Call Recording Policy

Person Responsible: Kieron Norris, Director
Last Reviewed: May 2019

General Principles

The Data Protection Act 1998 (the Act) protects personal information held by organisations on computer and relevant filing systems. It enforces a set of standards for the processing of such information. In general terms it provides that all data shall be used for specific purposes only, and not used or disclosed in any way incompatible with these purposes.

In the course of its activities Norris will collect, store and process personal data, including the recording of all telephone calls, and it recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

Call Record Overview

Purposes of call recording

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

- Help identify Norris' staff training needs;
- Help improve Norris' staff performance;
- Help protect Norris' staff from abusive or nuisance calls;
- Establish the facts in the event of a complaint either by a customer or a member of staff and so assist in resolving it;
- Assist in quality control to identify any issues in processes, with a view to improving them through one to one call feedback sessions and group call levelling sessions.
- Demonstrate that calls are accurately and efficiently transcribed onto the case management system or to other databases.

The telephone call recording system in operation will record incoming and outgoing telephone calls and recordings may be used to investigate compliance with Norris' Quality Standards, to provide further training, to support the investigation of complaints, to ensure that Norris complies with regulatory procedures.

Norris will record telephone conversations from its central telephone system. Norris currently does not record the content of any telephone conversations outside of this operating system, telephone conversations made to and from work provided mobile telephones, nor calls initiated as internal calls between extension users.

All calls that are recorded are encrypted via a 256-bit encryption method. Access to the call recording interface is also password protected.

Communicating the Call Recording System

Norris will make every reasonable effort to communicate that calls will be recorded. This will be done by:

- Publishing this policy on the company website; www.norris.co.uk
- General notification e-mail to all staff to inform that telephone calls will be recorded for training and monitoring purposes.
- Informing all clients in the first instance via a recorded announcement for Incoming calls, also on outbound calls where no automated announcement exists the advisor will read a script to advise the client, that all calls made to and from the business will be recorded for training and monitoring purposes.

What if the Customer doesn't want to be recorded?

- The customer will ask the Norris representative to stop the recording, or
- Email enquiries@norris.co.uk with your telephone number and name. We will then add this to our system and your calls will no longer be recorded.

What if the customer wants Norris to delete any historic call recordings relating to me?

Please email enquiries@norris.co.uk with your telephone number and name. We will then add this to our system and an email will be sent to you with a document detailing your call recordings and confirmation that they have been deleted.

Procedures to prevent the recording of sensitive data

The purpose of this section is to advise all staff at Norris of our position on taking credit card details from clients and how to keep those details safe & secure. It is our responsibility to protect credit card data.

Our credit card provider requires us to comply with their Payment Card Industry Data Security Standards (PCI DSS) compliance programme. The programme aims to ensure that all merchants accepting card payments do so securely. A data breach can make us liable for any fines incurred by

Card schemes in addition to the cost of remedying the breach plus any compensation payable.

Norris will make every reasonable effort to ensure (PCI DSS) compliance is upheld regarding the recording of such telephony stored data. Credit Card information should only be taken from the client either in person or over the phone. Card details should not be accepted by e-mail or other insecure messaging technologies. For compliance purposes the telephone recording system will provide for automated start/stop recording or muting of the conversation when completing certain fields within an application. In the event that payments are being received verbally over the telephone, all agents will be required to stop/start the telephone call recording mechanism to ensure that such data is not captured.

Procedures for managing and releasing call recordings

1. The recordings shall be stored securely, with access to the recordings controlled and managed by the Data Protection Officer or any other persons authorised to do so by the DPO.

2. Access to the recordings is only allowed to satisfy a clearly defined business need and reasons for requesting access must be formally authorised only by a relevant Partner / Head of Department. All requests for call recordings should include the following:

- The valid reason for the request.
- Date and time of the call if known.
- Telephone extension used to make/receive the call.
- External number involved if known.
- Where possible, the names of all parties to the telephone call.
- Any other information on the nature of the call.

3. The browsing of recordings for no valid reason is not permitted.

4. The Data Protection Act allows persons access to information that we hold about them. This includes recorded telephone calls. Therefore, the recordings will be stored in such a way to enable the Data Protection Officer to retrieve information relating to one or more individuals as easily as possible.

5. Requests for copies of telephone conversations made as Subject Access Requests under the Data Protection Act must be notified in writing to the Data Protection Officer immediately and, subject to assessment, he/she will request the call recording and arrange for the individual concerned to have access to hear the recording.

6. In the case of a request from an external body in connection with the detection or prevention of crime e.g. the Police, the request should be forwarded to the Data Protection Officer who will complete the request for a call recording.

7. Requests for copies of telephone conversations as part of staff disciplinary processes will only be released with the written agreement of the DPO, or any other person authorised by the DPO, who will consult with the Data Protection Officer before approval is granted.

8. Recordings of calls will be encrypted and stored electronically in a secure environment. Call recordings will periodically be archived, in line with electronic and paper file archiving time scales, to external hard drives.