Access Control Code of Practice

1. Introduction

1.1 The University of Worcester uses an electronic Access Control system (SALTO) to control access to its buildings both on and off campus including residential accommodation. The system allows remote access to authorised users of various buildings linked to the system via the University network.

1.2 Buildings and rooms can be accessed by using either your Staff, Student or Guest card which acts as identification to the proximity readers fitted to each door and allows access to authorised users.

1.3 Controlled doors are located across the University estate including the following buildings:

- Residential Accommodation
- Teaching Rooms
- Laboratories
- Skills/Simulation Suites
- Offices
- Storage Facilities
- Service Buildings
- Catering provisions including Bar
- Students' Union

1.4 The system allows the University to:

- Register users
- Allocate doors and/or door groups to users
- Allocate time profiles to users
- Allocate time profiles to doors
- Record usage of user cards by automatically logging the time/date and door location each time the card is used.
- Remotely lock/unlock some doors

2. Objectives for the use of Access Control

2.1 The objectives for the use of the Access Control System are:

i. Assist in providing a safe and secure environment for the benefit of those who might visit, work or live on campus;
ii. Reduce the likelihood of opportunist crime;
iii. Reduce the fear of crime by reassuring students, staff and visitors that they are in a secure environment;
iv. Deter and detect criminal activity;
v. Assist in identifying, apprehending and prosecuting offenders in relation to crime and anti-social behaviour;
vi. Provide the Police and University investigators with evidence upon which to take criminal, civil and disciplinary action respectively;
vii. Limit access to certain buildings/rooms in the University;
viii. Reduce the requirement for manual locking/unlocking of buildings.

2.2 Access control data must not be used to generally monitor staff or student activity.

3. Administration of the System

3.1 The Assistant Director – Security & Operations retains responsibility for the Access Control system and delegates the day to day management to the Head of Security & Operations.

3.2 The Police may make application for data from the Access Control log which will only be released upon receipt of an appropriate GDPR request form, approved by the Head of Governance & Regulatory Affairs.

3.3 Personal data held on the Access Control system including patterns of usage may on occasion be released when it is considered that it is appropriate to do so under a relevant University procedure, for example Staff or Student Disciplinary Procedures. Requests for this data should be made to the Head of Governance & Regulatory Affairs in the first instance.

3.4 Reports showing who has access to what building or room and which buildings or rooms an individual has access to will be used for the management of the estate and to ensure access is appropriate. This data should be requested from the Assistant Director – Security & Operations, or the Head of Security & Operations. Reports on pattern of usage will not be provided.

3.5 Viewing of the data is limited to those with access to the SALTO software. The software is password protected. Viewing of this data is restricted to:

- Assistant Director – Security & Operations
- Head of Security & Operations
- Control Room Supervisor
- Control Room Operator
- Head of Governance & Regulatory Affairs (in the context of the approval of release of data as per paras 3.2 and 3.3)
- Certain members of the IT Department for maintenance purposes
- University contracted Access Control engineers for maintenance and installation purposes

4. Data Protection

4.1 The University is committed to complying with the requirements of data protection legislation (GDPR, Data Protection Act 2018) and will operate the system in accordance with the principles of data protection (GDPR Article 5):

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality (security);
- Accountability

4.2 All members of staff involved in operating the system will be made aware of the objectives of the system as set out in Section 2 of this Code and will be permitted only to use the system to achieve those objectives.

4.3 The University recognises the importance of strict guidelines in relation to access to and disclosure of data and all members of staff should be aware of the restrictions relating to this which are set out in this Code and the rights of individuals under data protection legislation.

5. Security of System

5.1 It is the responsibility of the Assistant Director – Security & Operations, or in their absence the Head of Security & Operations to:

i. Ensure the use of the system and data arising from the system complies with data protection legislation
ii. Be responsible for the control of the data and make decisions on how this can be used.

iii. Ensure the system is secure and only viewed by authorised persons

5.2 It is the responsibility of the individual operating Security Officer to:

i. Comply with the objectives outlined above
ii. Seek guidance from the Assistant Director – Security & Operations, or in their absence the Head of Security & Operations, before divulging any information from the system.

5.3 All Operators and other authorised users must read this Code of Practice prior to being instructed in the operation of the system.

6. Storing and viewing of data

6.1 All data is stored on the University servers.

6.2 In the event of a request from the Police for data an appropriate Data Protection request form must be provided (see 3.2 above).

6.3 Requests for data by University staff must be made in accordance with paragraph 3.3 and 3.4 above.

7. Disclosure of Data

7.1 The following guidelines will be adhered to in relation to the disclosure of data:

- It will be in line with the above objectives
- It will be controlled under the supervision of the Assistant Director – Security & Operations, or in their absence the Head of Security & Operations.
- A log will be maintained itemising the date, time(s) and data disclosed together with the reason for disclosure.
- The appropriate documentation from the Police will be filed for future reference

7.2 Any other requests for data not covered under Section 3 should be made to the Assistant Director – Security & Operations, or in their absence the Head of Security & Operations, who will consult the Head of Governance & Regulatory Affairs on the appropriateness of the release of the data.

7.3 The University has discretion to refuse any third-party request for information unless there is an overriding legal obligation such as a court order or information access rights. Once the data has been disclosed to third party, such as the Police, they become the data controller for their copy of that data. It is their responsibility to comply with the requirements of data protection legislation in relation to any further disclosures.

8. Complaints

8.1 Complaints in relation to the disclosure or data supply should be made in writing to the Head of Governance & Regulatory Affairs (the University's Data Protection Officer).

Item	**Detail**
Author	Head of Governance & Regulatory Affairs
Owner	Associate Director – Security & Operations
Approved by	VCEB
Approval Date	15th January 2020
Published	January 2020
Accessibility Checked	Yes – 3/12/19
Version number	1
Review Date	January 2023