Internal Data-sharing Protocol – One-off Request

**Introduction and Scope**

This protocol provides the basis for making a one-off request for personal data held by another Edinburgh Napier University team/school/department and sets out the requirements that must be met. A legal basis for processing must be established and all potential risks must be identified and mitigated. This protocol should be read alongside the University’s [Data Protection Code of Practice (Section 8)](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/CodeofPractice/Pages/DataSharing01.aspx) and [Data Protection Policy](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/default.aspx).

**1. Data being requested:**

Click or tap here to enter text.

**2. Data held by:**

Click or tap here to enter text.

**3. What purpose will the data be used for?**

Describe the specific purpose the data will be used for, including what will be achieved and the benefits. The purpose should be clearly defined and should explain why it can only be achieved using personal data, consideration should be given as to whether the same outcome could be achieved using anonymised data. The data must only be used for the purpose set out below, re-use is not allowed without the submission and agreement of a new Data-sharing Protocol. If you intend to use the data for e-marketing please read the guidance [here](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/PECR.aspx) and contact the University’s [Information Governance Manager](https://staff.napier.ac.uk/services/governance-compliance/Pages/who.aspx) to discuss

Click or tap here to enter text.

**4. What is the legal basis for processing this personal data?**

A legal basis for processing must be identified, please read the guidance [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/) and select from the dropdown list below. Please contact the Information Governance Manager if you require guidance on which legal basis to choose.

Choose an item.

**5. How many times do you intend to use the data?**

There is a high risk when re-using data without first confirming its accuracy, especially data used for e-marketing as the user may have unsubscribed since the data was shared. If using the data more than once the accuracy must first be confirmed with the original holder.

Click or tap here to enter text.

**6. Have you completed a Privacy Impact Assessment (PIA) for the processing of this personal data?**

**Yes**

**No**

If you haven’t please contact Governance Services who will assist you to complete one, further guidance can be found [here](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/PrivacyImpactAssessments.aspx). Once you have completed the PIA a copy should be submitted with the protocol.

**7. What measures do you have in place to avoid a data breach?**

Based on your PIA please describe the organisational and technical measures you have in place to mitigate any risk of accidental loss or destruction, unauthorised access or disclosure etc. (Examples of measures: secure storage, signed oaths of confidentiality, staff training). Guidance on security of personal data can be found [here](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/CodeofPractice/Pages/SecurityofPersonalData01.aspx). If a breach occurs, you must notify [Governance Services](https://staff.napier.ac.uk/services/governance-compliance/Pages/who.aspx) as soon as the breach has been identified providing them will all details of the breach and how it occurred.

Click or tap here to enter text.

**8. Do you have a privacy notice in place?**

**Yes**

**No**

A Privacy Notice (PN) must be created which clearly sets out how the individual’s data will be used. If you do not have a Privacy Notice in place please contact Governance Services. The completed PN should be submitted with the protocol.

**9. How long will the data be held? (Retention period)**

Personal data must be kept for only the minimum time required, once the agreed retention period has been reached the data must be confidentially destroyed. The destruction should be recorded and the holder of the original data (i.e. the team who have shared the data with you) must be notified. Enter the retention period below and the destruction process you will use at the end of the retention period, including who will be responsible for carrying this out.

Click or tap here to enter text.

**10. How will the data be transferred and who will be responsible for receiving the data?**

The data must be transferred securely, it must not be passed on via email or USB drive, please discuss with IS and Governance Services if guidance is required.

Click or tap here to enter text.

**11. Where will the data be stored?**

The data must be stored securely on the S:Drive or an appropriate SharePoint and access should be restricted to appropriate staff only (see Question 12). Please read the guidance on [securing personal data.](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/CodeofPractice/Pages/SecurityofPersonalData01.aspx)

Click or tap here to enter text.

**12. Who will require access to the data?**

Please list below the staff who will be accessing the data. All staff must have previously completed [Data Protection training](https://staff.napier.ac.uk/services/governance-compliance/governance/Pages/IGTraining.aspx).

Click or tap here to enter text.

**Once the protocol has been completed and agreed, sign off must be given below by a senior manager in each area.**

Requester

Name: Job Title: School/Dept: Signature:

Data Holder

Name: Job Title: School/Dept: Signature: