SafePod Network

SAFEPOD®

SECURE DATA ACCESS

CCTV Governance Statement

Copyright

Version control

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

Version No.	Name	Date	Update
1.1	Darren Lightfoot	10.11.20	Minor update to 'Controllers' section
1.2	Chris Milne	27.05.20	Minor updates and clarifications throughout document
1.3	Darren Lightfoot	27.05.20	Minor updates and clarifications throughout document
1.4	Chris Milne	28.05.20	Minor updates and clarifications throughout document
1.5	Darren Lightfoot	09.06.20	Updated to include SafePoint
2.0	Chris Milne	30.08.22	University as a Controller for 24x7 CCTV recording and review; use of behaviour recognition software to identify if third party devices are present in a SafePod.
2.1	Chris Milne	09.11.22	Minor updates
2.2	Darren Lightfoot	01.06.23	Updated to include SafePoints

Authors

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

Darren Lightfoot, University of St Andrews.

.

Introduction

This statement explains how the SPN CCTV System will operate fairly and lawfully in-line with UK data protection law.

Controllers

Controllers for personal data recorded by the SPN CCTV System are:

- **A Data Centre**, where they have:

  (i) Determined that CCTV footage of a SafePod or SafePoint booked session is necessary for a SPN User to access and use their datasets in accordance with their terms and conditions of dataset access and use established between both parties;

  (ii) When reviewing CCTV still images provided by the SPN where it appears that SPN Users have broken their conditions of data use agreed with a Data Centre for a SafePod or SafePoint booked session; and

  (iii) When managing the data protection rights of SPN Users captured by CCTV footage when using a SafePod or SafePoint.

- **The University of St Andrews**, for the purposes of:

  (i) Determining whether a SPN User has complied with the terms of the SPN User Agreement;

  (ii) Protecting the integrity of SafePod and SafePoint facilities;

  (iii) Determining whether an organisation has complied with their SafePod or SafePoint agreement; and

  (iv) Managing the data protection rights of individuals other than researchers, captured by CCTV footage when present in a SafePod or SafePoint e.g., responding to a subject access request made from an employee of a SafePod or SafePoint Organisation.

Each Controller is independent; there are no Joint Controllers (as defined by UK General Data Protection Regulation, Article 26).

The legal basis for the recording of CCTV footage and using behaviour recognition software

It is for each Controller to determine the legal basis for recording CCTV footage. For a Data Centre, it is anticipated that in most instances ‘contract’ will be an appropriate basis, as introduced below.

The University of St Andrews processes personal data collected via CCTV and behaviour recognition software under a range of lawful bases:

- Contract, as the University operates the SafePod Network and provides services to Data Centres and SPN Users via agreements with those parties.
- The University also has powers delegated to it via legislation (the Universities Scotland Acts) to protect its property and revenues. Capturing and reviewing CCTV

footage of SafePods and SafePoints are necessary to support those purposes.

CCTV recording scope and coverage

CCTV **always records** footage inside a SafePod or SafePoint. For each booked session, it is for each Data Centre to determine whether they require activities within a SafePod or SafePoint to be recorded for their own purposes, as set out herein.

The University of St Andrews requires to record and maintain CCTV footage for the purposes of understanding how SafePods and SafePoints are used and to protect and maintain them.

Transparency

When a SafePod or SafePoint booking is made and the Data Centre requires that CCTV footage is recorded, the email confirming the booking will also remind the SPN User of that arrangement.

CCTV recording: Data Centre

Where a Data Centre requires CCTV footage as a condition of access to their dataset(s) with a SPN User, that requirement must be included in their terms and conditions of dataset access agreement and a relevant privacy notice must be provided by them to the SPN User.

A Data Centre can access both live and recorded CCTV footage via the SPN CCTV System made available to them by the University of St Andrews.

The University of St Andrews as a Processor

The University of St Andrews will be a Processor for a Data Centre, as the third-party providing CCTV facilities to a Data Centre, as required and when providing Data Centres with notice where it is suspected that a SPN User may have broken their Agreement with a Data Centre for data use during a SafePod or SafePoint booked session.

Agreements between the University of St Andrews and a Data Centre contain the Processor provisions required by the General Data Protection Regulation, Article 28, 3.

Necessity

Where there is no requirement by a Data Centre for CCTV recording of a SafePod or SafePoint booked session, then the University is the only Controller, for the purposes stated herein.

CCTV recording: University of St Andrews

SPN Users

The University may make use of CCTV footage to establish whether a SPN User has or has not misused or damaged a SafePod, SafePoint or SPN equipment in accordance with the SPN agreement they have signed. The legal basis for use of personal data in these instances is contract.

SafePod and SafePoint Organisations

The University may make use of CCTV footage to establish whether a SafePod or SafePoint Organisation has undertaken their duties as set out in their terms and agreement with the SPN. Where individuals (working for a SafePod or SafePoint Organisation) are recorded by CCTV inside a SafePod or SafePoint when performing their duties, then the legal basis for the recording is legitimate interests, and the University is the Controller.

CCTV recording: SafePod or SafePoint Organisation

Where individuals employed by a SafePod or SafePoint Organisation (e.g. a cleaner, or technician), or other individuals have entered a SafePod or SafePoint, then their footage will be recorded by CCTV.

In circumstances where a SafePod or SafePoint Organisation believes that they require CCTV footage for internal purposes (e.g., to support an accident investigation), then they can request access to recorded CCTV footage from the SPN.

A SafePod or SafePoint Organisation must demonstrate that their intended processing will be lawful before CCTV footage is made available to them. Requests for access should be emailed to safepodnetwork@st-andrews.ac.uk.

If there is any dispute as to whether CCTV footage cannot be made available from the University of St Andrews to a SafePod or SafePoint Organisation, then the University of St Andrews Data Protection Officer will adjudicate.

CCTV footage retention period

CCTV footage recorded inside a SafePod or SafePoint will normally be held for 30 days. Where footage has been transferred then the footage will automatically be held by the SPN CCTV System supplier for up to 365 days before being deleted. Where CCTV footage is transferred to a Data Centre, that Controller will apply their own retention periods to that footage.

Transfer of CCTV footage

The SPN will only normally make CCTV footage available to an authorised member of staff at a Data Centre. Transfer of CCTV footage to other parties may be undertaken where there is a lawful basis to do so.

Requests for live footage by a Data Centre will be provided online through the SPN CCTV system.

Where a request for recorded footage is approved, the footage will be encrypted and transferred to the requestor. The access credentials will be provided under separate cover, applying recognised best practice standards for their construction.

Use of behaviour recognition software

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, SafePod or SafePoint use e.g., if an individual has taken a mobile phone into a SafePod or SafePoint, 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, SafePod or SafePoint use. A Data Centre will be advised of any suspected security incidents relating to their data access conditions.

A list of all SafePod and SafePoint facilities equipped with behaviour recognition software is available from: www.safepodnetwork.ac.uk/behaviour-recognition.

Data protection rights

Where the University is the Controller, they will also use personal data recorded by CCTV in a SafePod or SafePoint (unless an exemption applies) to provide individuals with their data protection rights, as per the UK data protection laws. Notices in each SafePod or SafePoint identifies the University of St Andrews as the operator of the CCTV camera.

If the University receives a data protection rights request from an individual and the University is not the Controller, that request will be passed to the appropriate Controller within 2 working days.

Summary of responsibilities

Data Centre	
	- To confirm with an individual where CCTV footage is to be recorded as a requirement for access to their datasets.
	- Confirm with the University of St Andrews where it is not necessary for a SafePod or SafePoint booked session to be recorded.
	- Make the relevant privacy notice information available to individuals, when an agreement for access to their datasets requires that CCTV imagery is to be recorded.
	- To respond to an individual's data protection rights.
	- To advise the University of St Andrews where CCTV footage is to be archived i.e., retained for longer than 30 days, before that retention period is reached.

The University of St Andrews	
	- To establish whether SPN agreements has been adhered with, including agreements with SPN users.
	- To have in place with the third-party suppliers (for CCTV and behavioural recognition software) contractual provisions as stipulated by UK data protection laws, and to respond in full to those provisions.
	- To provide CCTV services to Data Centres, acting under the instructions of a Data Centre, and per the Agreement between both Parties.
	- Where Behaviour Recognition Software has created an alert, the University will review and verify against the Data Centre's conditions of access for the booking. The SPN will provide Data Centres with notice where it appears that SPN Users may have broken their Agreement with the Data Centre for data use.
	- To have in place and keep under review a legitimate interests assessment, for the capture of CCTV imagery out with that captured at the request of a Data Centre, for a SafePod or SafePoint booked session.
	- To provide CCTV footage to SafePod or SafePoint Organisations, where a request has been validated.
	- To provide a privacy notice for display inside a SafePod or SafePoint for CCTV and when behavioural recognition software is in use.
	- Refer to a Data Centre any requests received from individuals to exercise their data protection rights where the University is not the Controller.
	- To delete CCTV footage and/or retain as per the agreements with Data Centres.

SafePod and SafePoint Organisations	
	• If requesting access to CCTV footage from the University of St Andrews, to provide adequate detail on the purposes of the processing to allow the University of St Andrews to assess whether making footage available will be lawful.
	• To ensure that the CCTV privacy notice supplied by the University of St Andrews is prominently displayed inside a SafePod or SafePoint.

Data Privacy Impact Assessment (“DPIA”)

The DPIA for the scheme is available on request.

Legitimate Interests Assessment (“LIA”)

The LIA for the scheme is available on request.

SPN contact information

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

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

SAFEPOD®

SECURE DATA ACCESS

SCOTTISH CENTRE FOR
ADMINISTRATIVE
DATA RESEARCH

UKRI

Economic
and Social
Research Council

ADR UK
Data-driven change