




The Open University

Control of Access to Premises Policy

Issue	Prepared By	Date	Description
10.0	Peter Ling	Sept 2021	Annual Review
11.0	Peter Ling	Nov 2022	Annual Review
12.0	Peter Ling	Nov 2023	Annual Review
13.0	Peter Ling	Jan 24	Annual Review

Approved for Distribution



Date: 02/01/2024

By:

If not signed above, then document is for reference purposes only, not for distribution and not subject to amendment control.

CONTENTS

		Page
	Foreword	4
1	Introduction	5
1.1	Policy Statement	5
1.2	Expectations	5
2	Control of Access	6
2.1	Entry / Exit Points	6
2.2	Issue / Authority	6
3	Visitors	6
3.1	Description	6
3.2	Visitor Responsibilities	6
3.3	Host Responsibilities	6
4	Cards	7
4.1	General	7
4.2	Issuing / Types	7
4.3	Leavers	8
App 1	Temporary Card / Key Log	9

Foreword

It is important for the security and safety of all members of the University and its visitors that the University is able to confirm the identity of anyone on its premises.

The principal mechanism used to identify members of the University is the Open University ID Card, which holds basic information including a photographic image. The Open University Card is a multi-purpose card which staff, contractors, research students and some visitors use while working for or on behalf of, or studying at, The University.

This Policy sets out the measures and responsibilities that allow all staff to ensure that staff, contractors, students and visitors in any University buildings or campus facilities have a legitimate reason to be there in order to work towards ensuring a safe environment for all. It also outlines the processes applicable to controlling access to University premises and supports the University's compliance with regulations and standards applying to its business operations.

The Policy will be reviewed annually taking into account feedback on its operation and the wider security context.

Dave Hall

University Secretary

1 Introduction

1.1 Policy Statements

The University seeks to ensure, as far as is reasonably practicable, the security and safety of all staff, students, visitors and contractors, whilst within or situated on University premises along with compliance with regulations and standards applying to its business operations. The Government's 'Prevent' strategy places a duty upon the University to have "due regard to the need to prevent people from being drawn into terrorism". The University's Codes of Practice in relation to Freedom of Speech and Events, should be read in conjunction with this document. It sets out the University's approach to arrangements and conduct at meetings and other activities held on University premises.

The Security Team is responsible for the effective operation and enforcement of the Security policies and procedures. Responsibility for security and personal safety rests with all persons who study, work or reside in, or who visit the University properties. All members of staff, students, visitors and contractors should assist the Security Team to ensure the success of the Policy. Security and personal safety is everyone's responsibility and cannot be left solely as a matter for the Security Team or Police. The University reserves the right to prosecute and/or take appropriate disciplinary action against any person who acts negligently, dishonestly, or commits a crime against the University.

All staff and students are required to carry their Open University Card when on University premises and to produce it if requested.

Open University Cards will occasionally be issued to contractors and other visitors working at the University. Any person issued with an Open University Card will be subject to the principles and procedures outlined in this policy in the same way as staff and students.

Staff are encouraged not to allow visitors access to buildings without displaying a valid ID or visitor's badge. If in doubt, staff are advised to contact Security on 01908 653666 (Ext 53666).

NB: Staff who are not part of the University's Security Team are advised not to put themselves at risk by attempting to detain individuals who they suspect are on University premises under false pretences. Instead staff are advised to contact their line manager or colleagues for support. Walton Hall staff should contact the University's Security Team on 01908 653666 (Ext 53666).

Managers have overall responsibility for visitors who enter their areas of authority. It is a management responsibility to ensure that this procedure is fully complied with and that any problems have been adequately resolved at the earliest opportunity and before visitors are permitted to proceed with their intended activity.

1.2 Expectations

We are committed to creating a diverse and inclusive work environment in which everyone feels safe and valued. Bullying, harassment, or victimisation of any kind across our university is unacceptable.

The Open University expects that:

- All persons on its premises will at all times adhere to the University's rules of behaviour as set out in its regulations, policies and procedures.

- All persons on University premises will comply with any reasonable request to provide proof of their identity and all Open University Card holders will be expected to produce this card as proof of their identity.

2 Control of Access

2.1 Entry/Exit Points

All external entry and exit points should be secured on a 24/7 basis unless staffed. No unattended points giving access to a building should be left insecure and unattended, excepting common areas such as foyers of building where further internal access control measures are in place. Owing to the high recurrent cost of guarding and receptionists this requirement will generally be met by the provision of electronic access control or suitable mechanical locks taking into account emergency exit requirements.

2.2 Issue Authority

The Security Team do not grant/deny authority for people to access areas. This is performed by the department access authoriser appointed by a Head of Unit or persons responsible for the area concerned, who also perform the same function relating to the issuing of keys. The Security Team carry out the requests of the department access authorisers or persons responsible for areas in relation to access card and key requests.

No access cards or keys should be issued without the authority of a department access authorisation signatory or OU manager responsible for a contractor.

3 Visitors

3.1 Description

The term visitor refers to a contractor, vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. It does **not** refer to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the University's premises for longer periods or on numerous repeat occasions such as named personnel of term contractors.

3.2 Visitor Responsibilities

All visitors are expected to conduct themselves in a professional and respectful manner to match the theme and tone of the institution/event they are visiting.

The University does not abide or tolerate any form of harassment, victimisation or discrimination in any form, including where it is verbal, physical, or on the basis of age, disability, ethnicity, gender reassignment, marital status, pregnancy or maternity, religion or belief, sex, or sexual orientation.

3.3 Host Responsibilities

- Wherever practicable, advance notice of visitors should be given by hosts to reception points.
- All visitors must first report to a reception point or Security.
- All visitors must sign in at a reception point and wear their identity badge at all times whilst on site.
- The receptionist/Security will notify the receiving employee of the visitor's arrival.

- The receiving employee must arrange to collect the visitor.
- All visitors must be accompanied or supervised by a member of staff at all times whilst on site. (Supervision can be classed as maintaining a visual awareness of the visitor's activities)
- The visitors badge must be returned to reception/Security at the end of the visit and the visitor sign out.
- Where reception points are closed, visitors must leave badges at the reception desks.
- Visitors attending site for more than one day must sign in and sign out each day.
- For visitors such as non-regular contractors working on behalf of University departments remote from the area in which the work is required to be carried out, host responsibilities will fall to the department in which the work is being undertaken whilst in their area.

4 Cards

4.1 General

Card controlled barriers/doors are an effective method of preventing unauthorised access. All staff are issued with a University card which is used as an identity card, a Library member card and access control card for certain areas. These cards should be regarded in security terms as equivalent to a key. Cardholders must safeguard their card and report any loss to the Security team as soon as possible, so that card access can be cancelled. University cards are not transferable and holders must not loan their card to other persons for means of access or any other purpose. Disciplinary action may be taken if a crime results from misuse of University cards.

4.2 Issuing/Types

- **Paper (VisitorNet) daily visitor passes.** These should be issued to visitors and contractors who will be on site for up to 5 days and have no requirement for access. These should be issued on a daily basis from the reception points on site. These passes give basic health and safety information and do not grant access to any areas. These should be returned at the end of each day.
- **Short term visitor passes.** Departments, (usually the key authorisation signatory), will be responsible for issuing these to visitors and contractors who will be on site for between 1 and 28 days (6-28 for non-access cards) along with appropriate H&S guidance, from a supply of passes issued to them by Security. A log should be kept relating to the temporary holder's details (see attached template Appendix 1). Access privileges for these cards will only be activated by Security on receipt of an e-mail from the access authoriser with details of the required access and an expiry date for the card. Alternatively, Security can issue these cards following an e-mail request from a department access authoriser.

In either case a maximum expiry period of 28 days will be allowed on these cards. Longer periods should be dealt with by issuing a long term visitor card. If however during the 28 day period it becomes evident that the visitor/contractor will require a longer stay, an extension of the card expiry date can be arranged by the authoriser sending a further e-mail to Security towards the end of the initial 28 day period.

Daily checks should be made at the end of each day to ensure all temporary visitors access cards issued are returned by the due dates. Any missing cards should be suspended by notifying Security. Department access authorisers should be contacted by Security to chase the return of missing cards and keys not issued by departments. The Security team check with the access authorisers on a monthly basis to ensure all cards can be accounted for. Any not accounted for will be permanently deleted from the system.

- **Photographic long term visitor passes.** These are issued at the Security Lodge for visitors or contractors who will be on site for more than 28 days. These should be applied for by departmental access authorisers in the same manner as staff identity/access cards and on the same form. These cards will be programmed with the required access level and a maximum expiry date of 6 months, subject to appropriate department authorisation. Long term visitor access passes for contractors should be issued via OU contract managers, who will be responsible for their issue and return. 3 monthly validation exercises will be carried out on these cards via the OU contract manager. H&S guidance should be covered by the department responsible for the visitor/contractor at the time of issue.
- **Photographic long term access passes.** These are issued at the Security Lodge and apply to permanent staff members along with post graduate research students, including part time, and should be applied for by departmental access authoriser on the correct form available on the intranet. These cards will be programmed with the required access level, subject to appropriate department authorisation.

4.3 Leavers

Departmental access authorisers and/or contract managers must inform Security in the event of a visitor, contractor or staff member leaving prior to expiry of the card and the card returned/cancelled. A monthly check of leavers is carried out in conjunction with People Services.

For further information about this policy and for any queries please contact the Security Manager on 01908 858507.

Access Card & Temporary Key Log Sheet

Keys and Cards to be Booked Separately

Card No.	Key No.	Issued to Name (PRINT)	Issued to Signature	Department or Company	Contact Number & Authoriser/ Host Name	Issued by	Issue Date	Issue Time	Expiry Date	Return to	Return Date	Return Time