the reason for hearing the recording via request it option on Minerva.
5.6 It should be noted that Senior Customer Services officer and the Customer Experience officer will, on a weekly basis, listen to calls in order to undertake performance monitoring of staff within Customer Services. Exceptions to this are the following:

5.6.1 Where the Customer Strategy and Services Manager has delegated actions to a designated deputy or equivalent, for the purposes of mystery shopping or dealing with a complaint, listening to any calls that have been recorded be that in real time or retrospectively.
5.6.2 Where the People and Organisational Development manager has delegated actions to a designated deputy or equivalent, for the purposes of evidence gathering during a disciplinary investigation or hearing.
5.6.3 In addition, Team Managers, can request to hear the recordings of a specific call or a random selection of calls for quality monitoring purposes.

5.7 Calls to be listen to will be accessed via the red box system only, calls will not be downloaded unless required as part of evidence in an appeal, hearing or employment tribunal.

5.7.1 Downloaded calls will be sent via email in an audio file, if required to be used as evidence as stated in 5.7

5.8 Authorisation to review calls will be granted by the Customer Strategy and Services or the People and Organisational Development Managers.
5.9 A telephone extension, that will not be subject to call recording by being excluded from the recording system, can be made available for confidential calls e.g. to union/manager

6. GDPR
6.1 A DPA has been carried out and is at Appendix A of this policy
6.2 Recordings constitute the personal data of the caller and the operator. Therefore they will be manage in such a way that the rights of the data subject (callers and operators) can be fulfilled, and all obligations of the data controller (WLDC) are observed, as per our data protection policy.
6.3 Every caller who telephones 01427 676 676 will be notified that the call may be recorded and why before the conversation commences. This is done through a pre-recorded message within the council's telephone welcome message before a connection is made to an officer. Details of call recording and the Councils GDPR requirements are also notified on our website
6.4 Recordings will be retained for 6 months and then automatically deleted
6.5 Some recording may be retained for longer than 6 months for the following reasons

6.a Required for a complaint. In this case the recording will be retained until the completion of the complaint process, including any appeals processes.

6.b Required as part of a staff disciplinary process which may result in use of employment tribunal

6.d Recording that have been identified by the following officers, Strategic leads for Customer First and Corporate Governance, Customer and Strategy and People and Organisational development managers and as identified as evidence for record keeping requirements in support of the dealing with unacceptable behaviour towards staff and unreasonable persistent complaints.

6.6 Staff need to be aware that customers/callers have the right to listen to or have copies of the recording made of their own calls, via the councils subject access request procedures.
6.7 Recording will be located by the customer/callers telephone number, date and time of the call and the officer's identity
6.8 Recordings will generally be emailed to customers. Exceptions to this will be reviewed as they occur.

Appendix A DPA

Call Recording – Redbox system

Data Protection Impact Assessment

Introduction

The Data Protection Impact Assessment (DPIA) process is an important means of evidencing our compliance with the requirements of the Data Protection Act 1998 and, from May 25th 2018, the General Data Protection Regulation (GDPR).

Where we are introducing new (or amending existing) systems or processes which involve personal data, the proposal will be reviewed against a set of criteria which determines whether it needs to be formally assessed under a DPIA.

The DPIA process will capture:

- *Requirements:* Any compliance issues with the initial requirements of a proposed change
- *Design:* Approval of a design which brings any compliance issues within our risk tolerance
- *Build & Test:* Final confirmation that the implemented change satisfies the agreed measures identified during the process

Completed DPIAs will form part of our ‘Record of Processing Activity’ which documents our practice and provides assurance that we comply with our statutory data protection responsibilities.

The process is also designed to ensure appropriate measures are in place to safeguard non-personal data in our custody, complying with HM Government Security Classification Policy across the OFFICIAL classification; including the OFFICIAL-SENSITIVE caveat.

Our Data Protection Policy sets out the requirement for changes to be reviewed and this process to be followed where the relevant criteria are met, using associated guidance.

The Proposal

About this Assessment

Title of Project:	To implement Redbox call recording software which will record incoming telephone calls to licenced extensions and store the recordings for a period which we can determine. The recordings can be listened to by authorised officers for training, monitoring and the resolution of disputes.

Brief summary and description of the project:

The Council has an aspiration to implement call recording software which will record incoming phone calls to all or selected telephone extensions, subject to licensing. This will allow call recordings to be replayed in the event of a dispute; to provide evidence of conversations; to monitor the performance of our staff and to demonstrate any areas of strength or weakness to aid training and the provision of excellence in telephone communication.

The maintenance and development of the telephony system is provided on our behalf through a contract with Amtech.

The chosen software solution is provided by Redbox.

The software is PCI compliant by automatically suppressing recording when agents access payment services.

GDPR compliance is simplified through search and delete facilities, along with automated retention scheduling.

Callers are advised that call recording is active through the IVR message. Callers can request that their call is not recorded by terminating their call or a call recording can be deleted on request.

Access to recordings is limited to authorised officers and an audit trail is maintained.

DPIA Risk Assessment

Assessment of the proposal against the GDPR 'High Risk' criteria requiring a DPIA

High Risk Processing

Does the processing meet the criteria of 'high risk' processing?	Yes☐
Comments:	
The ICO Guide to GDPR high risk checklist completed and indicates that processing DOES NOT meet the criteria for 'high risk' processing.	

The Data

Describe the data/ list the fields

What items of data are being processed and what is the sensitivity classification?

Field Name (or Data Type)	Format	Classification
Name	Electronic	Official
Contact details (address, telephone number, email)	Electronic	Official
All information disclosed during the telephone conversation which may include personal and sensitive information.	Electronic	Official

(add additional entries as required)

Comments:
It is expected that sensitive information of this nature will not occur on a large scale and will be freely given and not requested.

'Special Categories' of Personal Data

Tick a box if the Personal Data processed fits into a relevant 'Special Category' below.

Religion or beliefs	☐	Genetic data	☐
Race or ethnic origin	☐	Health	☐
Political opinions	☐	Sex life	☐
Trade-union membership	☐	Criminal convictions	☐

Categories of Data Subject

Tick a box next to the categories of data subject whose personal data will be processed

Customers	☒	Complainants (& Reps)	☒	Suspected Offenders	☒
Suppliers	☒	Advisors/ Consultants	☒	License/ Permit Holders	☒
Offenders	☒	Benefits Recipients	☒	Inspected Persons	☐
Claimants	☒	Carers (& Reps)	☒	Captured on CCTV	☐
Students/ Pupils	☒	Incident witnesses	☒	Employees of other Orgs	☒
Landlords	☒	Employees/ Contractors	☒	Holders of Public Office	☒

Data Risk Profile

The general risk level associated with the data, derived from the Risk Treatment Process

For Personal Information		For Business Information	
Impact	Minor (1)	Impact	Minor (1)
Classification	Official	Classification	Official

Overall Risk Profile	Minor (1)

The Principles

Processed lawfully, fairly and in a transparent manner

i. Legal basis for processing

Conditions for Processing

Tick all relevant conditions which provide a legal basis for the processing of personal and special category data.

Personal Data			Special Categories		
6(1)(a)	Consent	☐	9(2)(a)	Explicit Consent	☐
6(1)(b)	Contracts	☐	9(2)(b)	Employment, Social Security, Social Protection law	☐
6(1)(c)	Legal obligation	☐	9(2)(c)	Vital interests	☐
6(1)(d)	Vital interests	☐	9(2)(d)	Not-for-profit body	☐
6(1)(e)	Public Interest/ Official Authority	☒	9(2)(e)	Made public	☐
6(1)(f)	(not applicable to Public bodies)		9(2)(f)	Legal claims / Judicial	☐
			9(2)(g)	Public Interest	☐
			9(2)(h)	Medicine, Employee capacity, Medical Diagnosis, Health or Social Care	☐
			9(2)(i)	Public Health	☐
			9(2)(j)	Archiving, Scientific and Historical Research or Statistical Purposes	☐

Legal Gateway

List any applicable legislation if a 'legal gateway' is selected above

(add additional entries as required)

Consent

If consent is being relied upon, confirm that the relevant conditions are in place	☐
Comments:	
We are not relying on consent for this processing	

ii. Rights

The Right to be Informed

Does the processing support this right?	Yes ☒
Comments:	
• Callers are advised that calls are recorded for training and monitoring purposes through the IVR message • Will be included on Corporate Privacy Notice and the Customer Services departmental privacy notice and any other dept where call recording is in place	

The Right of Access

Does the processing support this right?	Yes ☒
Comments:	
• Information and recordings can be provided if requested	

The Right to Rectification

Does the processing support this right?	Yes ☐
Comments:	
• Calls can't be amended once made	

The Right to Erasure

Does the processing support this right?	Yes ☒
Comments:	
• If a customer requests this, recordings can be searched by a variety of criteria including, date and time, officer name or extension, etc and can be deleted from the database, providing the legal basis enables that right.	

The Right to restrict Processing

Does the processing support this right?	Yes ☒
Comments:	

• **This Right is not absolute. It applies in this case when:**
  ○ **subject contests data accuracy and controller is verifying**
  ○ **data has been unlawfully processed**
  ○ **if data no longer needed but subject needs it for legal claim**
•	

The Right to Data Portability

Does the processing support this right?	Yes ☒
Comments:	
• **Right to Data Portability is absolute where the legal basis is "consent" or "contract".** •	

The Right to Object

Does the processing support this right?	Yes ☒
Comments:	
• **Right to object is not available where the legal basis is "consent" or "contract".** •	

Rights related to automated decision making and profiling

Does the processing support this right?	Yes ☒
Comments:	
• ~~**N/A**~~ • **NO decision making or profiling will take place**	

iii. Data Subject consultation

Describe any consultation with Data Subjects over appropriate processing of personal data

Has any consultation been undertaken with Data Subjects?	Yes ☐
Comments:	
N/A	

Collected for specified, explicit and legitimate purposes

State the 'purpose(s)' for which personal data is being obtained

Purpose 1	Quality assurance and training
Purpose 2	Resolution of queries and to provide evidence
Purpose 3	

(add additional entries as required)

Further processing

Confirm that no further use is intended to be made of the data	☒
Comments:	
No intention to use data for any other purposes than listed above	

Adequate, Relevant and Limited

Minimising Personal Data

Confirm that the personal data being obtained is a minimal amount necessary to fulfil the purposes above	☒
Confirm if any pseudonymisation or anonymisation processes will take place, and if so, describe them below	☐
Comments:	

It is not possible to perform pseudonymisation or anonymisation of data as this will prevent the customer from receiving this service

Accurate and, where necessary, kept up to date

Accuracy	
Confirm that there is a process in place for ensuring that personal data is accurate and is reviewed where necessary	☐
Comments:	
N/A	

Kept no longer than is necessary

Retention	
The process effectively manages retention of personal data and is aligned to the Organisation's published retention schedule	☒
List the relevant Retention Period(s):	
All data will be deleted in accordance with our retention policy of 6 months	
All data will be held on WLDC servers, not Redbox hosted service	

Comments:

Appropriate Security

i. Organisational Controls

a) ***Procurement***

The Tender process:	
Based on the risk rating of the data, this is the level of assurance required for the procurement process	
Procurement Assurance requirement	Stage 1 Only (Minor (1))

Contractual Control:

The contract contains the Organisation's standard contract schedule relating to Information Governance requirements	☐
If the schedule is not in the contract, what equivalent control is in place?	
Formal contract in place with Amtech	

Contract Term: 2 years + year extension option

Start Date:	28 Feb 2018	End Date:	27 Feb 2020
		Optional extension period (years):	1 year

Contract Term:

Start Date:	Feb 18	End Date:	Feb 2020
		Optional extension period (years):	

The Selected Supplier(s) & Accreditation

Supplier Name(s) and whether they are accredited to a recognised Code of Conduct

Supplier Name	Accredited
Amtech	☒
	☐
	☐
	☐

(add additional entries as required for framework contracts/ 'lot' winners)

b) Training

Training in how to securely process the data

Confirm that employees (and users where relevant) of the system will receive appropriate training	☒
Confirm that comprehensive written guidance will be available to employees and users	☒
Comments:	
• **WLDC is responsible for ensuring that training and written guidance is available to designated employees**	

c) Policy

Capture issues impacting on Organisational Policy

Confirm that the proposal does not impact current Organisational Policy in a way that requires a review of a Policy's adequacy? (identify affected Policies below)	☒
Comments:	
• **Will review if any Policies are effected**	

ii. Technical Controls

a) Access

Access controls

Confirm that the Access Controls in place will effectively ensure that only those with a valid need to access the data can do so	☒
Confirm that the Access Controls in place will effectively ensure that a management scheme is in place which assigns and reviews appropriate permissions to view, create, amend and delete data	☒
Comments:	
• **Requests for access to recordings to be made to designated officers who will assess how the recording is going to be used and who it can be shared with** • **Process for requests and authorisation to be in place** • **Access through URL link only – this does not allow the recoding to be saved to any other location and the link is deactivated in accordance with the retention period.** • **Audit trail in place**	

b) Security at Rest

Securing the data within a system

Confirm that appropriate technical security is in place to protect the data at rest from threats appropriate to the security classification of the data	☒
Comments:	
• **Redbox service is PCI and GDPR compliant and has ISO9001 accreditation. Calls are fully encrypted.**	

c) Security in Transit

Securing the data when transferred from one system to another	
Confirm that appropriate technical security is in place to protect the data in transit from threats appropriate to the security classification of the data	☒
Comments:	
Data is encrypted and transmitted securely.	

Demonstrate Compliance

Records of Processing Activity (ROPA)	
Have the Organisation's ROPA entries relating to Information Assets and Data Flows been updated to reflect any change?	Yes ☒
Comments:	
• **Any dept requesting a call recording will need to amend their ROPA**	

Transfer outside the EEA

Transfer of Personal Data to Third Countries

No personal data is anticipated being transferred to third countries, but the activity manager will refer to the Data Protection Officer for assessment if a need arises	☒
There is an expectation that it may be necessary to transfer personal data to third countries and this activity will meet the required criteria in law (comment below)	☐
Comments:	
• **The server is located within the EEA and there is no requirement or intention to transfer personal data elsewhere.**	

Risk Management

#	Risk Ref	Risk Description	Mitigating Control(s)	Likely	Impact	Score
1	Sharing	Personal data and special categories of personal data of citizens could be compromised if inappropriately shared or Redbox is not accessed by an approved user. This will cause potential loss of reputation to partners and the possibilities of actions taken by the regulator as defined under article 58 of GDPR.	• Training and guidance to be available for all users • User access will be controlled/approved by the system administrator	1	1	(1) Minor
2	Sharing	Official Sensitive information regarding Partners' vulnerabilities and risks could be compromised if inappropriately shared or the database is not accessed by an approved user. This will cause potential loss of reputation to Partners and the possibilities of actions taken by the regulator as defined under article 58 of GDPR.	• Training and guidance to be available for all users • User access will be controlled/approved by the system administrator • Access to recordings through application only specifying reason for request and who will listen to it.	1	1	(1) Minor
3	GDPR	Some of the recordings may be given an extended retention period if they are to be used as evidence etc	• Retention periods for the data held within the ROPA database will need to be defined.	1	1	(1) Minor

		Would this would breach principle 1(e) of GDPR, action may be taken against Partners by the regulator as defined under article 58 of GDPR				
4	Governance	Payment card details recorded	• The software automatically suppresses recording when the agent connects to the council payment provider website. • Training and guidance to be available to users	Select	Select	Select

Linked to Risk Register Information Risks	
Education	Breach of IG policies and guidance due to lack of visibility, communication and training
GDPR	Non-compliant with GDPR implementation
Malware	Threat from malicious links/ attachments
Process	Information is lost/ processed in a non-compliant manner due to gaps in processes and poor controls
Purchasing	Limited governance over low spends allows DPIA process bypass
Sharing	Sharing information inappropriately or illegally due to immature technology or understanding of legislation
Supplier	Suppliers breach Privacy Law due to poor information handling practices/ IT security

In accordance with the **Risk Treatment Process**

Score	Risk Class
1	Minor
2	Moderate
3	Major
4	Critical

		Impact			
		Minor (1)	Moderate (2)	Major (3)	Critical (4)
Likely	Critical (4)	Medium (4)	High (8)	Very High (12)	Very High (16)
	Major (3)	Medium (3)	High (6)	High (9)	Very High (12)
	Moderate (2)	Low (2)	Medium (4)	High (6)	High (8)
	Minor (1)	Low (1)	Low (2)	Medium (3)	Medium (4)

Attachments

Please embed relevant documents below.
This section and the documents within will not be routinely published with the DPIA.

Document	Title/ Summary
Information Governance (Privacy Notice/ Consent Form)	
[Embed Doc]	**N/A**
[Embed Doc]	
Project (including Business Case, PIDs etc)	
[Embed Doc]	N/A
[Embed Doc]	
[Embed Doc]	
Design (including Specification, High level, Low level, network diagrams etc)	
[Embed Doc]	N/A
[Embed Doc]	
[Embed Doc]	
Procurement (including IG evaluation(s), Contract/ Agreement)	
[Embed Doc]	N/A
[Embed Doc]	
[Embed Doc]	

Reviews

Regularity of Reviews

The processing does not meet the criteria requiring a review	☒
A timetable for reviewing the processing has been identified, taking into account the intended length of the activity and the risk rating	☐
Comments:	
•	

Review Outcomes

Review 1

Where items below cannot be ticked, explain why in the comments and explain what action is to be taken

Date Review Undertaken:	
Confirm that the processing as initially approved in this assessment remains unchanged	☐
All mitigations remain in place and are effective and appropriate to the level of risk	☐
No further action is required as a result of the review	☐
Comments:	
•	

Review 2

Where items below cannot be ticked, explain why in the comments and explain what action is to be taken

Date Review Undertaken:	
Confirm that the processing as initially approved in this assessment remains unchanged	☐
All mitigations remain in place and are effective and appropriate to the level of risk	☐
No further action is required as a result of the review	☐
Comments:	
•	

(Add additional sections for further reviews)

Approvals

Stage 1 – Requirements Approval (IGIA Stage)			
Function/Role	*Officer Approving (Name)*	*Date*	*Comments*
Customer Services Manager	Lyn Marlow	Sept 18	• N/A
	Cliff Dean	Sept 18	• N/A

Stage 2 – Design Approval (LLD Stage)			
Function/Role	*Officer Approving (Name)*	*Date*	*Comments*
SIRO	Ian Knowles		•
Role 2			•

DPO Sign-off (Design approval – if required)			
Function	*Officer Approving (Name)*	*Date*	*Comments*
DPO	Steve Anderson		•

Stage 3 – Build & Test Approval (All IG mitigations have been delivered in the live solution)			
Function/Role	*Officer Approving (Name)*	*Date*	*Comments*
Customer Services Manager	Lyn Marlow	Feb 19	• N/A
	Cliff Dean	Feb 19	• N/A

DPO Sign-off (Build & Test Approval – if required)			
Function	*Officer Approving (Name)*	*Date*	*Comments*
DPO			•

SIRO Sign-off (Build & Test Approval – if required)			
Function	*Officer Approving (Name)*	*Date*	*Comments*
SIRO			•

Appendix 3 Call recording policy – external

West Lindsey District Council
Policy:
Recording Customer telephone calls
January 2019

1: Introduction

1.1 West Lindsey District Council uses call recording technology and like many organisations, this is standard practice and allows us to monitor the quality of calls, to train and develop our staff, and adhere to compliance and security procedures.
1.2 All calls made from or received into the Customer Services Centre, our reception desks and the Revenues and Benefits Team will be recorded, without exception, if the customer does not wish their call to be recorded then they need to terminate the call and make contact with the Council in a different way.
1.3 Where a call is transferred outside of these teams, recording of the call will end at the point the call is handed over.
1.4 Exception may occur when as part of a planned mystery shopping event other teams telephones calls will be recorded. In this event customer will be advised that the call is being recorded.
1.5 In future the Council will include other teams to be subject to daily telephone call recording and when this occurs this policy will be reviewed.
1.6 The recordings will only be used for the purposes set out in this policy.
1.7 Data/recordings will be held securely and only accessible to authorised users/managers

2: The Purpose

2.1 We will ensure that the recording are used fairly, and that we comply with the requirements of relevant legislation, including:

- The Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Inception of Communications Regulations) 2000
- The Telecommunications (Data Protection and Privacy) Regulations 1999
- Payment Card Industry Data Security Standards (PCiDSS)
- The General Data Protection Regulations 2018
- The Data Protection Act 2018
- The Human Rights Act 1998

3: The Scope

3.1 All calls made from or received into the Customer Services Centre, Reception desks or the Revenues and Benefits team will be recorded. Under normal circumstances, all calls will not be retrieved or monitored unless:

3a. It is necessary to assist with the investigation of a complaint
3b. It is part of our "spot checks" to ensure customer services standards are being met
3c. To help us to improve standards of call handling through use in training and coaching with West Lindsey staff.
3d. There is a threat to the health and safety of staff and/or visitors
3e. To check compliance with regulatory procedures

3.2 The Council reserves the right to undertake planned mystery shopping events of teams not currently subject to daily telephone call recording. During these events customers will be advised that telephone call recording is taking place.

4: Collecting your information

4.1 Any personal data collected in the course of our recording activities will be processed fairly and lawfully, in accordance with Data Protection Law. It will be:

4a. Adequate, relevant to the purpose and not excessive
4b. Used for the purposes stated in this procedure only
4c. Treated confidentially
4d. Stored securely
4e. Accessible only to relevant managers for the purposes stated in this procedure
4f. Not kept longer than 6 months
4g. Under the Payment Card Industry Data Security Standard (PCiDSS) we will not record any payment card information on our telephone recordings, by using a mid call solution.

5. Advising callers that calls are being recorded

5.1 On telephone lines where call recording is taking place, we will inform the caller that this is the case so that they have the opportunity to consent by continuing with the call or terminating the call.

5.2 Callers are advised that call recording is in operation via the telephone menu message and our website

6. Accessing call recordings

6.1 Recording will be located by the callers telephone number, the officer extension and the date and time of the call.

6.2 Customers and callers asking for the recordings of their calls will have to provide information about callers telephone number, date, time and extension called to enable the recording to be located.
6.3 If a customer or callers wishes to access call recording of their calls they must submit a subject access request (SAR) providing the information outlined in 6.2.
6.4 The SAR process will be followed to determine that the customer requesting the call recording is the customer within the call recording
6.5 A permanent copy of the recording will be provided by email as an audio file only.
6.6 To request a call recording submit a subject access request (SAR)
6.4 A customer can request that call recordings relating to them are deleted retrospectively, this will be carried out as long as the recording does not contain information that will help the Council in performing its duties or protecting its staff
6.5 If the Council needs to retain the recording/s the customer will be advised that this is the case and why the Council feels it is necessary to do so