THE FERGUSLIE GROUP

CLEAR DESK POLICY

Date Approved by the Management Board	28 October 2020 Signed:	Chairperson
Date of Next Review	OCTOBER 2023	

1. Overview

1.1 A clear desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an employee's workspace, and locked away when the items are not in use or when an employee leaves his/her workstation. It is one of the top strategies when trying to reduce the risk of security breaches in the workplace, and such a policy can also increase an employee's awareness about protecting sensitive information. In addition, a clear desk makes it easier for appropriate hygiene protocols to be followed, to minimise the risk of cross- contamination arising from the spread of any virus.

2. Purpose

2.1 The purpose of this policy is to establish the minimum requirements for maintaining a clear desk – where office desks are cleared for clearing/hygiene and where sensitive/critical information about our employees, our assets, our customers and our suppliers / contractors is secured, scanned and otherwise stored in locked areas, and out of sight.

2.2 With the move to electronic and homeworking, the amount of paperwork has been significantly reduced and staff will be required to:

- Keep all information in electronic formats
- Only print out essential paperwork
- Ensure that all 'hard copy' paperwork received is scanned as soon as possible and then the hard copy destroyed.

2.3 Hard copies should only be retained by exception and only where this needs to be retained for legal/audit etc. purposes. Finance, HR and Governance documents that are kept in hard copy must be kept in the locked cupboard in the Finance room. Tenancy agreements are stored in the upstairs locked room outside reception.

3. Scope

3.1 This policy applies to all Ferguslie Group employees and any consultant using our premises. The policy applies to working from the Association's offices, although the principles in relation to GDPR and data security should be followed when working from home.

4. Policy - General

4.1 With the exception of paperwork (see below), staff desks should be kept clear apart from:

- PC/laptop and stand
- Keyboard
- Mouse/keypad
- Telephone
- Hand sanitizer
- Clearing products or tissues
- A note pad and pen

4.2 Items such as staplers, tape dispensers, desk tidies etc. should be stored in an employee's filing drawers.

4.3 All personal items and stationery should be stored by staff in their lockable, storage cabinets – located under each employee's desk.

Policy - Paperwork

4.4 Employees are required to ensure that all information in hard copy is scanned and stored electronically.

4.5 Computers must be locked at all times when the employee's workspace is unoccupied. Where there has been no activity for 10 minutes, PC's and laptops have been set to automatically logout.

4.6 Computers, including interview room PC's, must be shut completely down at the end of the work day, and will be logged out following 10 minutes of activity.

4.7 As the Association's default position is that no hard copy information should be retained, there should be very limited hard copy information held by any employee. All sensitive or personal data that is received in hard copy and held by an employee must not be left unattended until scanned to a confidential location and the hard copy deleted.

4.8 Personal data, such as tenant or Board members' names, addresses, telephone numbers and email addresses, must not be displayed on any noticeboard in the Association office.

4.9 Where possible, staff should avoid having any sensitive or personal data in hard copy format in their possession when they are homeworking. Instead, employees should ensure that any such material is available electronically, where it will be protected through laptop passwords etc. Should any employee need to have such material in their possession at home, this should be discussed with their line manager in order that arrangements can be made for such data to be held securely.

4.10 Filing cabinets containing personal data must be kept closed and locked when not in use or when not attended.

4.11 Laptops must always be kept secure when at home. All files should be properly stored within the network drives, rather than on 'desktop' or in 'my documents' so that they are backed up every evening. Where spare laptops are not being used, they should be stored in the locked cupboard in the Finance room. Laptops must always be booked out using the register maintained by the Governance & Corporate Services Co-Ordinator.

4.12 Passwords must be appropriately protected by staff and not written down and left at or near any PC or laptop.

4.13 Printing should be avoided unless essential. Printouts containing any personal data should be immediately removed from the printer.

4.14 Personal or sensitive data should only be disposed of using the confidential disposal bins. Bins will be checked frequently by the Corporate Services department and arrangements made for disposal as necessary.

4.15 The use of storage devices such as DVD or USB drives should be kept to a minimum and must comply with the ITC Policy. Only encrypted devices should be used for transferring data, and should always be virus scanned prior to use. Any personal or sensitive data should be erased from such devices, as soon as this is no longer required. Portable storage devices containing such data should never be removed from the office.

5. Policy Compliance

5.1 The Association's Data Protection Officer will undertake periodic reviews to ensure compliance with this policy. Non-compliance will be notified to the relevant line manager.

5.2 Managers will ensure that incidents of non-compliance are discussed with the employee concerned. Any employee found to have breached this policy on a recurring basis may be subject to disciplinary action, in accordance with the terms of the Association's relevant policies.

6. Related Policies

6.1 This policy should be read in conjunction with the Group's other related policies including the Privacy Policy, ICT Policy, Employee Fair Processing Notices, Code of Conduct for Employees, and the Staff Handbook.