**Legitimate Interests Assessment Template**

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing of personal data. This template is based on the ICO guidance. Please refer to the [ICO’s guidance](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/) for further information.

You should complete this form and retain a record of the assessment to provide justification for your decision to use legitimate interests as a lawful basis for processing before you start processing the data.

|  |  |
| --- | --- |
| **Name/description of Project/reason for processing personal data** | University CCTV system |
| **Process/project owner (name, job title, department)** | Colin Montgomery, Head of Security Services, SHAW |
| **LIA completed by (if different to above)** | Elaine Grant (IGU) |
| **Date** | 01/12/2023 |

|  |  |
| --- | --- |
| **Part 1: Purpose Test**  **You need to assess whether there is a legitimate interest behind the processing** | |
| Why do you want to process the data? | * To detect, prevent or reduce the incidence of crime; * To prevent and respond to any incidents which may affect the safety and security of the University community and the University estate; * To assist in the management of University facilities/estate/assets, including car parking * To assist with health and safety investigations; * To investigate suspected breaches of University regulations/policies/procedures; * Defending the University in relation to any claims made against it, including employment tribunals. |
| What benefit do you expect to get from the processing? | The main purpose is to provide a more secure campus environment for the whole university community as well as visitors and members of the public.  There will also be benefits in relation to the other purposes stated above: it will enable the University to manage incidents, its facilities/estate, enable investigations where any issues/incidents have occurred and/or there is reason to believe University policies, procedures, regulations or other legislation has been breached. Also, there may be cases where the University is required to defend itself in respect of legal claims/processes. Where CCTV footage relates to these claims/processes, then it will be used for these purposes (although this is not the main purpose of the system). |
| Do any third parties benefit from the processing? | Yes, staff, students, contractors, visitors and members of the public benefit from having a more secure and safe campus. |
| Are there any wider public benefits to the processing? | Yes, staff, students, contractors, visitors and members of the public benefit from having a more secure and safe campus. |
| How important are the benefits that you have identified? | It is vital that the University campus and buildings are safe for anyone who uses, visits and/or is in the vicinity. The main aims are around providing a safe and secure environment which is essential for everyone. |
| What would the impact be if you couldn’t go ahead with the processing? | Security would be diminished and it is likely to have a highly detrimental effect on the Uni community, who would feel less safe. It may also increase the chance of crime which can have a huge impact on any victims and on the University. |
| Are you complying with any specific data protection rules that apply to your processing, e.g. (profiling requirements, or –privacy legislation)? | Have conducted a DPIA as required in relation to high risk profiling i.e. due to monitoring publicly accessible places on a large scale.  No other specific DP rules. |
| Are you complying with other relevant laws? | No other specific laws to comply with |
| Are you complying with industry guidelines or codes of practice? | Yes, ICO guidance |
| Are there any other ethical issues with the processing? | No |

|  |  |
| --- | --- |
| **Part 2: Necessity test**  **You need to assess whether the processing is necessary for the purpose you have identified** | |
| Will the processing actually help you achieve your purpose? | Yes |
| Is the processing proportionate to that purpose? | Yes |
| Can you achieve the same purpose without the processing? | No |
| Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way? | No – location of cameras in buildings is assessed in relation to risk. |

|  |  |
| --- | --- |
| **Part 3: Balancing test**  **You need to consider the impact on individuals’ interests and rights and freedoms and assess whether this overrides your legitimate interests.** | |
| **Nature of the personal data** | |
| Is it [special category data](https://moss.strath.ac.uk/stratpolicy/infoman/SitePages/WhatisPersonalData.aspx) or criminal offence data? | Unlikely. Any special category data is more likely to be inferred from the specific circumstances of an event/protest etc. taking place that might be caught whilst routine recording is taking place. There is no explicit intention to capture this data. |
| Is it data which people are likely to consider particularly ‘private’? | No |
| Are you processing children’s data or data relating to other vulnerable people? | No |
| Is the data about people in their personal or professional capacity? | Both |
| **Reasonable expectations** | |
| Do you have an existing relationship with the individual? | Mostly – for staff, students and visitors. Members of the public may cross the campus. |
| What’s the nature of the relationship and how have you used their data in the past? | Staff, students – purposes are set out in relevant privacy notices. Attendees at events, should be provided with privacy notice for events. Users of facilities, e.g. library, sports centre, will also be provided with specific privacy notices. |
| Did you collect the data directly from the individual? What did you tell them at the time? | No – routine recording. There is signage up where cameras are recording. |
| If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? | N/A |
| How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? | N/A |
| Is your intended purpose and method widely understood? | Yes – use of CCTV is common and is generally understood. |
| Are you intending to do anything new or innovative? | No |
| Do you have any evidence about expectations – e.g. from market research, focus groups or other forms of consultation? | No |
| Are there any other factors in the particular circumstances that mean they would or would not expect the processing? | No |
| **Likely impact** | |
| What are the possible impacts of the processing on people? | Little impact unless an individual is someone involved in an incident that requires further investigation. |
| Will individuals lose any control over the use of their personal data? | Possible |
| What is the likelihood and severity of any potential impact? | Images may be used for further investigations, either internal or external. If the images provide evidence, this may be significant for individuals, if they are the perpetrator or the victim. For most people, there is no impact. |
| Are some people likely to object to the processing or find it intrusive? | Unlikely. CCTV has been in operation for many years and rarely receive complaints about its operation. |
| Would you be happy to explain the processing to individuals? | Yes |
| Can you adopt any safeguards to minimise the impact? | Yes – access restricted, purpose clearly identified to Security Services staff, thorough training of SS staff re acceptable use of the system and reproduction of images. If images are downloaded they are only made available to a restricted group of people, depending on authorisation from a senior member of Security Services staff. |
| Can you offer individuals an opt-out? Yes/No | No |

|  |  |
| --- | --- |
| **Part 4: Making the decision**  **Use your answers to Parts 1, 2 and 3 to decide whether or not you believe you can apply the legitimate interest’s basis.**   * **You should weigh up the all the factors identified for and against the processing, and decide whether you still think your interests should take priority over any risk to individuals.** * **You should be as objective as possible.** * **You must be confident that you can show why the benefits of the processing justify and risks you have identified.** | |
| Do you believe you rely on legitimate interests for this processing? Yes/No | Yes |
| Do you have any additional comments to justify this answer? | No |
| **IGU review - you should also submit the LIA to the Information Governance Unit for assessment (dataprotection@strath.ac.uk)** | |
| IGU Assessment | No further IGU assessment undertaken as completed by IGU |
| DPO Opinion | The LIA was completed by me based on my understanding of the system and in collaboration with Colin Montgomery, Head of Security Services. I have no concerns about the reliance on legitimate interests for the use of this system. |
| Date | 11/04/2025 |

|  |  |
| --- | --- |
| **Outcome and decision**  **Based on the information included in the assessment above and following the comments from the DPO, you should indicate whether or not you are going to rely on legitimate interests as your lawful basis for processing.**  **NB the final decision should be made by a senior member of staff with responsibility for the project/processing. They must sign this section (or otherwise indicate their authorisation).**  **You should retain a copy of this form, along with other relevant information relating to the processing.** | |
| We **are** relying on legitimate interests for this processing (tick if relevant). |  |
| We **are not** relying on legitimate interests for this processing (tick if relevant).  NB if not, you must ensure you can rely on another [lawful basis](https://moss.strath.ac.uk/stratpolicy/infoman/Shared%20Documents/GDPR%20Guidance%20Note%20-%20Lawful%20Basis%20for%20Processing.pdf). |  |
| Authorised by:  (include name, job title/role, dept) |  |
| Signed by |  |
| Date |  |