Single ID Card Use Policy

Version Number 0.9

Effective from 1 December 2021

Author: Head of Security & Community Support
Estates & Facilities

Document Control Information			
Revision History incl. Authorisation: (most recent first)			
Author	**Summary of changes**	**Version**	**Authorised & Date**
T.Jones and D Grundy	Removal of temporary card issue.	V.09	11/11/21
T. Jones	New policy	V0.8	2012
Policy Management and Responsibilities:			
Owner:	The Director/Deputy Director of Estates and Facilities has the authority to issue, implement and communicate the Single ID Card Use Policy in a fair and consistent manner and has delegated responsibility to: • Head of Security & Community Support for day-to-day management and authorship of the policy; • E&F Admin Support Team to administer the process;		
Others with responsibilities (please specify):	Student Information Directorate (AskUS, University House) Library Staff, Clifford Whitworth		
Author to complete formal assessment with the following advisory teams:			
Equality Analysis (E&D, HR) *Equality Assessment form*	Submitted 2012		
Legal implications (LPG)	N/A		
Information Governance	Yes		
Academic Governance	N/A		
Consultation:			
Students via USSU			
Review:			
Review due:	1 August 2024		
Document location:	University Policy Pages at http://www.salford.ac.uk/policies		
The owner and author are responsible for publicising this policy document.			

1.0   Purpose

The purpose of this document is to specify the University of Salford (the University) policy on the issue, use and return of the University Single ID Card. This will help to;

- inform users of correct usage
- manage security requirements
- reduce potential for unauthorised access or use of the card.

2.0   Scope

The policy applies to all Single ID card recipients including students, staff, associates and contractors (i.e. anyone in a valid contractual relationship with the University who requires on-site access as part of the relationship). The 'Single ID Card' replaces any previously issued proximity cards or library ID cards. This policy covers use of the card for the following purposes;

1. Building, room and limited areas access across University sites (which is the responsibility of Estates & Facilities)
2. Car parking access for which a charge is applied (which is the responsibility of Estates & Facilities)
3. Proof of the contractual relationship with the University for students, staff and approved contractors (responsibility of Student information Directorate, Human Resources and Estates & Facilities respectively)
4. Card holder identification for the Number 50 bus on Media City Bus routes
5. Library borrowing (which is the responsibility of the Library)
6. Printing functions (which is the responsibility of the Library)

Specific guidance on the above areas 1-6 is available from the responsible divisions.

The policy does not specify;

a. Physical security measures or access control rules for University sites and buildings
b. Rules on Library borrowing
c. Installation and management processes for the 'Single Card' card readers

Specific guidance covering aspects a-c above is available from the responsible divisions or in separate University policies.

3.0   Governance and Management

The Executive Director of Estates & Facilities is responsible and accountable for issuing the policy and ensuring it is appropriately implemented and communicated across the University. The Single ID Card Access Control system is owned and managed by Estates & Facilities. Responsibility for the management and issue processes associated with the ID Card will be delegated to a number of roles within the University

4.0   Policy Statements

4.1   ID card issue

All ID card issue will comply with the following principles;

1. All cards will include University name, magnetic strip and chip, card type e.g. staff or student, Cardholder name, expiry date (Security Staff only) and photograph taken by the University (except pool cards). The decision to accept photos taken by third parties rests with the issuing Division. The photograph must have a good likeness and may not be animated.
2. Estates & Facilities will issue staff, associate and contractor ID cards. Student Information Directorate will issue student ID cards. The Library will issue Library Community (visitor) ID cards.
3. Before any ID card can be created or issued, a source record containing relevant data must exist i.e. HR, Student and Associate databases. Separate requirements are in place for Contractor pool cards.
4. The ID card is unique to the card holder and is not transferable.
5. There should only be 1 card active per cardholder at any one time.
6. The ID card remains the property of the University at all times (not the individual user).

The ID card is valid until end of relationship with the University. For students, the expiry dates will be the anticipated end of the end of study at the time of the issue of the card. Security staff ID cards will be valid for a 3- year period, then updated.

4.2   ID Card Use

In order to gain access to University site and buildings card holders must comply with the following principles;

1. Card holders must carry the ID card with them when on campus.
2. Card holders must use the card responsibly as a form of ID.
3. Staff, Associates and Contractors must visibly display the ID card on their person, to assist in identification at all times when on University premises.
4. Card holders must show their ID card on request to University personnel e.g. Security or Library staff.
5. Card holders should be prepared to challenge any unknown or unidentified people within their own departmental/School areas in University buildings, requesting to see the unknown person's ID card. The card holder can request support from Estates Security officers to escort the individual(s) from the building (or relevant security staff in Media City UK).
6. Refusal by a card holder to show his / her ID card may result in disciplinary action.
7. Card holders must not sell or lend the card to other people (internal or external to the University),or attempt to masquerade as another cardholder.

8. Card access to buildings, rooms and limited access areas is programmed according to business and security requirements. All requests for additional or amended access (with the appropriate building controller approval) should be directed to Estates & Facilities Services by emailing Estates-SupportTeam@salford.ac.uk.

4.3 Stolen, Lost and Replacement ID Cards

1. Any found student cards must be immediately sent to, AskUs, University House. Any found Staff cards must be sent to Estates Reception, Maxwell building.
2. Card holders must immediately report loss or theft of card during core office hours to;
   a. AskUs, University House (students)
   b. Estates & Facilities Services, estates-supportteam@salford.acd.uk (Helpdesk ext 54444)- (Staff & Contractors)
   c. Out of core office hours to Maxwell Security hub (ext 54773).
3. Card holders must report stolen ID cards directly to Maxwell Security hub (ext 54773)
4. Estates & Facilities will disable cards after they have been reported lost or stolen.
5. Card holders are responsible for the security of their own issued card. Card holders are also personally liable for the cost of a new card (£10) in the event of loss.
6. Stolen ID cards will be replaced free of charge where the crime has been reported and he/she has been issued a crime reference number.
7. There is no charge for issue of a new card where the person's name has changed or appearance has significantly changed. Their old ID card must be returned

4.4 Card return, deactivation and termination

1. Card access will be automatically terminated at the end of the card holders relationship with the University (i.e. employment, contract or study period) based on data from the source record.
2. Card holders must return the ID card at the end of this period to Estates & Facilities. The card can also be returned via the Line Manager, Tutor or other relevant staff. Card return must be in person or by securely sealed envelope - not by transit envelope.
3. ID cards may be manually deactivated (and the card required to be returned) if the card holder is;
   a. on long term leave
   b. suspended pending or following investigatory, disciplinary or fitness to practise proceedings
   c. banned from University sites
   d. dismissed (staff) or expelled (student) from the University.
4. Human Resources (staff), GSU and / or the relevant School (student) will have appropriate procedures to notify Estates & Facilities (specifically by email to Head of Security & Community Support (or Deputy)) of such circumstances in a timely manner.

5. Deactivated ID cards will be destroyed after 3 months, unless there is an ongoing investigation or disciplinary action.
6. The ID card can only be confiscated by appropriate University personnel (i.e. people in positions of line management, HR staff and Security staff) and official law enforcement agencies.

4.5   Retention of ID card and door access data

ID card records are retained for 2 years after cardholder's relationship with the University has ended. After this period the record will be deleted.
Records of ID card history are generally retained for 3 months.

5.0   Policy Enforcement and sanctions

5.1   Monitoring

Occasional and/or systematic monitoring of card usage and access records may be carried out for the purposes of;
- Checking compliance with the policy
- Checking accuracy and relevance of access rights
- Checking correct operating of the system
- Reporting purposes (such as room usage, traffic flow etc.)
- Supporting investigations or disciplinary matters.

All monitoring will be carried out in line with the requirements of the Data Protection Act 1998. All requests for ID card activity reports (by individual(s) or by door/area) must be directed in writing to the Head of Security & Community Support (or Deputy). ID card activity reports will not be provided from any other source. In relation to individual ID card activity reports the following procedures will be in place;

1. In the case of investigations or disciplinary action an ID Card Investigation Authorisation form (Appendix 1) must be completed as part of the investigation and then appropriately authorised (HR for staff or relevant Head of School for students). This should be sent to the Head of Security & Community Support (or Deputy) for further action. Completed forms will be securely stored with strictly limited access (subject to legislation) for 7 years from end of case.

2. In the case of police (or other law enforcement agency) investigations, information will be provided in line with existing information sharing protocols and / or Data Protection disclosure requests for the purposes of;
   - Prevention or detection of crime
   - Apprehension or prosecution of offenders

Failure to comply with the above procedures may lead to disciplinary action.

5.2   Misuse and Sanctions

Failure to comply with this policy will be investigated in accordance with the relevant University Disciplinary Policies. Sanctions for violations of this policy may include;
- Informal and formal Disciplinary Policy sanctions

Any fraudulent card use may be reported to the Police for investigation and further action

6.0   Related Documentation

- Estates Security Assignment Instructions (for controlled distribution and readership)
- Staff and Student Disciplinary Policies (via University Policy Pages)
- Data Protection Policy

Controls addressed in this policy from ISO/IEC 27001:2005 Information Security Management Systems – Requirements

8.3.2	Return of assets
8.3.3	Removal of access rights
9.1.2	Physical entry controls
15.1.4	Data Protection and privacy of personal information
15.2.1	Compliance with security policies and standards

7.0   Appendices

Appendix 1: ID Card Investigation Authorisation Form

ID Card Investigation Authorisation form V1.0

In line with the Single ID Card Use Policy, this form **must** be completed when requesting any individual ID card activity reports. The requester should obtain relevant authorisation (HR for staff or relevant Head of School for students) **before** sending the form to the Head of Security (or Deputy) for further action. This form **does not need to be completed** for general requests to check door access rights.

A)	Details of person making the request	
Name (in capitals):		**School/PAS:**
Role:		**Phone ext:**
Signature:		**Date:**

B) Details of cardholder(s) to be investigated (staple numbered continuation sheet if more than 1 cardholder)
Name (in capitals):
School/Division:
Building

C) Purpose of request and details of alleged activity
Reason for investigation:
Date, time and nature of alleged activity**:**

D) Authorisation by HR (for staff) or relevant Head of School (for student)	
I approve / do not approve (circle as relevant) the investigation to proceed as detailed above. I confirm that I am acting in accordance with University Policy.	
Name (in capitals):	**Signature:**
Role and School:	**Date:**

E) Authorisation by Head of Security (or Deputy)	
I authorise /do not authorise (circle as relevant) the investigation to proceed as detailed above. I confirm that where relevant I have obtained advice from the University Data Protection Officer and that I am acting in accordance with University Policy.	
Name (in capitals):	
Signature:	**Date:**
Send completed form in a securely sealed envelope to Head of Security & Community Support (or Deputy), Maxwell Security Hub.	