

## Guidance on the use of images

### Photographs

- **Are photographs personal data?**  
Photographs of living people are personal data and therefore fall under the Data Protection Act and must be treated accordingly.
- **Are photographs sensitive personal data?**  
Sensitive personal data consists of information on someone's racial or ethnic origin, political opinions, religious beliefs, trade union activity, physical or mental health, sexual life or any offences committed. Photographs can often contain some of this information, so in certain circumstances, photographs can be sensitive personal data.
- **Information to consider** when you are collecting photographic images: – what is being used, how it will be displayed, how long it will be kept, who will be able to view it and who the data subject should contact if they wish to withdraw their consent.
- Photographs of **crowds** are not classified as personal data, providing no one person is the focus of the photograph. It is good practice, before taking a photograph of a group, to verbally ask permission to do so, therefore giving anyone who does not wish to be included the opportunity to opt out. Crowd photographs which are cropped to focus on one individual will become subject to the Act.
- Photographs taken purely for **personal use** are exempt from the Data Protection Act, e.g. photographs taken by family members at graduation.
- Photographs taken at **registration** are only to be used for security purposes and access to services and can only be used for those reasons. If you wish to use registration photographs for any other reason, you should obtain consent from the individual.
- Staff or student photographs should not be displayed on the wall (noticeboards etc.) or online without consent from the individuals concerned. Any staff or students who do not wish for their photograph to be displayed in a public area should **not** be forced to do so.

### CCTV

- The ICO have produced a Code of Practice for CCTV, which is available here:  
[https://ico.org.uk/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/cctv-code-of-practice.pdf](https://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/cctv-code-of-practice.pdf)

- The Code of Practice covers the use of CCTV, Automatic Number Plate Recognition, body worn video, unmanned aerial systems and other systems that capture information of identifiable individuals or information relating to individuals.
- If you are intending to use such a system, you should always consider the impact it will have on the individuals captured on CCTV.
- The ICO advise:  
*“The fact that it is possible, affordable or has public support should not be the justification for processing personal data.”*
- You must ensure that staff and students are aware of any monitoring taking place and the reasons for it. The University must include it in our notification to the ICO - please contact the Records Management Office for advice on this.
- The monitoring must be appropriately signed, giving contact details for the data controller and reasons why the monitoring is taking place.
- The main CCTV system at the University is managed by the Directorate of Estates and Facilities. All security staff are fully trained in the use of CCTV and follow the national surveillance camera code of practice and the Data Protection Act. If you are going to implement such a system, you must ensure your staff are also trained to follow these standards, both with reference to operating and securely storing images and in responding to requests for information.