Phase 1 – Determining whether a Privacy Impact assessment is required

If the answer to any of the questions in below is ‘yes’, proceed to Phase 2.

If the answer is ‘no’ to all the questions, a Privacy Impact Assessment is not required. That decision and the authority for it should be documented and retained.

Questions:

i) Will the project involve the collection of new information about individuals? NO

ii) Will the project compel individuals to provide information about themselves? NO

iii) Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? NO

iv) Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? NO

v) Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. YES – the use of heat sensors to monitor room use has the risk of a perception of intrusion even though no personal data is being processed.

vi) Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them? NO

vii) Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private. NO

viii) Will the project require you to contact individuals in ways which they may find intrusive? NO

A privacy impact assessment is required.
Phase 2 – Conducting a Privacy Impact Assessment

Step one: Identify the need for a PIA

[Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.]

The University of Dundee has been carrying out physical surveys of teaching space for the past 12 years, employing up to 5 staff or students to survey space on an hourly basis during a 40 hour timetabled week. Over this period, little impact has been made on the problem of booked but unused space – the latest survey in October 2017 showed that 30% of bookings during the week were unused. This is a problem because rooms remain unused yet show up on the booking system as booked thus restricting access to others and creating timetabling and booking difficulties for Schools and administrators.

For the same cost of a week-long physical survey, the University can collect room use data over a longer period by sensor technology using CadCapture Ltd’s product Occupeye. These mobile phone-sized wireless sensors are mounted on a wall in the teaching room. Based on passive data technology (PIR), the sensors are triggered by heat and motion and transmit data to a host receiver which records if a room is in use or not in use – there is no personal information collected. The sensors do not monitor individuals or their performance. The room use data will give the University some certainty about the extent of the problem and inform decisions going forward.

No decisions will be made concerning individuals.

Step two: Describe the information flows

[The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.]

From the vendor:

The secure OccupEye host is responsible for receiving data from the OccupEye sensors in packets of bytes, which are serially transmitted via a proprietary wireless protocol. The microprocessor in the OccupEye Host inspects the format of the packet and performs a cyclic redundancy check (CRC) on the data. If the format is correct and the calculated CRC matches the transmitted CRC, the packet is forwarded via the microprocessor’s serial interface to a Serial-to-Ethernet bridge (xPort). The xPort is a widely-used secure communications device, manufactured by Lantronix Inc, a global provider of smart networking and communications solutions.
Our sensor data is Manchester coded to ensure its robust transmission and we also use CRC (cyclic redundancy checking) to ensure that it is received without loss or corruption. However, the data - solely utilisation-related - is completely benign and presents no security risk to any party at any time.

**Step three: Document the consultation requirements**

The project was initiated by Estates and Campus Services. Local trades union branches, HR and the Students’ Association have been consulted and their concerns are addressed in the controls detailed below.

**Step four: Identify the privacy and related risks**

[Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.]

<table>
<thead>
<tr>
<th>Privacy issue</th>
<th>Risk to individuals</th>
<th>Compliance risk</th>
<th>Associated organisation / corporate risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. No personal data is being collected. However, based on the widely-report issues arising from the deployment of this technology at the University of Glasgow, it is recognised that there may be a perception of intrusion through its use.</td>
<td>The deployment of the technology does not, in and of itself, pose a risk to individual privacy.</td>
<td>No personal data is being processed, therefore there is no intrinsic risk associated with the use of the system.</td>
<td>Based upon the experience at the University of Glasgow, a poorly-managed deployment of this technology does carry a risk in respect of the goodwill of staff and students and a degree of reputational risk.</td>
</tr>
</tbody>
</table>

**Step five: Identify privacy solutions**

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

| Risk | Solution(s) | Result: is the risk eliminated, reduced, or accepted? | Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and |
### Step six: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

<table>
<thead>
<tr>
<th>Risk</th>
<th>Approved solution</th>
<th>Approved by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perception of intrusion through the deployment of wall-mounted occupancy sensors.</td>
<td>Comms plan, signage, limitation of project to wall-mounted sensors, limitation of project to high-traffic shared-use spaces.</td>
<td>Aidan McColgan, Acting Director, Estates &amp; Campus Services</td>
</tr>
</tbody>
</table>

### Step seven: Integrate the PIA outcomes back into the project plan
[Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?]

<table>
<thead>
<tr>
<th>Action to be taken</th>
<th>Date for completion of actions</th>
<th>Responsibility for action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development and dissemination of communications.</td>
<td>January 2018 (prior to project start)</td>
<td>Marianne Kenley, Building Space Manager with External Relations.</td>
</tr>
<tr>
<td>Signage to be installed in all rooms where system used.</td>
<td>January 2018.</td>
<td>Marianne Kenley, Building Space Manager.</td>
</tr>
<tr>
<td>Limitation of project scope to teaching rooms.</td>
<td>January 2018.</td>
<td>Marianne Kenley, Building Space Manager.</td>
</tr>
<tr>
<td>Limitation of project scope to wall-mounted sensors.</td>
<td>January 2018.</td>
<td>Marianne Kenley, Building Space Manager.</td>
</tr>
</tbody>
</table>

**Contact point for future privacy concerns**

Marianne Kenley, Building Space Manager.