SAFEPOD NETWORK

SECURE DATA ACCESS

SafePod Network Privacy Notice

Version control

Updates to this document will be summarised in the table below.

Version No.	Date	Section	Update
1.	23.02.21	Throughout document	Updated document with information about unsuccessful registrations.
1.3	29.04.21	3.6 and 3.7	Amendment to third party provider and retention periods.
1.4	31.05.21	Throughout document	Minor text updates and amendments.
1.5	01.06.21	Throughout document	Minor text updates and amendments.
1.6	03.06.21	Throughout document	Minor text updates and amendments.
1.7	16.07.21	Throughout document	Added information about SPN enquiries.
1.8	02.08.21	3.11	Statement on use of Processors added.
2.0	30.08.21	Throughout document	Minor amendments for the University as a Controller of CCTV footage and use of behaviour recognition software with CCTV.
2.1	09.11.21	Throughout document	Minor amendments
2.2	19.03.24	Throughout document	Minor amendments

Authors

Christopher Milne, Head of Information Assurance and Governance and University Data Protection Officer, Office of the Principal, University of St Andrews.

Darren Lightfoot, SPN Manager, University of St Andrews.

Contents

1. Definitions

- **Advisory Board:** a group of representatives from Swansea University, the University of Edinburgh, University of Essex, and the University of St Andrews, who are responsible for the long term objectives of the SafePod Network.
- **Data Centre:** an organisation which has agreed to provide access to their data from a SafePod.
- **SafePod:** SPN prefabricated safe setting that provides the physical security and necessary controls for secure access to data.
- **SafePod Network (SPN)**: the service which provides an independent UK network of standardised safe settings for use by researchers, SafePod Organisations and Data Centres.
- **SafePod Network Organisation**: an organisation that has purchased and installed a SafePod or SafePoint.
- **SafePoint:** SPN standardised room that provides the physical security and necessary controls for secure access to data.
- **SPN Services:** the services provided by the SafePod Network for secure access to data (e.g. SafePod or SafePoint)
- **SPN User:** a person that uses a SafePod, SafePoint and other SPN services, this is typically either a researcher or a person supporting a researcher.
- **SPN User registration**: the information that must be supplied by a person together with acceptance of the terms to become a member of the SPN.
- **SPN services**: services provided by the SPN to assist with and enable access to data for research.
- **University:** The University Court of the University of St Andrews having its registered office at College Gate, North Street, St Andrews KY16 9AJ. Registered Charity Number SCO13532.

2. Document application

This document provides information on how personal data are used throughout the SafePod Network. This document will be updated as and when required.

Contact the SPN for further information on this document.

3. SPN Privacy Notice

3.1. How the University will make use of personal data

The University operates and manages the SPN, which has been set up to provide SPN Services (such as SafePoint and SafePod) to enable researchers to access data provided by Data Centres for research purposes in the UK.

As part of providing these SPN services, the SPN will collect and use personal data from individuals that use these services, and from individuals at organisations that support the SPN. Members of the public can also sign up to receive SPN news and events items.

SPN Users

The University will collect personal details to:

- Register a person as a SPN User.
- Manage the SPN User registration process.
- Maintain records of successful and unsuccessful applications for registration as a SPN User.
- Manage SPN Service bookings.
- Manage other SPN Services provided to SPN Users.
- Understand whether the terms and conditions of data access and SPN Service use were upheld.
- Provide key aggregated and anonymised statistics about the SPN to funders and other stakeholders.
- Provide individuals with data protection rights for personal data for which the University is responsible for as a Controller.

The University will also collect personal data via CCTV footage i.e. recordings (video only) of individuals when using a SPN Service. The CCTV facilities within a SPN Service always record.

Data Centre and Organisation personnel

The University will collect personal details from Data Centres and SafePod Network Organisation personnel for SPN Services to be provided to SPN Users. For example, for the notification, cancellation and management of SPN Service bookings.

If so wished, Data Centre and SafePod Network Organisation employees and contractors can provide the University with their consent for their contact details to be used to advise about SPN news and events. Consent can be withdrawn at any time.

Contractors

The University will collect personal details from contractors for SPN registration purposes. Contractors must agree to the SPN terms and conditions before any required work can be carried out for the SPN.

If so wished, contractors can provide the University with their consent, for their contact details to be used to advise about SPN news and events. Consent can be withdrawn at any time.

Members of the public

The University will collect personal details from members of the public to provide information to them about SPN news and events. Consent can be withdrawn at any time.

Individuals may make enquires of the SPN. Personal details received will be used to respond to those enquiries.

3.2. How Data Centres will make use of personal data

Data Centres that join the SPN will collect and use personal data when:

- Working with a SPN User, when agreeing how access to data is to be provided.
- Approving SPN Service bookings.
- They require a SPN Service booked session to be recorded by CCTV.
- They require to understand whether a SPN User has or has not met the terms of their data access agreement.
- Providing individuals with data protection rights for personal data for which the Data Centre is responsible for as a Controller.

Data Centres can also access CCTV footage from the SPN, where they require that a SPN Service booked session is recorded.

For all the above reasons the associated Data Centre is the Controller. They will need to provide a relevant privacy notice and data protection rights to individuals.

3.3. The identity and the contact details of the University data controller

University of St Andrews, College Gate, North Street, St Andrews, KY16 9AJ, Fife, Scotland, UK. The University is a charity registered in Scotland, No SC013532.

3.4. The contact details of the University Data Protection Officer

Mr Christopher Milne, Head of Information Assurance and Governance, University of St Andrews, Email dataprot@st-andrews.ac.uk.

3.5. The purposes for which the University will make use of personal data

Administration for a SPN User

Personal data is primarily used by the University to set-up and administer a SPN User's registration and for the management of SPN Service bookings and other services provided by the SPN. This information will be shared between Data Centres and SafePod Network Organisations as needed, which will involve creating a unique user record. The personal data collected will include name, email address, telephone number, affiliated organisation and booking details.

The use of a SPN Services is subject to the terms and conditions agreed between the University and the individual and the relevant Data Centre and the individual.

Understanding whether a user has met terms and conditions

CCTV footage of a SPN Service booked session or other services provided by the SPN may be used by the University to help determine whether the terms of the SPN User Agreement have been upheld.

From September 2022, behaviour recognition software will be added to CCTV cameras across the SPN. This software identifies where an SPN User's behaviour may be inconsistent with data access conditions or SPN Service use e.g., if an individual has taken a mobile phone into a SafePod, then the software may detect this and create an alert for footage of a session to be reviewed.

Where an alert is created, the SPN will arrange for the footage to be reviewed against the data access conditions and SPN Service use. A Data Centre will be advised of any suspected security incidents relating to their data access conditions.

A list of all SPN Services equipped with behaviour recognition software is available from: www.safepodnetwork.ac.uk/behaviour-recognition.

If there are reasonable grounds to suspect that an individual has not upheld the agreed terms and conditions with a Data Centre or the University, their personal data which may include CCTV footage may be used by either of the parties to understand if the said terms and conditions have been met or otherwise.

If a breach of SPN User Agreement has been established, details of that may be shared with relevant parties. The parties with whom details may be shared are set out in the SPN User Agreement.

Where an application for registration as a SPN User was not successful, records of that application will be maintained and may be cross referenced against future applications.

Personal data may also be anonymised and aggregated for the provision of statistics about the SPN to funders and other stakeholders.

Personal data will also be shared with the Advisory Board when priority access to a SPN Service is requested, and those applications need to be considered and a decision made.

Administration for Data Centre and SafePod Network Organisation personnel

Personal details for Data Centre and SafePod Network Organisation personnel will be used to:

- Enable SPN Services bookings to be confirmed or declined.
- Administer other SPN Services where appropriate.
- Management of security incidents.

This will involve creating a unique user record with the SPN. The personal data collected will include name, email address and affiliated organisation.

These details will be provided by the University and will be made available to SPN Users, Data Centres, SafePod Network Organisations for those purposes as relevant. A Data Centre or SafePod Network Organisation may use a SPN User's contact details to also advise of changes to booking arrangements or other SPN services where appropriate.

Personal data may also be anonymised and aggregated for the provision of statistics about the SPN to funders and other stakeholders.

Administration for contractors
Personal details for contractors will be used by the University to set-up and administer their SPN registration to repair or maintain a SPN Service. This will involve creating a unique user record. The personal data collected will include name, email address, and affiliated organisation.

SPN news and events
Any person can consent for their contact details to be used by the University to advise about SPN news, events and other SPN materials. Consent can be withdrawn at any time by replying to a SPN email with the subject line 'Opt out of SPN updates' or by contacting safepodnetwork@st-andrews.ac.uk.

Improving SPN services
If a person provides the SPN with feedback about the SPN, then the University may use that information to improve SPN services.

3.6. The lawful bases for processing personal data

For setting up an individual's registration with the SPN and the management of SPN Service bookings between SPN Users, Data Centres and SafePod Network Organisations, the lawful basis for processing personal data is contract.

Where the University needs to establish if a SPN User has or has not upheld the terms of the SPN User Agreement then personal data, including CCTV footage may be used. The lawful basis being contract.

For providing information about the SPN News and events, the lawful basis is consent.

In other instances, notably where an employee of a SafePod Network Organisation or a contractor is recorded on CCTV when entering a SPN Service, the lawful basis for capturing those personal data is legitimate interests. For the avoidance of doubt, the University is the Controller of those personal data.

3.7. CCTV and personal data

The University uses third party suppliers to provide CCTV services and a managed booking system via the SPN website. The University of St Andrews has contracts with those providers, which establishes the roles and responsibilities for the protection and use of personal data, which meets the requirements of data protection law.

The University will make use of SPN User Registration details and CCTV footage to assess whether an individual has or has not upheld their SPN User Agreement. Where a breach of the SPN User Agreement has been established, the associated personal data may be shared with the parties listed in the SPN User Agreement.

The University may transfer SPN User registration details, CCTV footage and other personal data held to a Data Centre, where it is necessary to establish if a SPN User has or has not upheld their data

agreement with them. CCTV footage may also be transferred to other organisations where there is a lawful basis to do so.

3.8. The period for which personal data will be stored, or if that is not possible, the criteria used to determine that period

Registration records

For SPN Users, the University will retain personal details and the SPN booking data for a period of 6 years after the last booking for a SPN Service, after which time records will be destroyed.

For Data Centre and SafePod Network Organisation personnel, registrations will be reviewed on an annual basis and destroyed if no longer active.

For contractors, registrations will be reviewed on an annual basis and destroyed after three years where the contractor has not completed any SPN repair or maintenance work.

For members of the public, registrations will be destroyed upon request or if the SPN is no longer operational, whatever is the earliest.

Records of an unsuccessful application for registration as a SPN User, SafePod Network Organisation personnel, Data Centre personnel or contractor will be retained for 3 years, before being destroyed.

CCTV footage

CCTV footage will normally be held for 30 days before being deleted. However, where footage is exported by the University to understand if a user has breached the SPN User Agreement or at the request of a Data Centre to review suspected misuse of a SPN Service, then this will be held for longer.

Enquiries

Details of any enquiries received to the SPN will be destroyed at the end of the University's financial year following the year in which those enquiries were received.

3.9. Rights available to individuals

UK data protection laws provides individuals with rights regarding the management of their personal data. In relation to the SPN, the rights are:

The right of access to personal data, commonly referred to as a subject access request, which involves the following being carried out within a calendar month:

- Confirmation that personal data is being processed.
- Access being given to a person's personal data (provision of a copy), unless an exemption(s) applies.
- The provision of supplementary information e.g. an explanation of how personal data is processed and who this is shared with.

The right to rectification, which may involve:

- The University working to correct any inaccuracies in personal data or to address any omissions, which may require personal data to be annotated to acknowledge that this is incomplete.

The right to data portability, which may involve:

- The University providing a copy of elements of personal data that exist in machine readable form that have been given to the University.

These rights must be met by the University and any other organisation that takes decisions about how or why your personal data is used. Details on how to access those rights are available from the University website, or you can contact dataprot@st-andrews.ac.uk.

If the University receives a request from an individual for a data protection right and the University is not the Controller i.e. not responsible for providing that right, the request will be passed to the appropriate organisation, within 2 working days.

3.10. The right to lodge a complaint with a supervisory authority

If you believe that the University has not made use of your personal data, in line with the requirements of the law, you have the right to raise this with the regulator i.e., the UK Information Commissioner Office's ("the ICO"). However, you must raise the matter with the University first.

Details on how to contact the ICO are available online from their website.

3.11. Contractual requirement to provide personal data and the consequence where no personal data are provided for SPN users

In order for the SPN to provide services to an individual (mainly for SPN Service bookings), SPN Users must provide their contact details for registration purposes, to process bookings and for the management of other SPN Services that maybe used. Without an individual providing these personal details, then SPN Services cannot be provided to them.

3.12. Who we may share personal data with

Personal data are shared with third party Processors who provide services to the SPN under contract for CCTV, booking and email services. Details of the providers of those services are available on request.

3.13. Revision of the Privacy Notice

This Privacy Notice will be reviewed at regular intervals. The review period will be approved by the University and recorded in the version control section of this document. Any significant change to relevant legislation, University policy or procedures primarily concerned with the protection of personal data may trigger an earlier review.

3.14. Availability

This Privacy Notice will be published on the SPN website.

Should a copy of this Privacy Notice be required in another form (including audio) please contact safepodnetwork@st-andrews.ac.uk.

4. Contact information

Darren Lightfoot
SafePod Network
University of St Andrews
91 North Street
St Andrews
KY16 9AJ

Web: safepodnetwork.ac.uk
Telephone: 01334 463901
Email: safepodnetwork@st-andrews.ac.uk

SAFEPOD NETWORK

SECURE DATA ACCESS