Process for running the Division of Population Health shared voice recorder pool

Approved at IG Committee Meeting 2024-07-22

Background

The sharing of voice recorders between users comes with inherent information governance risks, and so is generally discouraged. However, in some cases it is pragmatic for certain devices to be loaned to people on a short-term basis.

A pool of shared voice recorders has been set up and is maintained by the Population Health Data Security team (DS).

Voice recorders can be used to store or access risk-bearing data, and there are associated information governance risks, so care must be taken to ensure that individuals understand their responsibilities, and that the management of the devices is undertaken in a way that reduces any potential IG risks. The loan term is kept short to keep the loan pool manageable and to reduce the risks. Where the same person repeatedly requires access to a device, or requires a long-term loan, consideration should be given to purchasing a device specifically for that person.

Purpose

To outline a process describing how DS can manage the device pool to allow voice recorders to be shared between individuals in a way which minimises and mitigates any IG risks.

Scope

Within the Division of Population Health, the shared pool of voice recorders should be managed in line with the procedure outlined below.

Procedure

The following steps should be taken:

1. Allocate individuals to be responsible for checking in and out devices
2. Document devices included in pool (see ‘Maintaining a device list’ section)
3. Appropriately set up devices to be loaned out (see ‘Setting up devices for loan’ section)
4. Include terms of use (privacy policy, etc.) and guidance (e.g. a “dos and don’ts” checklist) with each device
5. Establish a system to log:
    - Which device
    - Person to whom it was loaned
    - When it was loaned
    - When it was due to be returned

    - When it was returned
6. Log any potential incidents with the IG committee

Maintaining a device list

Any devices to be included within the pool should be assigned an identifying name and logged (e.g. in a spreadsheet).

Setting up devices for loan

- Devices must be reformatted
- Devices must be encrypted with a new encryption key
- Devices must be protected with a new PIN

Suggested guidance to include with loaned-out devices

The same basic principles apply as for any device used for data storage:

1. look after the device:
    a. take care not to lose it or leave it unattended when in public
    b. ensure that it is suitably secured (e.g. behind a locked door) when you do not have it with you
2. use only for the agreed, specific, work-related reasons
3. erase all recordings before returning the device
4. return the device by the agreed date

Eligibility for loans

Devices may be loaned to:

- Division of Population Health staff
    - Name and username required
- Division of Population Health students
    - Division of Population Health Supervisor must take responsibility, and make the request on the student's behalf
    - Supervisor's name and username required
    - Student's name and username required

This information must be provided in writing to ensure proof of responsibility
User must have an up-to-date Information Security training record

Loan Terms

The maximum loan term is one month.
An extension to the loan term can be requested in writing shortly before the current loan term expires. An extension is not guaranteed and is subject to availability.

Loan Process

User (Staff)	Contacts DS to request a loan Provides contact details Specifies required loan period (up to 1 month)
User (Student)	Contacts Division of Population Health Supervisor Supervisor contacts DS to request a loan Provides contact details for self and student Specifies required loan period (up to 1 month)
DS	Reserves a 'READY' device Records user details against device log Sends loan information and Hardware Acceptance Statement (see Appendix) Specify return date Specify that collection of device indicates acceptance DO NOT send PIN and encryption key at this stage
User	Collects device
DS	Records the device as 'ON LOAN' Sends PIN and encryption key via email
DS	1 week before return date, contact user to remind them of the following: ● the loan period is about to end ● the device must be returned to reception on or before the agreed date ● the user is responsible for downloading any files they wish to keep from the device before it is returned
User	Securely downloads any files from the device that need to be kept and erases the device Returns the device to reception
DS	Records and labels the device as 'USED' Stores the device securely Sends email confirmation that the device has been returned
DS	Processes the 'USED' device to make it secure and ready to be loaned out again

Processing a 'USED' device

Before a device can be considered 'READY' to loan out, it must be processed as follows:

- The device must be formatted (ensuring all recordings are erased from the device)
- The PIN must be changed
- The encryption key must be changed

Appendix

Hardware Acceptance Statement

You have been provided with a voice recorder on a loan basis for use at the University. You have been logged as responsible for the device. You are required to read and abide by the following policies, codes of practice and undertake mandatory information security training:

- Division of Population Health Information Governance Policy
- University IT Code of Practice
- University GDPR and Data Protection Policies

You are responsible for the voice recorder, and for any devices you use in connection with the voice recorder. You must ensure that your account and any devices you are responsible for are secure. You must abide by the University's Code of Practice at all times. This protects you, your devices and other users of the University network. For information on securing your devices please visit our advice on safe computing. https://staff.sheffield.ac.uk/it-services/information-security

If you have any queries regarding this device please contact Population Health Data Security (DS):

Email: population-health-ds@sheffield.ac.uk

As a condition of the loan, you are required to read the following and abide by the terms set out below:

Encryption & PIN code

The voice recorder has been encrypted and configured with a 4-digit PIN. You will need the PIN to operate the device, and the encryption key to access your recorded files. Do not change or disable the PIN or the encryption key, or share them with anybody else.

If you think that somebody else may know the PIN or encryption key, please return the device to DS immediately.

Safekeeping

Please look after the device that has been assigned to you. We recommend that when you are not actively using it, the device should be stored securely (for example, in a locked drawer).

Loss of hardware

If you lose the recorder, it is imperative that you inform DS immediately. Furthermore, if you believe the recorder has been stolen, you are also expected to report the theft to the police. They will issue you with a crime reference number (CRN) which needs to be provided to DS.

Faults and Damage

The device has been inspected before deployment. If the device is damaged or if you suspect that the device may be faulty, please contact DS as soon as possible.

End of Loan Period

Do not pass the device on to another user. At the end of your loan period, please return the device to ScHARR Reception, who will return the device to DS. DS will update the asset register and send you confirmation by email. Please retain the confirmation as proof that you have returned the device and are no longer responsible for it.

The device will be cleared and all codes changed before redeployment.

Leaving the University

If you are to leave the University before the end of your loan period, the loan device will need to be returned to DS before you leave. There are no exceptions to this rule.

Version	Effective Date	Summary of changes
1	22nd July 2024	n/a first version