Data Protection Impact Assessment

DPIA_113

Primary contacts

Durham Burt **Data Protection Officer** dataprotection@york.ac.uk	Paul Massheder **Security Operations Assistant** paul.massheder@york.ac.uk

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer to or link to other documents, such as a project proposal or ethics application form. Summarise why you identified the need for a DPIA.
The University of York faces a number of key challenges in relation to the management of security and safety, such as; ● A large open campus spread over two sites, with significant number of students, staff and members of the public having access and visiting the campus regularly; ● A large number of students resident on these campuses; ● Several venues offering the sale of alcohol are located on campus; ● Ensuring the continued security of academic buildings in which sensitive materials and assets are stored; ● Providing the physical security element of the Information Security Management system across the university's establishments The University of York has a duty of care to its staff, students and to members of the public who may access its campuses. An operational CCTV system (including Body worn video cameras) is a proportionate response to the associated challenges of the factors listed above and in facilitating the university in meeting its wider legal obligation. In addition, the use of CCTV will also allow the university to establish, exercise and defend its own legal rights and claims. A DPIA is considered necessary because we are: 1. systematically monitoring a publicly accessible area on a large scale; 2. processing data on a large scale; 3. [likely] processing data concerning vulnerable data subjects; 4. [likely] processing special category data or criminal offence data.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?
Data collection CCTV video footage is captured by the cameras and transmitted via network to University servers for storage. Body WornVideo footage is captured and initially stored securely (encrypted) on the device. This is then later uploaded into a secure cloud based storage system (Dedicated bucket on AWS london based server). **Data use and storage** Live viewing of CCTV on the East and West campuses will ordinarily be through a feed into the security control room. CCTV is monitored in the security control room at the University's West campus 24 hours a day, 365 days of the year. The University shall ensure that live feeds from CCTV and Surveillance Systems are only viewed by authorised personnel from the University's security staff and members of staff approved by the Head of Security whose role requires them to have access to such Data. Recorded images will only be viewed in the security control room. Recorded CCTV will be stored on secure university servers, with access restricted to designated security staff and the Head of Security. In certain circumstances in order to preserve recordings captured on CCTV or Surveillance Systems, the Head of Security may direct that recordings captured on CCTV or Surveillance Systems be transferred to DVD (or another service medium) to achieve the purposes and objectives for which CCTV or Surveillance Systems are installed. The transfer of any such recording to DVD (or other service medium) will be processed by the duty security supervisor or any person designated by the Head of Security to carry out that function. Body worn video footage that is captured cannot be viewed from the camera and is transferred to the cloud once the camera is booked back in. Access to any downloaded footage is restricted to designated security staff and the Head of Security.The transfer of any recorded footage will follow the same principles as that of CCTV footage. **Data retention and disposal (same principle for BWV footage)** Typically, recordings shall be retained for a maximum of 31 calendar days following capture and will be securely overwritten or destroyed after this time. Footage captured by BWV cameras will be retained securely on the camera until being uploaded into the cloud. The uploading of footage will automatically wipe the internal storage within the camera. Any captured BWV footage that is requested as part of an active investigation will be marked as evidential and protected from loss. These recordings will be held for 6 months following the date of capture or until the investigation is completed whichever is the later.. All other captured footage will be automatically deleted from the system after 31 days. Where recordings are requested as part of an active investigation, they will be protected against loss or held separately from the surveillance system. These records will be retained for 6 months following the date of last action and then disposed of as per the paragraph above.

Once hardware has reached the end of its active life, DHSS will work with the University's IT Services to ensure safe disposal in line with best Data Protection practice.

Data sharing

Data may be disclosed to law enforcement agencies, insurance companies and also to support internal investigations. Any disclosures will be made in full compliance with UK GDPR requirements. In addition, members of the public may request access to copies of their own data i.e, video footage in which they feature.

As a technology, CCTV is tried and tested. However, it can be privacy intrusive, especially where it is located in areas close to private property, student accommodation blocks etc. All efforts will be made to ensure any privacy intrusion is minimised.

Body worn video is recorded at the discretion of the individual using the device in line with training. All BWV operators will give a clear verbal warning whenever the device is operated. All efforts are made to minimise privacy intrusion.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

CCTV and BWV will be used to monitor and collect video footage for purposes of security and the prevention and detection of crime. In addition it will support initiatives created to reduce vandalism, anti social behaviour, trespass and the protection of University property and assets. Footage is likely to capture special category data (e.g., disability, race and ethnic origin) and/or criminal offence data.

Currently, the University has 411 CCTV cameras in operation. These camera's record 24 hours a day, 365 days a year. In addition the University has 7 Body worn video cameras that are allocated to operational security staff.

For data retention, see section immediately above.

CCTV will be captured across the university campus, spread over three sites, Campus East, Campus West and Kings Manor.

In theory, any individual on campus will be affected. As the campus is open to the public, we are unable to provide an estimate of daily/monthly/annual footfall.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in?

Students, staff, visiting lecturers, contractors and members of the public will be captured on the recordings. We have a direct relationship with our students, staff and other stakeholders and an indirect relationship with any campus user. CCTV is, typically, quite visible across the University and some signage is in place. In addition, CCTV is widely used across the UK so it's presence on campus is unlikely to be unexpected.

Body worn video cameras are worn securely in a prominent position on the high visibility vest of operation security staff. Each Camera is signed identifying that it records Video and Audio

Children (i.e, students under the age of 18 and members of the public under the age of 18) are likely to be captured on the recordings. In addition, vulnerable individuals (e.g., students, staff and members of the public with certain disabilities) and older individuals are also likely to be captured on the CCTV.

There are privacy concerns arising from the use of surveillance technologies. However, the University is committed to careful placement of CCTV cameras to minimise privacy intrusion. For example, our policy states:

Cameras must not be used to view into private property and operations staff must be mindful of student privacy within accommodation blocks.

In addition, equipment must be carefully positioned to:

- *cover the specific area to be monitored only;*
- *keep privacy intrusion to a minimum;*

In addition, CCTV or BWV is not used in changing rooms, toilets or other areas where privacy expectations are high.

The technology, itself, is not novel and there are no known security flaws. For example, cameras are high quality and secure when properly configured.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

The University uses CCTV and BWV;

- to demonstrate a duty of care to its students, staff and campus users;
- to protect university property, both external and internal
- as a deterrent e.g, to discourage anti-social behaviour, vandalism;
- to monitor public areas, to detect incidents and to coordinate university responses;
- to provide assistance in the detection and prevention of crime.
- to provide reassurance to all campus users
- to create a secure and safe environment for all
- to support our safeguarding responsibilities
- to support access control systems

CCTV (along with quality doors, locks, alarms, security lighting etc.) also provides a 'technical measure' under the GDPR to protect paper and electronic data stored on campus.

For individuals, CCTV can be reassuring and provide that safe environment.

For the University, we have a duty of care to our students, staff and campus users. CCTV allows us to monitor the campus, deter anti-social behaviour and support security patrol initiatives

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
We have consulted and continue to communicate with departments, receptions, student unions and trade unions whenever,changes are made to the CCTV infrastructure. This includes the sighting of new CCTV cameras to support initiatives highlighted in step 1.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Data is processed under Article 6 (f) legitimate interests and Article 9 (g), Processing is necessary in the substantial public interest, specifically for the purposes of the prevention or detection of an unlawful act. The University of York maintains a dedicated campus security team, who are ultimately responsible for providing the security function at the University. As part of their wider work, they conduct regular patrols, providing a security presence when needed, they also are responsible for responding to security incidents on campus. The team are the main point of contact for enforcement authorities around wider public order and crime issues. Additional security measures adopted by University of York include electronic access control systems to all academic buildings and residencies. Improved lighting both internally and externally across the estate. Identified safe routes across campus and use of 'Safezone' a phone app directly linked to the security control room. The CCTV system and Body worn video are designed to complement these activities and provide a greater oversight of the security landscape, thereby making the most of the resources available to the team. All recorded CCTV data and Body worn video footage will be retained for no longer than 31 days unless part of an ongoing investigation/court case. All CCTV cameras across the University are being replaced with HD 4K quality cameras to ensure any data captured is of a high quality. Any data captured is stored on secure servers within the University. The Body worn video cameras are current technology, do not allow the user to view footage which is encrypted. The cameras upload to a secure digital evidence management system that ensures footage is managed in a secure environment. The University is committed to using CCTV and Body worn video cameras sparingly. As part of the CCTV system upgrade, careful review will be undertaken to ensure cameras: 1. cover the specific area to be monitored only;

2. keep privacy intrusion to a minimum;
3. ensure that recordings are fit for purpose and not in any way obstructed (e.g. by foliage);
4. minimise risk of damage or theft.

In addition, cameras will be placed in strategic locations to ensure they can (a) fulfil the intended purposes and (b) minimise privacy intrusion. CCTV cameras will not be placed in areas where privacy expectations are high e.g., changing rooms/toilets.

Signs will be displayed at campus entrance/exit points and in areas of strategic importance and will communicate:

- that monitoring and recording is taking place;
- who the system owner is;
- where complaints/questions about the systems should be directed.

In addition, the University has produced a standard surveillance notice for use on campus. Amongst other things, this notice sets out the rights of individuals.

Function creep will be avoided by:

1. capturing the minimum amount of data necessary for the purpose;
2. articulating the purpose in our Surveillance Policy;
3. restricting access to CCTV images on a need-to-know basis;
4. retaining CCTV footage for no longer than necessary;
5. training staff with access to the footage on how it can and cannot be used.

All data, including backups, are stored on the University network. As a result, no third party processor has access to University data.

Step 5: Identify and assess risk

Risk no.	Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
		Remote, possible or probable	Minimal, significant or severe	Low, medium or high
1	Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, CCTV recordings.	Remote	Significant	Medium
2	Lack of privacy information leading to non-compliance with first data protection principle i.e., requirement to ensure processing is fair, lawful and transparent.	Remote	Significant	Medium
3	Local installation of surveillance equipment by Depts. without Security's involvement.	Possible	Significant	Medium
4	Excessive data capture e.g., placement of multiple cameras covering one location or capture of footage 24 hours per day 7 days per week.	Possible	Minimal	Low
5	Excessive data retention i.e., retention of surveillance footage for longer than needed.	Remote	Minimal	Low
6	Excessive sharing within UoY i.e., as a result of failure to lock-down access on a need-to-know basis.	Remote	Minimal	Low
7	Unlawful sharing with 3rd parties i.e., disclosure to third parties without appropriate GDPR safeguards in place.	Remote	Minimal	Low
8	Privacy intrusion e.g., location of cameras near accommodation block windows, private residences, in changing rooms, toilets etc.	Remote	Minimal	Low
9	Poor quality recordings unable to fulfil their intended purpose.	Possible	Minimal	Low

10	Risk that CCTV is renewed and/or installed without following policy requirements e.g., undertaking a DPIA to minimise privacy risk.	Remote	Minimal	Low
11	Risk of function creep i.e., reuse of surveillance footage for a secondary, incompatible purpose.	Remote	Significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated, reduced or accepted	Low, Medium or High	Yes/no
1	All footage is stored securely on University servers or a secure cloud. Access to footage is restricted to authorised personnel in line with GDPR requirements. Footage captured on portable BWV is encrypted and uploaded to secure servers at the end of shift. In the event a portable device is lost, footage is not accessible. For data to be viewed, the portable cameras need to be downloaded to proprietary DEMS software provided by Pinnacle under licence.	Reduced	Low	Yes

2	Privacy notices published and communicated to data subjects widely e.g., via online privacy information/campus signage.	Reduced	Low	Yes
3	Communication across all departments identify the need to ensure that CCTV installation requests are communicated to, and assessed by security before that installation is made. Thus ensuring compliance with this DPIA and a consistent approach.	Reduced	Medium	Yes
4	Careful consideration during renewal/first time installation to ensure the number of cameras in situ is not excessive. A light touch DPIA checklist will be developed to sit alongside this DPIA to ensure all installations are (a) fit for purpose and (b) not excessive and (c) not privacy intrusive.	Reduced	Medium	Yes
5	Agreed retention periods are set out in this DPIA and in the University's Surveillance Policy. Deletion is automated so risk of excessive retention is low. Where records have been manually flagged for extended retention, standard operating procedures will ensure they are deleted as soon as they are no longer required.	Reduced	Medium	Yes

6	Access will be restricted on a need-to-know basis. Where access is granted to colleagues in the UoY, it will be (a) justified and (b) properly documented.	Reduced	Low	Yes
7	Access will be restricted on a need-to-know basis. Records of any 3rd party disclosure will be maintained by DHSS. The University's Information Governance Officers will provide further training/checklists and templates as required.	Reduced	Low	Yes
8	See mitigation 4 above. In addition, where camera location carries possible privacy intrusion but is considered necessary, technologies such as privacy masking will be considered.	Reduced	Low	Yes
9	DHSS will ensure the chosen surveillance hardware is fit for purpose i.e., can record footage at a high enough quality to support the purpose.	Reduced	Low	Yes
10	See mitigation 4 above.	Reduced	Low	Yes
11	Accepted uses for surveillance footage are set out in this DPIA, the University's Surveillance Policy and in published privacy notices. As a result, risk of secondary re-use is low as all	Reduced	Low	Yes

	individuals with access to the footage understand how it can (and can't) be used. In addition, by retaining data for a limited timeframe, opportunity for secondary re-use is further reduced. Finally, all staff with access to surveillance footage undergo training in its accepted use.			

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Durham Burt, DPO, 01/04/2021.	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Durham Burt, DPO, 01/04/2021.	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes, at the point of DPIA submission.	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Provided the mitigations outlined in step 6 above are fully incorporated, data protection risk is low. This DPIA should, of course, be kept under review and should be revisited in the event a change to the processing arrangement is envisaged e.g., a new use for the data is identified or a n		
DPO advice accepted or overruled by:	Accepted by Geoff Brown, Security Manager**.**	If overruled, you must explain your reasons
Comments: None.		
Consultation responses reviewed by:	N/A	If your decision departs from individuals' views, you must explain your reasons
Comments: N/A.		
The DPIA will be kept under review by:	Paul Massheder Security Operations Assistant	The DPO should also review ongoing compliance with DPIA

Source: Information Commissioner's Office, *DPIA Template, available,* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.