Policy statement: Disclosure of Access Card Data V.1

The University maintains policies and procedures that govern the disclosure of personal data in relation to the exercise of its many legal duties. At present, the University does not actively disclose Access card data, either to external or internal parties and therefore does not have an established policy regarding the handling of such requests.

It is recognised that in order to properly monitor the effectiveness of the University's COVID-19 risk management activities, there may be circumstances where the analysis of Card Access data is necessary. The University's Head of Security and Data Protection Officer have worked together to produce this policy statement, outlining the principles and procedures that should govern any such disclosure so that requests are processed in compliance with data protection law.

The policy statement is based on the principles outlined in the University's CCTV policy having been endorsed through various University committees.

Background

It is recognised that in certain circumstances it may be necessary to analyse Card Access data where the University deems doing so is essential to meet its various legal and duty of care obligations. It is obvious that accessing such information has a number of associated privacy implications, therefore the University must have attempted to achieve the same outcome using less intrusive methods or have established that other methods would prejudice the intended outcome before seeking access to those records.

Disclosure of Access Card data and the Data Protection principles

Access card records will be processed in compliance with the data protection principles contained in the General Data Protection Regulation:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals.

Card access data must only be used where all other approaches to achieve a particular aim have failed or would attempting to achieve the same outcome using alternative methods would be likely to prejudice the intended aim. When processing card access information, the University will rely on a lawful condition of processing, which must be outlined in any request for access. The University must ensure that the existence of this policy statement and associated process is placed on an internal webpage.

b) Collected for specified, explicit and legitimate purposes and will not be further processed in a manner that is incompatible with those purposes.

Requests for Access card records shall be considered on a case-by-case basis and any request must be made using the process outlined in this document. If a decision is made to disclosure access card records, then disclosed records must not be used of any other purpose.

Disclosure of Access card data shall only be considered where it is necessary for the University's legitimate business purposes as detailed in the 'Purposes and Objectives of Card Access Systems' section of this document. This list is not exhaustive and other purposes may be or become relevant.

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed - data minimisation.

Any request for Access card data must be specific and can extend to staff ID/name, entry times and where available exit times.

d) Accurate and, where necessary, kept up to date.

Colleagues must understanding that card access data is limited in its usefulness (in that they only records how many/who has accessed the building, bot how many are occupying a building at any one time). Staff holding disclosed Access card data must ensure that data is retained in compliance with the retention periods as outlined in this policy statement.

e) Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Any disclosed data must been retained only for as long as it is necessary to meet the aims of disclosure.

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Any request for Access Card data must be made using the procedure outlined in this document. Any data disclosed shall be transferred to the request through secure means and shall be password protected. The requester must ensure that the data transferred to them is stored in a secure location with access limited to those necessary to complete any related tasks.

The process for requesting Card access records shall be modelled on the processes laid out in the CCTV policy.

Purposes and Objectives of Card Access Systems

1. Ensuring the safety of staff, students and visitors and to act as a deterrent against crime;
2. To prevent crime and protect buildings and assets from damage, disruption, or vandalism;
3. Assist in deterring, investigating and detecting crime or reports of possible crime;
4. Facilitate the identification, investigation, apprehension and prosecution of offenders or suspected offenders;
5. Support law enforcement bodies in the prevention, detection, investigation and prosecution of crime;
6. Support the investigation of safety and security-related incidents and suspected misconduct by staff, students or visitors;
7. Provide law enforcement bodies or the University with evidence which may lead to possible criminal, civil or disciplinary action against either staff, students or visitors or to investigate the possibility of any possible criminal, civil or disciplinary action against either staff, students or visitors;
8. Provide evidential material for use in potential criminal, civil or disciplinary actions including employment tribunal proceedings;
9. Facilitate the identification and investigation of any suspected breaches by the University or staff of their respective obligations and rights in connection with employment;
10. Assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings.

Procedure for requesting Access Card data

1. The University may share Data with other organisations, for example with the police or law enforcement agencies, where it considers that this is reasonably necessary for the purposes and objectives set out in the 'Purposes and Objectives of Card Access Systems'.

2. No data from the University's Card Access Systems will be disclosed to any third party, without express permission being given by the Head of Security. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or a court order from a court with competent jurisdiction has been produced.

3. In other appropriate circumstances, the University may allow law enforcement agencies to view or remove Card Access data where this is required in the detection or prosecution of crime.

4. The University's Head of Security will maintain a record of all disclosures of recordings made on Card Access Systems.

5. Requests to access Card Access data for the purposes of reviewing the data to establish if any evidence has been captured on Card Access Systems will be restricted. Currently this is the Electronic System Technician(s) [Tracey Davies who runs the reports], University Head & Deputy Head of Security, the Deputy Director Estates (Campus Services), professional legal advisors and the police or other relevant law enforcement agency where appropriate.

6. Requests to access Card Access data under 'Purposes and Objectives of Card Access Systems' should be made by the University manager and /or HR Manager responsible for the relevant investigation or hearing only, and will be authorised by the University's Head of Security. In this context, "investigation" refers to both formal and informal investigatory processes which may be initiated by the University from time to time. Any such request will be accompanied by a statement from the responsible manager confirming whether the images will (or may) require disclosure to a Trade Union or employee representative.

7. Before disclosing any Card Access data including Personal Data in response to a request, the University's Head of Security will be satisfied that the request is compatible with the 'Purposes and Objectives of Card Access Systems' and the necessary Data Subject Access Request form has been correctly completed and submitted. Where necessary, the University's Head of Security will consult with the University's HR Director and Data Protection Officer (and if needed professional legal advisors) in order to determine whether it is appropriate to grant any requested disclosure.

8. Where any request made pursuant to 'Purposes and Objectives of Card Access Systems' is authorised by the University's Head of Security, copies of any Card Access data will be produced in PDF format. It can also be transferred to CD or another service medium) to achieve the purposes and objectives for which the request was made and will be signed for by the authorised University Manager and or HR Manager.

9. Copies made of any Card Access Systems will be securely destroyed once there is no reason to retain the recorded information.

10. If the Head of Security is unavailable, the Deputy Head of Security or nominated appointee from the Estates Senior Management Team are authorised to carry out the same functions as the Head of Security.