# Physical and Environmental Security Policy

**Corporate Information Governance Group**
**Physical and Environmental Security**

## Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

## Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

# Physical and Environmental Security

## General Information

- Always display and present a valid ID card or name badge.
- Challenge anyone who is not wearing a valid ID card or name badge.
- Do not allow anyone into the staff areas who is not displaying a valid ID card.
- Do not allow anyone to use your ID card.
- Never leave personal possessions or sensitive papers unattended. Lock them away or keep them out of sight.
- Do not leave Business Equipment unattended in unsecure locations.
- Close and secure all windows in your immediate work area when you leave the office at night. This is a staff responsibility and must not be left to the cleaners or caretakers.
- Internal staff doors are for staff access only and must be kept closed during public opening hours (8.30am – 5pm)
- External staff entry doors must be kept closed at all times. Do not leave these doors on the catch or prop them open.

## Out of hours access

- Please refer to the Out of Hours Access Procedure if you require out of hours access.
- For meetings involving external visitors held outside of public opening hours you will need to make arrangements for your visitors to gain access to the building. It is staff responsibility to ensure visitors are met and escorted to the meeting place and shown out of the building once the meeting has finished.
- Please email prior to the meeting so that arrangements can be made with the on-duty caretaker for locking up the building.

## Visitors

- All visitors must be signed in at main reception and issued with a visitor's pass, which they must display.
- When your visitor leaves the building, please ensure they are 'signed out' and their visitor badge is returned.
- If your visitor is here outside of public opening hours (after 5.00pm), you must escort your visitor safely out of the building.
- Remember, you are responsible for your visitors whilst they are in the building. Do not allow your visitor to wander unaccompanied in the staff areas.
- Where enforced, visitors with vehicles will need to display a car park permit from Main Reception if they have been unable to park in the Visitor Space.

### Contractors

- All contractors must either display a company ID badge or a temporary contractors ID badge/ card.
- Where enforced, contractors with vehicles will need to obtain a car park permit from main reception, which must be displayed in the vehicle.
- It is also advisable that the company or the individual contractors sign a copy of the confidentiality statement to ensure our information is protected.
- Where provided, contractors must park their vehicles in the designed contractor spaces in the staff car parks.
- If contractors are required to work outside of normal office hours, you must follow the Out of Hours Procedure for contractors.

### Deliveries

- Receipt of deliveries and onward movement to other offices are managed through the print and mail room, with the exception of ICT which is delivered directly to ICT.

### Emergency procedures

- Each council will have separate policies and procedures for managing an emergency which might impact on the security of council owned buildings and records. Examples include evacuation of the building, dealing with suspicious mail or packages or responding to a bomb threat.

## Maintenance of paper records

### 1. Overview

Each department must manage the council's records to ensure that:

- The council complies with the eight principles of the Data Protection Act 1998;
- Records meet the authority's business needs;
- Records are retained and then destroyed in accordance with departmental retention schedules;
- Records are destroyed using confidential disposal procedures when necessary; and
- The council conforms to any legal and statutory requirements relating to record-keeping.

Each department should have in place a record keeping system (paper or electronic) that documents its functions and provides for quick and easy retrieval of information. It must also take into account the legal and regulatory environment specific to the area of work.

The record keeping system must be maintained so that the records are properly stored and protected, and can easily be located and retrieved. Sensitive information should wherever possible be stored in a lockable cabinet.

## 2. Record Retention and Disposal

Records should be disposed of in line with the Information management policy. Therefore, departments must have in place clearly defined arrangements for the assessment and selection of records for disposal, and for documenting this work.

The system should ensure that appropriate records are reviewed and disposed of or transferred. Documentation of the disposal/transfer of records must be completed and retained. Records selected for permanent preservation are transferred to the appropriate location within the council's own offices.

## 3. Departmental responsibilities

1. There should be a clear understanding on the relationship between manual and electronic records. For example the appropriate use of shared folders, personal folders, email folders and paper filing systems. No 'corporate' information should be stored on personal directories or in personal files.

2. All staff should be familiar with the department's records management processes. It is recommended that a named person be responsible for the management of those processes.

3. Each division should have prepared a retention schedule detailing each record series. The retention schedule should state how long the records should be retained in the offices or in the records centre before disposal. It is recommended that records are reviewed against the retention schedule at least once a year.

4. Any sensitive records should be kept in a secure location. Where this is not feasible, staff should be made aware of the sensitivity of the information and be clear who is permitted access.

5. Staff should be made aware of the council's responsibilities under the Access to Information legislation and must comply with the Freedom of Information Act, Environmental Information Regulations and the Data Protection Act. The council is under a duty to respond to requests if the information exists in an accessible format, unless it relates to information which is exempt from disclosure.

## Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

| **Document Control** | | |
|---|---|---|
| **Title/Version** | - | Physical and Environmental Security |
| **Owner** | - | Corporate Information Governance Group |
| **Date Approved** | - | |
| **Review Date** | - | |
| **Reviewer** | - | |

**Revision History**

| **Revision Date** | **Reviewer (s)** | **Version** | **Description of Revision** |
|---|---|---|---|
| | Matthew Archer | 1.0 | First Draft for Consideration |
| 18/01/2016 | Hannah Lynch | 1.1 | Amended Version |
| 17/03/2016 | Dave Randall | 1.2 | Amended for Final Consideration. |
| | Hannah Lynch | | |
| 23/09/2016 | CIGG | 1.3 | Final Review |