Data Privacy Notice

Campus Closed Circuit Television (CCTV), Automatic Number Plate Recognition (ANPR) and Body Worn Video (BWV) systems.

Keele University is committed to looking after your data.

This ancillary privacy notice details the specific data processing activities which the Security team at Keele will undertake in relation to Closed Circuit Television (CCTV), Automatic Number Plate Recognition (ANPR) and Body Worn Video (BWV) recording systems. This Privacy Notice should be read in conjunction with other privacy information which you can find at: www.keele.ac.uk/privacynotices/

Data Protection Principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

Categories of personal data to be processed in respect of this notice include:

- Moving and still digital images obtained from the CCTV system
- Still digital images from the ANPR system and automatically generated data (vehicle registration mark) arising from these images;
- Moving and still digital images including audio recordings from the BWV camera's issued to Security and Traffic Enforcement Officers as part of their personal protective equipment.

This data is processed on the basis of the following conditions:

- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official duty vested in Keele (as the Data Controller)
- The processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

And in respect of sensitive personal data captured by these systems that in addition:

- The processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement; or
- The processing is necessary for reasons of **substantial public interest** and is authorised by domestic law, under Sch 2 Part 2 of the DPA18 – in respect of:
    - Preventing or detecting unlawful acts; or
    - Protecting the public against dishonesty; or
    - Regulatory requirements relating to unlawful acts and dishonesty etc; or
    - Safeguarding of children and of individuals at risk.

How is your personal information collected?

CCTV: digital moving images are captured from cameras sited at various locations across the campus, both outside and also within academic and accommodation buildings. Notices warning people that CCTV is in operation are sited at the entrances to campus and also at numerous locations around the campus, particularly in proximity to areas where CCTV is in operation.

ANPR: digital images are obtained as vehicles pass the ANPR cameras at the main entrance/exits to campus near to the main A525 roundabout and on Keele Drive towards Keele Village. These digital images are automatically processed by the camera and a vehicle registration number generated which is then stored by the system and time, date, location stamped alongside the image itself.

BWV: the body worn camera's do not continuously record as they need to be activated by the officers they are issued to in line with their training and when circumstances justify it. Digital images and audio are encrypted and recorded securely on the device itself and then transferred to a secure database when the camera is docked within the Security Control Room before being formatted to erase all recordings from them.

How we will use personal data from our CCTV, ANPR and BWV systems?

The purpose of collecting and processing the data is as follows:

Across all these systems:

- the provision of a safe and secure campus environment for all users and the prevention, reduction, investigation and prosecution of crimes, and acts of anti-social behaviour or disorder;
- the maintenance of health & safety regulations and requirements;
- the provision of information to support student discipline and fitness to practice investigations and hearings where major breaches have taken place;
- the provision of information to support internal University staff/member disciplinary proceedings linked to serious breaches of contract or misconduct.

and additionally in respect of just the ANPR and CCTV systems

- the provision of information to support the University to carry out research to develop strategies to understand and better manage the environmental impact of campus users transportation choices leading towards 'greener' and better outcomes.
- the processing of information about the presence and flow of vehicles on campus to enhance the of vehicles where there is abuses or breaches of contract, or fraudulent uses of parking permits and the effective operational management of the campus car parking and roads infrastructure.

How personal data from CCTV, ANPR and BWV will be used and processed.

CCTV: Our CCTV cameras are monitored live 24/7/365 by trained officers within a Secure Control Room, which will also deploy our Campus Security Team to incidents in order to enhance safety and confidence within our community. Digital images from all cameras on the campus system are securely stored on servers (none of our cameras monitor or record audio) and can only be accessed by staff who have appropriate authority and training to do so.

ANPR: Digital images are obtained by our ANPR camera's as vehicles pass them at our main entrances/exits to campus. The cameras automatically process images in order to generate vehicle registration numbers linked to each image and this information along with the time and date, location, direction is then securely stored on a server. Access to data from this system is heavily restricted and can only be obtained by a small number of trained and authorised staff within the Security Team. After the data retention period has expired personal information from this system (the image of the vehicle registration plate and the vehicle registration mark generated from it) is automatically deleted, however the non-personal data is retained in order to support the University in analysing, understanding and improving traffic movement and management on campus.

BWV: Digital images and audio are gathered when a trained Security or Traffic Enforcement Officer activates the device (normally with a verbal warning being issued to anyone present). Initially this information is encrypted and stored securely on the device itself, which when returned to the Security Control Room downloads the data onto a secure server before formatting itself to remove all data and images prior to charging and re-issue. Access to data from BWV is heavily restricted to a small number of trained and authorised University staff with specific responsibilities and limited to the level necessary in order that they can undertake work in line with the purposes outlined above.

Data Sharing

Personal data obtained through these systems may be shared under the following circumstances: -

- Internally with HR and investigating officers appointed by the University, where there is an investigation into staff misconduct, which is sufficiently serious that it may result in a staff discipline hearing being convened.
- Internally with the Student Discipline Team or their appointed investigating officers, where there have been alleged breaches of student discipline and the information held on the system is reasonably believed to be materially important to their investigation
- Externally with the Police, when we have been legally requested/required to provide it in support of the investigation or prosecution of crime AND where sufficient grounds exist to satisfy us that this is necessary.
- Externally with third parties in support of civil claims or action which have resulted as incidents on our site that have been captured on our systems, where this is allowed in law, reasonable, necessary and proportionate to the circumstances. (This includes for instance providing images of offending vehicles colliding with and damaging cars parked on our car parks to an insurance company, solicitor or injured party where this is formally requested and directly in support of a civil claim or legal action being taken against the party responsible).

- Externally to third parties who are contractor organisations providing services, or managing compounds on our campus; or the Health & Safety Executive if undertaking an investigation into a serious incident, arising from dangerous contractor or operator behaviour which is in breach of our Campus Safety requirements, a contractors Risk Assessment and Method Statements or safe working practices, where this disclosure is legally allowed, and in the interests of maintaining a safe campus environment or it is clearly in the public interest.

We require any third parties with whom we share data to respect the security of your data and to treat it in accordance with the law.

PLEASE NOTE: ANPR is not operated in order to monitor or investigate staff attendance or time-keeping issues and data from this system will not be shared for these purposes)

Data Retention Period

Personal information obtained from these systems is automatically deleted after a period of 30 days unless its retention is necessary and justified in support of University procedures associated with student discipline or staff misconduct, or for other legally allowable grounds (e.g. in cases where civil liability issues may arise). Any subsequent storage will be for the minimum necessary duration in line with the University's published Retention Schedule.

Your Rights

You have a number of rights with regards to how we process your information including access, correction, erasure and restriction.

Full details of these rights and how to exercise them can be found at: https://www.keele.ac.uk/informationgovernance/yourdata-yourrights/

Data Protection Officer

We have appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

DPO contact details: dpo@keele.ac.uk
ICO contact details: www.ico.org.uk

Changes to this Privacy Notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.