SafePod Network

SAFEPOD®

SECURE DATA ACCESS

SPN General Overview

Version control

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

Version No.	Date	Section	Update
1.3	09/06/20	Throughout document	Minor updates
1.4	22/08/21	Throughout document	Minor updates
1.5	30/08/21	3.4	Added section

Author

Darren Lightfoot, University of St Andrews.

Contents

1. Document application

This document provides a general overview of the SafePod Network (SPN).

This document will be updated as and when required. Contact the SPN for further information on this document.

2. Definitions

- **Booked Session:** a continuous time period in a single day where a SafePod has been booked and in use by a researcher.
- **Dataset:** a collection of data provided by a Data Centre for research use.
- **Data Centre:** an organisation which has agreed to provide access to their datasets from a SafePod.
- **Data Centre thin client:** a thin client that can be provided by a Data Centre for remote access to their datasets from a SafePod.
- **Emergency alarm:** an alarm within a SafePod that can be used by a SafePod User to request attention from the emergency alarm staff.
- **Remote dataset access:** the connection between a SafePod and a Data Centre which provides a researcher with access to a Data Centre's datasets.
- **Researcher:** a person that analyses datasets for research purposes using a SafePod.
- **Researcher Area:** the area inside of a SafePod where a researcher works. Contains the desk, monitor, whiteboard, keyboard, mouse and CCTV system.
- **SafePod:** The SPN prefabricated safe setting that provides the physical security and necessary equipment for access to datasets.
- **SafePod Coordinator:** a full time member of staff(s) at a SafePod Organisation that is responsible for the operational management of a SafePod in line with SPN policies.
- **SafePod Coordinator Manual:** the document that outlines the duties and procedures to be followed by a SafePod Coordinator for management of a SafePod booked session.
- **SafePod Network (SPN):** the service run by the University of St Andrews which provides an independent UK network of standardised safe settings for use by researchers and Data Centres.
- **SafePod Organisation:** an organisation that has purchased and installed a SafePod.
- **SafePod thin client:** the thin client within a SafePod which provides the configuration for remotely accessing datasets from Data Centres.
- **SafePod User:** a person that uses a SafePod, either a researcher or a person supporting a researcher to use a SafePod.
- **SafePod User Agreement:** the document that provides the policy and terms for SafePod use.
- **Secure Service Area:** the locked area of a SafePod containing the service equipment, the secure storage locker and cupboards A and B and C.
- **SPN Dataset Access Service:** the SPN webpage that provides the links to connect to a Data Centre web page for a researcher to access their project datasets.
- **SPN Policy and Terms for SafePod Ownership:** the document which provides the policy and terms for ownership and management of a SafePod.
- **SPN User Support Service:** the central service provided by the University of St Andrews to assist researchers, Data Centres, SafePod Organisations and other stakeholders with enquiries relating to the SPN.

End of definitions

3. About the SafePod Network

3.1. Introduction

The SafePod Network (SPN) is a major new research innovation to provide and manage a network of standardised safe settings (SafePods) across the UK for data that requires secure access for research.

For a researcher, the major benefit of the SPN is local secure access to their research datasets. This reduces the cost and need for travel to the existing limited and fragmented safe settings in the UK. Consequently applications for access, and use of datasets for vital public benefit research should be improved by the SPN.

For a Data Centre, the SPN provides a low cost and secure platform to widen access to their research datasets. Every SafePod is built to the same specification and the SPN policies and procedures for their management are standardised. Therefore, a single accreditation of a SafePod by a Data Centre is all that is required to accredit every SafePod in the network.

Unlike a traditional safe setting, a SafePod can support secure access to datasets from many Data Centres. The convenience and widening of access to datasets that the SPN provides is also likely to encourage more applications to Data Centres for public benefit research.

The SafePod Network is managed by the Scottish Centre for Administrative Data Research and both are part of Administrative Data Research UK. The SPN is funded by the Economic and Social Research Council, which is part of UK Research and Innovation.

3.2. SPN composition

The SPN comprises of:

- A network of SafePods based within higher education institutions and other eligible organisations across the UK;
- A website to provide information about the SPN and book SafePods;
- Policies, procedures and assurances for the operation and management of SafePods;
- An IT system to provide secure access to datasets;
- A CCTV service to enable Data Centres to view and monitor activity within a SafePod;
- A dedicated User Support Service to assist stakeholders with SPN enquiries; and
- An Advisory Board to plan and make decisions on the long term objectives of SPN.

3.3. Major benefits of SPN

Some of the major benefits of the SPN and SafePods are as follows:

- A SafePod provides the opportunity, flexibility and convenience for a researcher to remotely access datasets from their local institution or organisation;
- Unlike existing safe settings, a SafePod can support access to datasets from multiple Data Centres;
- A SafePod replicates traditional safe setting requirements without the need and costs for an organisation to set up a dedicated room as a safe setting;
- A SafePod provides a pleasant working environment for a researcher with strong environmental cues to encourage safe behaviour;

- Once set up, a SafePod requires minimum management by a SafePod Organisation;
- The design and space of SafePods are identical, consistent and operate under the same standard SPN procedures and assurances. This will provide Data Centres with a platform and low cost opportunity to extend access to their datasets across the UK through the SPN
- All the above benefits will help encourage the greater use of datasets for public benefit research; and
- SafePods can also potentially be used by a SafePod Organisation for other internal confidential / sensitive work. See section 5 for more information.

3.4. SPN principles

There are four main SPN principles that underpin secure access to data for research from a SafePod. These are:

- **Safe researcher:** A researcher must abide by the SPN User Agreement and pass a training questionnaire before they can book and use SafePods.
- **Safe access:** A local SafePod Coordinator manages their SafePod in line with SPN procedures. SafePod Coordinators are background checked and must pass a training questionnaire.
- **Safe data:** A hardened IT system stored securely in a SafePod provides connection over a VPN for a researcher to remotely access their project datasets from a SafePod.
- **Safe analysis:** A SafePod provides a dedicated area for a researcher to analyse and work on their project datasets. The area is door access controlled and contains a CCTV system.

4. About a SafePod

4.1. Introduction

A SafePod is a small prefabricated safe setting that can provide access to sensitive or confidential datasets for research purposes from Data Centres across the UK.

A SafePod measures approximately 2.66m(w) x 3.33m (d) x 2.35m(h) and has been designed for use for a single SafePod User only. Note it is possible for an additional SafePod User to use a SafePod at the same time, but this would be subject to a Data Centre's approval.

A SafePod includes:

- Height adjustable desk;
- Air ventilation system;
- Adjustable lighting;
- Monitor information protection
- CCTV system;
- Emergency alarm;
- Chair, monitor, keyboard, mouse and whiteboard;
- Connections for fire alarm;
- Door access control system;
- Secure IT storage cupboard; and
- Locker storage for SafePod User possessions.

A SafePod has been designed with accessibility in mind, including wheelchair access.

4.2. SafePod Design

A SafePod is split into two separate secure areas as follows:

Researcher Area

This area is where a researcher can view and work on their project datasets. It contains the desk, CCTV camera, monitor, keyboard, mouse and whiteboard and controls for the lighting and emergency alarm.

Secure Service Area

This area contains the equipment for SafePod services (such as the door access control and CCTV system) and IT systems. Only a SafePod Coordinator is allowed access to this area.

4.3. SafePod finishes

A SafePod is available in a choice of two finishes – Classic (brown) and Contemporary (grey).

4.4. SafePod pictures

Figure 1: SafePod exterior view (Classic)

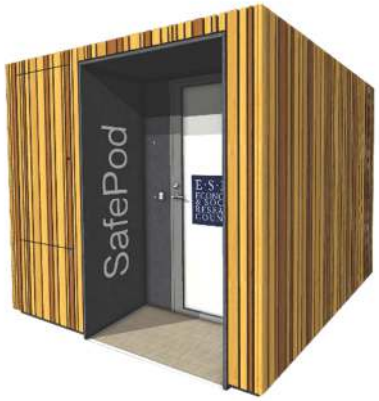


Figure 2: SafePod exterior view (Contemporary)

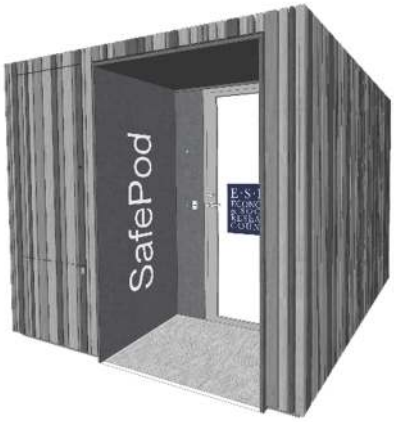
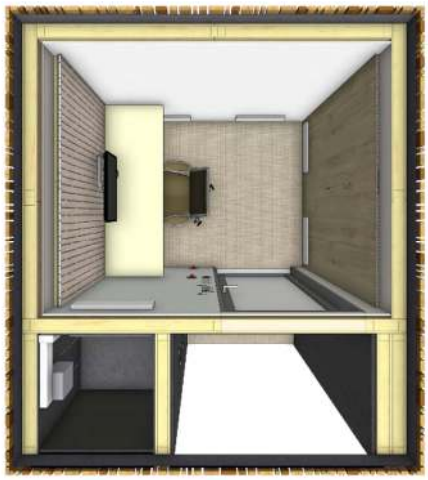


Figure 3: Top down view of a SafePod



4.5. SafePod manufacture

SafePods are manufactured to the highest quality standards. The SafePod manufacturer has been awarded the Manufacturing Guild Mark.

5. SafePod uses

A SafePod can be used for the following purposes:

- By a researcher to access their project datasets from SPN approved Data Centres; and
- By members of staff or researchers based at a SafePod Organisation for confidential research projects subject to the SPN approval. Projects are likely to be approved that are for public benefit and / or health and social science related and where the use of a SafePod does not compromise the primary purpose outlined in point 1 above.

Contact the SPN User Support Service for more information about authorised uses for a SafePod.

6. Joining the SafePod Network

This section details the procedures for researchers, SafePod Organisations and Data Centres to join the SPN.

6.1. Researchers

A researcher that wishes to join the SafePod Network and use a SafePod must first register via the SPN website. The SPN User Agreement which sets out the terms for SafePod use will need to be accepted and the SPN Training Questionnaire completed before a SafePod can be booked and used.

6.2. SafePod Organisations

An organisation that wishes to own a SafePod and be part of the SPN must contact the SPN for further information about application procedures. An organisation must agree to any terms issued for the purchase or funding of a SafePod as well as the SafePod Policy for Ownership. The application will be reviewed by the SPN Advisory Board.

6.3. Data Centres

A Data Centre that wishes to provide access to their datasets through the SPN must contact the SPN to request an application form. The SPN Data Centre Agreement sets out the terms for joining the SPN. The application will be reviewed by the SPN Advisory Board.

7. Dataset access from a SafePod

The SPN does not hold datasets but instead provides SafePods to facilitate secure access to a Data Centre's datasets. Connectivity options for dataset access are detailed below.

7.1. Remote dataset access: SPN Dataset Access Service

This service will facilitate secure remote access to a Data Centre's web portal from a SafePod using a VPN connection. A researcher will choose which Data Centre to connect to from a menu and then login to a Data Centre's web portal to access their project datasets.

7.2. Remote dataset access: Data Centre thin client

A Data Centre can provide their own thin client for use in a SafePod. The thin client will be installed by a SafePod Coordinator prior to a researcher arriving for their session. A Data Centre is responsible for ensuring a secure network connection between a SafePod and a Data Centre.

7.3. Local dataset access: Data Centre PC or hard drive

In cases where options 7.1 and 7.2 are not achievable, a Data Centre can consider providing datasets held on an encrypted PC or other suitable hard drive directly to a SafePod for secure storage and access.

7.4. Approval for dataset access from a SafePod

Access to datasets from a SafePod is approved by the relevant Data Centres. A researcher must have a project approval in place with a Data Centre before a SafePod can be booked and used.

7.5. Participating Data Centres

From launch, the SPN will support remote dataset access from:

- UK Data Service;
- SAIL Databank; and
- Office for National Statistics.

The SPN will also work closely with other key social science Data Centres and government departments to provide access to their research datasets over time.

8. Overview of how a SafePod would be booked and used by a researcher

A university has installed a SafePod in their library. A researcher has an agreement with Data Centre that allows them to remotely access their project datasets from a SafePod.

A Data Centre would typically have a secure encrypted remote access system in place which accepts connections from a SafePod. Citrix and VMWare View are the two most used secure access systems.

A researcher must register with the SPN and pass a training questionnaire. This is a one-time process achieved through the SPN website and a researcher can then make a SafePod booking. A Data Centre confirms the booking and booking details are sent to a SafePod Coordinator, Researcher and Data Centre.

On the day of the booking, a SafePod Coordinator carries out security checks on their SafePod.

A researcher arrives at the university at the designated date and time and provides photographic identification (passport or driving licence only) to a SafePod Coordinator, who then verifies a researcher's identity and issues them with a swipe card which opens a SafePod. The researcher deposits their personal possessions in the SafePod locker and can then enter the SafePod.

A researcher then sits at the desk, chooses their Data Centre from the SPN Dataset Access Service menu and logs in using the credentials supplied by a Data Centre.

At the end of the session, a researcher logs off from the system and returns the swipe card to a SafePod Coordinator.

A SafePod Coordinator completes end of session procedures with a researcher and carries out security checks on a SafePod.

9. SafePod website and bookings

The SafePod website is at www.safepodnetwork.ac.uk. The primary purpose for the website is to facilitate SafePod bookings. The website also provides information about the SPN, SafePod locations and the SPN policies and procedures.

9.1. SafePod booking process

A researcher wishing to book a SafePod must first register with the SPN on the website and agree to the SPN terms and conditions for SafePod use. A training questionnaire must also be passed.

A researcher chooses a SafePod to book from the website, the date and time they wish to book a SafePod for, the Data Centre to connect with and any requests for SafePod use (see below).

A provisional email is then sent to the requested Data Centre who will then confirm or reject the booking.

If a booking is confirmed by a Data Centre, then a confirmation email is sent to the researcher and SafePod organisation with conditions of SafePod access. If a booking is declined, then an email is sent to the researcher with the reason for the decline.

On confirmation, the researcher can attend at a SafePod Organisation on the booking date. Local identification checks are completed by a SafePod Coordinator at a SafePod Organisation before a researcher can access and use a SafePod.

9.2. Requests for SafePod use

A researcher can request the following for their research as part of a SafePod booking:

- A second researcher to use a SafePod at the same time;
- Another person to assist a researcher to use a SafePod;
- The SafePod writing panel to make temporary notes;
- Specific books or journals to be taken into a SafePod;
- Writing materials to be taken into a SafePod; and
- Devices to be taken into a SafePod.

A Data Centre will decide on any such requests and a researcher will be notified of these in their confirmation booking email.

9.3. Additional website functionality for researchers

Once a researcher has created a SPN account, then they can:

- Make SafePod bookings;
- View a diary of their SafePod bookings and make cancelations;
- View relevant SPN policies and documents; and
- Provide a profile for other researchers to view on the SPN website.

9.4. Additional website functionality for SafePod Organisations

SafePod Organisations can manage their SafePod using the SPN website. This includes the following:

- Content management for their public SafePod page which details a wide variety of information about their SafePod;
- Update forms to record security checks for bookings, incidents and SafePod faults and maintenance;
- View a calendar for SafePod bookings; and
- Functionality to update calendar for SafePod booking availability.

9.5. Additional website functionality for Data Centres

Data Centres will be able to:

- Provide information about their organisation on their public SPN page;
- View security checklists for SafePod bookings;
- View security information for SafePods;
- View SafePod incident reports;
- View a calendar for SafePod bookings; and
- View maintenance checklists for SafePods.

10. CCTV system

A CCTV system is installed into a SafePod. The main purpose of the SPN CCTV system is:

- To provide evidence to Data Centre that a researcher is accessing and using their datasets in accordance with their terms and conditions of dataset access and use established between both parties;
- For the University of St Andrews to ensure SafePods are protected and help to establish whether a researcher and SafePod Organisation has complied with the relevant SPN terms; and
- Management of the data protection rights of researchers and other individuals captured by CCTV footage when using a SafePod.

Further information is contained in the SPN CCTV Governance Statement document available from the SPN website.

11. Further information for Data Centres

11.1. SPN Data Centre agreement

A Data Centre will need to sign the SPN Data Centre Agreement which sets out the terms and conditions to be a part of the SPN. An authorised signatory at a Data Centre will need to sign the agreement.

11.2. Data Centre staff

A Data Centre must provide the names and contact information to the SPN for the following:

- A Senior Responsible Person that has overall responsibility for a Data Centre to be part of the SPN; and
- A minimum of two members of staff that will manage the requests for SafePod bookings and update the SPN website as and when needed.

11.3. Approval for a researcher to use a SafePod

It is for a Data Centre to determine whether a researcher can use a SafePod to access their datasets and under what access conditions. Dataset access is subject to a Data Centre's own terms and conditions and must include appropriate CCTV terms and a relevant privacy notice if the SPN CCTV system is to be used.

11.4. Credentials for a SafePod booking

Where required, a Data Centre must provide the necessary credentials and passwords to a researcher to access their project datasets from a SafePod.

11.5. Data Centre staff availability for a SafePod booking

It is for a Data Centre to determine whether they should have a member of staff on duty during a SafePod booking. It is suggested that as a minimum, a member of staff should be available at the start of a SafePod booking in case a researcher had problems with authentication to connect to their project datasets.

11.6. Researcher identification checks

When a researcher arrives to use a SafePod, a SafePod Coordinator will check a researcher's identification prior to giving access to their SafePod. Only a valid original driving licence or passport are acceptable forms of identification.

11.7. Cancelling a SafePod booking

A Data Centre can cancel a SafePod booking by contacting the relevant SafePod Coordinator. An email or telephone call will be sent to the researcher to advise of the cancellation. A cancellation should only occur if a Data Centre no longer wishes a researcher to use a SafePod or if any required staff members are not available for a SafePod booked session.

11.8. CCTV system

The CCTV system inside of a SafePod will automatically record a SafePod booked session. If a Data

Centre does not require a SafePod booked session to be recorded, they can request this is turned off when the SafePod booking is confirmed.

To view CCTV, staff at a Data Centre must request access through the SPN website.

11.9. Updates to the SPN website

A Data Centre must keep the information about their organisation on the SPN website up to date.

11.10. SPN policies

A Data Centre may wish to familiarise themselves with the various policies and agreements for the operation, management of the SPN and booking procedures for SafePods. Details of policies are available from the SPN website and copies can be requested from the SPN

11.11. SafePod Assurances

For every SafePod that a Data Centre provides access to their datasets, they can from the SPN website:

- For each SafePod booking, check that a SafePod Organisation has completed the security checks (as detailed in the SafePod Coordinator Manual);
- View incident reports for a SafePod;
- View security information; and
- View SafePod maintenance and fault reports.

11.12. SafePod Coordinator assurances

SafePod Coordinators manage SafePod bookings and complete security checks for every booking at their SafePod Organisation. Prior to appointment to the role, they must complete the SPN background check (which includes a basic disclosure check) and pass a training questionnaire based on SPN policies.

11.13. Supply of a Data Centre thin client to a SafePod Organisation

If the SPN Dataset Access Service is not used, as an alternative a Data Centre can supply their own thin client or PC to a SafePod Organisation to facilitate a remote or local connection for access to their datasets.

Any maintenance or updates are the responsibility of a Data Centre, but they can request a SafePod Organisation to complete any procedures if they wish.

The cost of any transportation of a thin client between a Data Centre and a SafePod Organisation is the responsibility of a Data Centre.

12. University of St Andrews responsibilities

The SPN is managed by the University of St Andrews. The following sets out the main resources and support that will be provided.

12.1. SafePod funding

The funding and provision of a network of SafePods, based within higher education institutions and other organisations across the UK.

12.2. SafePod design

To ensure that the design, specification and security features for a SafePod are implemented and maintained.

12.3. SafePod security and management

To ensure that SafePod security and their management is in line with the controls detailed in the SPN internal procedures document.

12.4 SafePod Network maintenance

To ensure that SafePods and associated services are properly maintained. To ensure that repairs or faults to a SafePod or associated services are remedied within ten working days of notification of the fault or repair.

12.5. Policies and procedures

To create, manage and update policies, procedures and agreements necessary for the operation, management and security of SafePods and the SPN.

12.6. CCTV system

To provide a CCTV service to enable Data Centres to monitor activity within a SafePod.

12.7. SPN website

To create and manage the SPN website to provide the functionality for the bookings and management of SafePods.

12.8. Secure IT system

To procure, configure and manage a secure IT system to enable secure remote access to a Data Centre's datasets from a SafePod.

12.9. User Support Service

To provide a User Support Service to assist with SPN enquiries and issues.

12.10. Advisory Board

To establish an Advisory Board to steer the long-term objectives of the SPN.

12.11. Scans and tests

To organise the necessary vulnerability scans and penetration tests for SafePod and services.

13. Contact information

Darren Lightfoot
SafePod Network
University of St Andrews
Irvine Building
North Street
St Andrews
KY16 9AL

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

SAFEPOD®

SECURE DATA ACCESS