Premises Access Control Security Policy

For the

County Hall Complex Matlock

Version 11.0

Version History			
Version	**Date**	**Detail**	**Author**
1.0	09/11/2014	Draft completed for distribution	Chris Martin
2.0	11/11/2014	Draft update	John Eade
3.0	21/11/2014	Draft update	Chris Martin
4.0	04/12/2014	Draft update	John Eade
5.0	07/01/2015	Final	Chris Martin
6.0	09/05/2017	Reviewed by Information Governance Group. ACD contacts and door change dates amended.	Jo White
7.0	27/10/2017	Contact for finance amended.	Jo White
8.0	08/01/2018	Contacts for Children's Services Chatsworth Hall added.	Jo White
9.0	05/02/2018	Amendments to finance contact.	Jo White
10.0	06/08/2018	Reviewed by Information Governance Group. Amendments to Door Access Code Managers.	Jo White
11.0	10/09/2019	John Hadfield House now included.	Jo White

This document has been prepared using the following ISO27001 standard controls as reference:	
ISO Control	**Description**
A.9.1.1	Access Control Policy
A.11.1	Secure Areas

Contents

1 Introduction

The object of this policy is to provide a secure curtilage around the council premises and for the protection of the employees within the County Hall Complex. The County Hall Complex comprises County Hall, Chatsworth Hall, John Hadfield House and Shand House. The security system will control access through both external and some internal doors. The system will provide a secure barrier between the public areas and the workforce and provide authorised staff entrances and public entrances.

The system will provide confidentiality and integrity governance for the fundamental aspects of the protection of employees and information within the council and is achieved through physical procedural controls. Authorised users who have access to the Council buildings and information, are aware of and understand how their actions may affect security.

Property – systems and information are physically secure and will be accessible to authorised persons.

Confidentiality – access control systems and associated information will only be accessible to authorised persons.

Integrity – the accuracy and completeness of the systems and information are safeguarded.

Authorised users referred to in this document are members of the following groups:-

- All employees (either as part of a contract of employment or third party contract) who have access to the County Hall complex, or are under the control of the Council including:

    - Council employees
    - Elected Members
    - Third Parties
    - Full and part-time staff
    - Temporary staff
    - Agency staff
    - Vulnerable and physically impaired staff
    - Partner organisations

2 Purpose

The purpose of this policy is to ensure that both physical access to buildings and the security of the building and its information and systems is controlled; and that procedures are in place to ensure the protection of employees, information and systems.

3 Cancellation or Expiration

The processes and statements in this document do not have an expiry date. However, this document is reviewed and updated annually, and is maintained in the Electronic Document Records Management system (EDRM).

4 Scope

The scope of this policy includes:

- all physical access to all buildings on the County Hall complex;
- the access to areas and locations where employees and information is located;
- The procedures and policies to administrate the systems.

This policy applies throughout the employee's period of employment.

5 Policy Statement

On-going education featuring corporate induction programmes, eLearning, line manager training, specific training and awareness programmes will be undertaken by staff to enable them to be aware of their responsibilities towards systems and information security.

6 Access Code Considerations

First grade of access (Grade 1) through a controlled doorway should be carried out by secure validation of a user authentication. As a minimum this should entail the use of a four digit access code issued by the security office once a month.

Second grade of access (Grade 2) will be an electronic fob / proximity card.

Third grade of access (Grade 3) will be by means of a proximity ID card and a 4 digit authorisation code.

Grade 2 & 3 are currently under review.

The access code once issued, should not be copied, shared or written down.

7 Physical Access and Control

Maintaining the physical security of premises where information is located is vitally important. There must be methods of physically securing access to areas of the County Hall complex and protecting employees and information:

1. Staff should wear their Council ID badges at all times whilst on the premises. People who are not displaying ID badges should be challenged. Any person not known to location personnel should be

challenged in order to establish who they are and whether authorisation has been provided for them to be there. If there is any doubt about the identity of the individual, the appropriate security officer/manager should be contacted to confirm the individual's identity.

2. County Hall Complex staff will be issued with a four digit access code and shall be made aware of the requirements within this policy.

3. At County Hall Complex sites, all visitors; except those attending meetings within the public meeting rooms; must wear a Visitor ID badge which is issued from the Main Reception on arrival. Appropriate recording mechanisms will be in place to record the names, dates, times and signatures of visitors.

4. All contractors must wear a Contractor ID badge which is issued from the Main Reception. Appropriate recording mechanisms will be in place to record the names, dates, times and signatures of contractors. All contractors shall further be required to sign for and be allocated with an access fob from the Facilities Management Reception (Room 78 behind Main Reception). Appropriate recording mechanisms will be in place to record their name, company and contact address against the registered access fob number including date and time of issue. In all instances access fobs allocated to contractors shall be returned to Facilities Management Reception before the individual leaves site.

5. Access fobs will be issued to authorised employees on an individual basis, i.e. physically impaired employees and employees that carry out business critical procedures. Appropriate recording mechanisms will be in place to record their names and employee numbers against the registered access fob number including date and time of issue.

6. Access fobs should only be used by the registered user and must not be lent out or given to other employees, regardless of their seniority.

7. Access fobs issued to employees who leave the employment of the Council must be deactivated and recovered immediately – a record of this action must be kept, using an official recording system

8. Locations housing critical or sensitive information and/or information processing facilities should have a secure, physically sound perimeter with suitable controls and restrictions allowing access to authorised staff only. CCTV and audible alarm systems may be used where sensitive information is located, such as in the data centre and the confidential waste process areas (Hopewell Road).

9. Privilege to use the access control system software will only be granted to staff following any required legal/council checks. Usage policies will also need to be signed by the appointed staff.

10. All interfaces used for managing physical access to the premises must be robust and secure.

11. Access to and knowledge of key fobs, door lock codes or access to keys for locks, is restricted to authorised personnel only and must not be shared with any unauthorised person.

12. Door access codes must be changed on a regular basis as specified by the governance policy/insurers and in line with professional best practice, i.e. once every month.

13. Direct access to secure locations, or access to adjoining offices which could provide access, must be secured using appropriate locking mechanisms.

14. All Council/Contracted Cleaners must have and display appropriate identification. Cleaners will be issued with a four digit access code and shall be made aware of the requirements within this policy.

15. Any access control equipment shall be sited to minimise unauthorised access. For example, electrical power supplies, network points and fire alarm relays shall be sited on the secure side of the door at an appropriate height and shall be placed in areas not accessible to the public.

16. Access through the doors should only be attempted using the authorised access code in accordance with Council policies.

17. Following successful access the user shall ensure that the door is not left open, no person(s) have tailgated and the door closes securely behind them.

8 Communication – Departmental Access Code Managers (DACM)

The access codes will be changed monthly on the first Monday of the month.

The access codes will be randomly generated on the Wednesday prior to each change by the Facilities Manager. This will apply to all of the access codes on site, including the ones previously installed and administered by individual departments.

The new access codes will be communicated by the Information Security Manager to “Designated Access Code Managers” (DACM) via email as soon as they are generated.

All general staff areas in County Hall will have the same access code.

Remote buildings’ main entrances, such as the Stable Block, Business Centre, The Lodge, Central Buildings, Rutland Street and Co-op Block will

have the same access codes as the County Hall Complex. Areas which require enhanced measures will have different access codes i.e. Audit Block, Derbyshire Dales Area Office (Gym) and the Legal Department.

Departmental access code managers (DACM) and reserve access code managers will be nominated by each departmental head. DACM's will inform their staff of the new access codes via email prior to the first Monday of the month.

All the door access coded locks will be reformatted by the commissionaires on the Sunday night prior to the first Monday of the month.

Anyone absent from work when the access code emails are sent out shall report to Main Reception to obtain the new access code on production of their personal DCC ID badge.

Departmental Access Code Managers (DACM)					
Department	**Name**	**Reserve(s)**	**Responsible For**	**Telephone**	**Email**
Adult Care	Patrick Kerr	Sue North	Responsibility for disseminating to staff the access code throughout the department	31312	patrick.kerr@derbyshire.gov.uk
				32185	susan.north@derbyshire.gov.uk
Call Derbyshire	Eileen Paing	Vanessa Rogers	Responsibility for disseminating to staff the access code throughout the department	33150	eileen.paing@derbyshire.gov.uk
				33175	vanessa.rogers@derbyshire.gov.uk
CCP – Members & Policy	Michelle Archer	Beverley Heath	Responsibility for disseminating to staff the access code throughout the department	36002	michelle.archer@derbyshire.gov.uk
				36022	beverley.heath@derbyshire.gov.uk
CCP – Trading Standards (Business Services)	Dawn Brooks	David Rudkin	Responsibility for disseminating to staff the access code throughout the department	39264	dawn.brooks@derbyshire.gov.uk
				38843	david.rudkin@derbyshire.gov.uk
Economy, Transport and Environment	David Massey	Kay McIntyre	Responsibility for disseminating to staff the access code throughout the department	38111	david.massey@derbyshire.gov.uk
				38189	kay.mcintyre@derbyshire.gov.uk
Children's Services	Sharon Elliott	Hayley Hurst	Responsibility for disseminating to staff the access code throughout the department	37179	sharon.elliott@derbyshire.gov.uk
				32409	hayley.hurst@derbyshire.gov.uk
		Adam Addis		36410	adam.addis@derbyshire.gov.uk
Children's Services Chatsworth Hall	Mel Moore	Lynn Steventon		35695	melanie.moore@derbyshire.gov.uk

			Responsibility for disseminating to staff the access code throughout the department	35896	lynn.steventon@derbyshire.gov.uk
		Anne Wright		36568	anne.wright@derbyshire.gov.uk
Corporate Finance	Mick Crawford	Brenda Rarity	Responsibility for disseminating to staff the access code throughout the department	39232	michael.crawford@derbyshire.gov.uk
				39197	brenda.rarity@derbyshire.gov.uk
		Samantha Woolley		38733	sami.woolley@derbyshire.gov.uk
Corporate Property	Jo Hollick	Chris Cooper	Responsibility for disseminating to staff the access code throughout the department	36290	jo.hollick@derbyshire.gov.uk
				36722	chris.cooper@derbyshire.gov.uk
ICT Services	Jo White	Sarah Wheeldon	Responsibility for disseminating to staff the access code throughout the department	32147	jo.white@derbyshire.gov.uk
				36959	sarah.wheeldon@derbyshire.gov.uk
Corporate Business Centre	Steve Harrison	Ashley Cook	Responsibility for disseminating to staff the access code throughout the department	35757	steve.harrison@derbyshire.gov.uk
					ashley.cook@derbyshire.gov.uk
		Laura Richford		35737	laura.richford@derbyshire.gov.uk
Legal Services	Sue Marsh	Andrea Dyson	Responsibility for disseminating to staff the access code throughout the department	38273	sue.marsh@derbyshire.gov.uk
				38307	andrea.dyson@derbyshire.gov.uk
Human Resources	Sue Rose	Chloe Jackson		36911	sue.rose@derbyshire.gov.uk

			Responsibility for manage the disseminating to staff the access code throughout the department	36911	chloe.jackson@derbyshire.gov.uk
Facilities Delivery Section	Wendy Pugh	Dawn Watson	Responsibility for manage the disseminating to staff the access code throughout the Facilities Management department	39955	wendy.pugh@derbyshire.gov.uk
				38399	dawn.watson@derbyshire.gov.uk
Facilities Management	Shaun Bowling	Karen Webster	Responsibility for ensuring the door code change is actioned each month.	38340	shaun.bowling@derbyshire.gov.uk
				36206	karen.webster@derbyshire.gov.uk
		Michael Baxter		07867 908165	michael.baxter@derbyshire.gov.uk
John Hadfield House – HR	Michelle Hallsworth	Jayne Mason	Responsibility for ensuring the door code change is actioned each month.	32778	michelle.hallsworth@derbyshire.gov.uk
				32915	jayne.mason@derbyshire.gov.uk
		Christine Vaughan		32848	christine.vaughan@derbyshire.gov.uk
John Hadfield House – Children's Services	Lena Drabble	Julie Mellon	Responsibility for manage the disseminating to staff the access code throughout the Facilities Management department	32712	lena.drabble@derbyshire.gov.uk
				32821	julie.mellon@derbyshire.gov.uk

9 Annual calendar of code changes

Month	Access code disseminated to DACM staff	Date of operation	Time of operation
January 2019	January 2nd	January 7th	7.00am
February 2019	January 30th	February 4th	7.00am
March 2019	February 27th	March 4th	7.00am
April 2019	March 27th	April 1st	7.00am
May 2019	May 1st	*May 7th	7.00am
June 2019	May 22nd	June 3rd	7.00am
July 2019	June 26th	July 1st	7.00am
August 2019	July 31st	August 5th	7.00am
September 2019	August 21st	September 2nd	7.00am
October 2019	October 2nd	October 7th	7.00am
November 2019	October 30th	November 4th	7.00am
December 2019	November 27th	December 2nd	7.00am
January 2020	December 23rd	January 6th	7.00am

*Denotes Bank Holiday

10 System/Information De-registration

1. If a member of staff changes role or their contract is terminated, their manager shall apply to have the user's access to the system/information reviewed or removed as soon as possible.

2. If a member of staff is deemed to have contravened any of the Premises Access Control Security policies or procedures, potentially jeopardising the confidentiality or integrity of any systems or information, their access rights to the system/information shall be reviewed by their departmental management.

3. If it is deemed that it is no longer appropriate or necessary for a user to have access to systems then the user's manager shall inform the Information Security Manager (01629 532147) that access rights are to be altered/removed immediately.

4. If any system/information rights are altered or removed, the relevant documentation will need to be updated accordingly.

11 Emergency Evacuation

In the event of an emergency which activates the fire alarm, all egress and exit doors will ‘fail safe’ and automatically release. All egress and exit doors will automatically reset and lock on completion of the resetting procedure of the fire alarm system. The evacuation procedure will not require any employees’ intervention to release the door. It is the employee’s responsibility to ensure that they evacuate through the nearest emergency exit.

12 Responsibilities

Directors are responsible for ensuring that all staff and managers are aware of security policies and that they are observed. Managers need to be aware they have a responsibility to ensure staff hold sufficient, relevant knowledge concerning the security of information and systems.

Designated owners of security systems; who have responsibility for the management of these systems and inherent information, need to ensure that staff have been made aware of their responsibilities toward security. Designated owners of systems and information need to ensure they uphold the security policies and procedures.

13 Breaches of Policy

A breach of this policy can be defined as an event which could have, or has resulted in, loss or damage to Council assets, or is in breach of the Council’s security procedures and policies.

All Council employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council’s Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the information systems of the Council.

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.