



Version 5, January 2018

Individual data sharing agreement

1. Introduction

This agreement sets out the basis on which the University of Cambridge shares alumni and supporter personal data with individuals in accordance with our data protection notice for alumni and supporters (alumni.cam.ac.uk/data-protection).

Personal data broadly means **any** information about an identifiable living individual (not just contact details).

All personal data is confidential wherever it is stored and whether on paper or held electronically. This applies to all records, not just formal records but also 'private' notes.

2. Details

Categories of alumni and supporter personal data shared	Name, contact information and details of their online donation.
Purposes for which personal data is shared	To enable thanking of donors only.
Duration for processing of shared personal data	Data to be deleted immediately after the donor has been thanked.

I agree to comply with the requirements set out below.

Signed: 

Name: Harry Anderson-Endean

Company or organisation where applicable:

Date: 18.08.26



3. Undertakings

I will use the shared personal data only for the purposes set out above.

I will treat the shared personal data as confidential and not share the personal data with any other person or party.

I will immediately notify Development and Alumni Relations of any loss or disclosure of the shared personal data, and cooperate with any required notification to the regulator or the data subjects.

I will cooperate as necessary with any request from Development and Alumni Relations in relation to the shared personal data with regard to the exercise of statutory data protection rights or the fulfilment of statutory data protection accountability requirements (such as audits or impact assessments).

I will delete all copies of the shared personal data on completion of the processing as set out above.

I will keep the shared personal data secure by complying with the section below *Putting data protection principles into practice*.

I will let Development and Alumni Relations know if I have any concerns about any aspect of how the shared personal data is used.

4. Putting data protection principles into practice

- Do not store personal data on portable storage (such as USB sticks) unless it is encrypted.
- Do not send personal data by email unless it is encrypted.
- Hard copy personal data must not be left unattended and must be disposed of securely.
- Always keep passwords secure and do not share them.
- Always lock PCs and laptops while unattended.
- Do not visit unsafe websites from any PC or laptop where you store personal data (you can check potentially unsafe sites at <https://global.sitesafety.trendmicro.com/>).
- Do not upload personal data into cloud services (including OneDrive and Dropbox) even if encrypted.
- Do not open email attachments from an unknown source on any PC or laptop where you store personal data.
- Enable automatic security updates on any device where you store personal data.
- Enable firewalls and run antivirus software on any Windows PC or laptop where you store personal data.
- Enable password protection and inactivity timeout on PCs and laptops where you store personal data.
- Do not share your PC or laptop account with other people.
- Reset your PC or laptop to factory settings before disposing, selling or passing to another person.
- Do not take a laptop on which you store personal data to Russia or China, because of the high likelihood of cyber-attack.