June 2015

Wheatley Group Clear Desk Policy

Policy Statement

This Policy, which is approved by the Group Board, is intended to support the Information Governance framework for the group comprising Wheatley Housing Group Limited and all of its subsidiaries ('the Group') for ensuring compliance with the relevant legislation, including the Data Protection Act 1998 (DPA) and any subsequent or related laws. To this end, the Group will:

- Regard Information Governance and compliance with DPA and information security as a key organisational activity,
- Raise awareness of and ensure compliance with this Policy;
- Define the responsibilities of those involved in information governance and provide training to ensure that these responsibilities are carried out successfully;
- Regularly review the Group's compliance with the Data Protection Act (DPA) and the Data Protection Principles which it enshrines, and information security to ensure this Policy remains appropriate to its needs.

This Policy provides a clear statement of our commitment to ensure that information is securely held and stored by the Group.

Signed: _____

Title: _____

Effective Date: _____

1. Introduction and Background

1.1 The Wheatley Group Clear Desk Policy is intended to improve security and protect confidentiality of information within the group comprising Wheatley Housing Group Limited and all of its subsidiaries ("the Group"). It is our commitment to a high standard of information security and a mandate for action to achieve this.

1.2 The establishment of a Clear Desk Policy is recognised as good practice in line with the principles of the ISO 27001: 2013 standard for information security management.

1.3 This Policy covers the Group as a whole. All employees (whether permanent or temporary), agency workers, contractors, consultants, modern apprentices, secondees, work experience placements and all visitors to and / or working in or from Group business premises shall comply with this Policy.

2. Scope

2.1 This Policy is designed to safeguard the physical security of physical information assets (such as papers and removable storage material) and electronic information assets through clear screen policy provisions. This is to reduce the risk of unauthorised access to, loss of, and / or damage to information during and outside normal working hours or when areas in which information assets are stored or accessible are left unattended.

3. Aims and Objectives

3.1 Information security and data protection compliance are an integral part of our day-to-day work. The Group holds a wide range of sensitive information, both of a personal and a commercial nature. We have a duty to protect this information and ensure it is not seen or accessed by people (whether internal or external to the Group) without the authority to do so.

3.2 Aims

The key aims of this Policy are to:

- reduce the threat of security breach and information theft by ensuring physical information is securely stored / locked away;
- ensure compliance with the Data Protection Act (DPA) by keeping personal information secure;
- reduce the possibility of identity theft as a result of data loss;
- reduce the risk of a breach of customer, supplier or stakeholder confidentiality;
- reduce the risk of theft of information, including intellectual property;
- ensure the Group is taking appropriate corporate responsibility for the personal data and business sensitive information in its care;
- manage records effectively through their lifecycle from creation through to disposal;
- maintain an acceptable office appearance; and
- meet health and safety considerations.

3.3 Objectives

In order for effective information security and data protection compliance to be successfully embedded, our objectives are to:

- promote an organisation-wide awareness of protecting the security and confidentiality of information;
- adopt a uniform approach protecting the security and confidentiality of information which is captured through our performance management system;
- ensure that senior management take individual responsibility to effectively protect the security and confidentiality of information across the Group and within each subsidiary;
- ensure that all staff are aware of what they must do to protect the security and confidentiality of information; and
- promote continuous improvement of the effectiveness of security measures.

Organisational Benefits

4.1 There are many benefits to be gained by embedding this policy into our culture and across the Group. These include:

- supporting the Group's business and discharge of its functions;
- supporting good governance;
- supporting compliance with other legislation and regulations which requires personal information and/or business information to be securely kept, controlled and accessed;
- improving accountability and enabling compliance with legislation and other rules and requirements to be demonstrated;
- protecting the rights and interests of the Group, its customers, staff and stakeholders';
- protecting the Group's reputation and brand image
- protecting the Group's assets; and
- the safety and wellbeing of our staff.

5. Roles and Responsibilities

5.1 To improve security and protect confidentiality of information, it is essential all management and staff take on an appropriate level of responsibility and comply with this Policy.

5.2 It is incumbent upon **all teams and employees** to:

- achieve and demonstrate an adequate level of general awareness of information security and confidentiality;
- familiarise themselves with and adhere to the key procedures, practices and guidance; and
- participate actively in information security and exercises when required.

5.3 **Group Directors** have overall responsibility for information security and confidentiality within their business division.

5.4 All **Board and Committee Members** who, during the course of their duties, deal with personal data must comply with this Policy.

5.5 The **Company Secretary** has particular responsibility for maintenance and implementation of this Policy to ensure that the Group complies with its legal and regulatory duties. The Company Secretary will report as necessary to the Group Board.

5.6 The Information Governance Team can provide advice and guidance on the legal requirements of information security and confidentiality.

6 Clear Desk Implementation

6.1 This Policy is intended to improve security and protect confidentiality of information. Effective and efficient implementation of the Policy should be carried out in accordance with the Clear Desk Guidance (Appendix 1).

7. Equal Opportunities Statement

7.1 This Policy complies fully with the Group's Equal Opportunities Policy. We recognise our pro-active role in valuing and promoting diversity, fairness, social justice and equality of opportunity by adopting and promoting fair policies and procedures.

7.2 We are committed to providing fair and equal treatment for all our stakeholders including tenants and will not discriminate against anyone on the grounds of race, colour, ethnic or national origin, language, religion, belief, age, sex, sexual orientation, gender re-alignment, disability, marital status, pregnancy or maternity. Indeed we will positively endeavour to achieve fair outcomes for all.

7.3 We carry out Equality Impact Assessments when we review our policies. We check policies and associated procedures regularly for their equal opportunity implications. We take appropriate action to address inequalities likely to result or resulting from the implementation of the policy and procedures.

8. Legal and Regulatory Framework

8.1 We adopt and regularly review best practice in information security and data protection. The Group aims to operate in accordance with best practice principles for information security and governance such as may be in place from time to time. This includes (but is not limited to):-

- British Standards Institute ISO 27001: 20013 - Information Security Management;
- British Standards Institute ISO 15489:2001 – Information and Documentation – Records Management (Parts 1 and 2);
- Relevant guidance and Codes of Best Practice published by the Information Commissioner's Office.

8.2 We adhere to principles of the DPA. The seventh data protection principle, schedule 1 specifically requires the data controller to take appropriate technical and organisation measures against:

- unauthorised or unlawful processing of personal data; and
- accidental loss or destruction of, or damage to, personal data.

9. Performance Monitoring

9.1 The Group will put in place a system which monitors and measures performance under this Policy. Regular compliance monitoring will be undertaken through the Group performance management system with updates being disseminated to senior management via the Information Governance Team.

10. Policy Review

10.1 We will review this Policy every year and on changes to the Group. More regular reviews will be considered where, for example, there is a need to respond to new legislation/policy guidance. Reviews will consider legislative, performance standard and good practice changes.

11. Links with other policies

11.1 This policy links other policies and strategies including (but not limited to):

- Wheatley Group Data Protection Policy
- Wheatley Group Records Management Policy

- Wheatley Group Records Retention Schedules;
- Group Information Management Strategy;
- Wheatley Group Business Continuity Policy;
- Wheatley Group Social Media Policy;
- Wheatley Housing Group Risk Management Policy;
- Physical Information and Security Policy;
- Unacceptable Actions Policy.

Appendix 1

Clear Desk Guidance

To implement the policy the following steps should be followed:

- At the end of the working day or when leaving the office for a major part of the day, all staff are expected to clear their desk of papers and any files containing personal or business sensitive information.

- Papers must be stored appropriately and not hidden in trays, files or stowed in piles of loose, unsecure paperwork. The Group has provided an under desk pedestal and/or storage cupboards for this purpose. Pedestals and/or storage cupboards must be locked overnight and the keys removed.

- This Policy also relates to moveable media which may contain business sensitive and personal information, including iron keys, mobile or smart phones and laptops. Media of this type must also be cleared from desks or, where possible, securely locked in the user's pedestal or a storage cupboard, before leaving your desk unattended for any significant period of time and / or before leaving the office.

- All information of a confidential, business sensitive or personal nature should be stored in a locked pedestal or storage cupboard. The facilities management team should be notified immediately of any storage cupboard, drawer unit or pedestals that are broken or have missing keys by the individual whom the pedestal has been allocated, or in the case of storage cupboards or drawer units, the manager of the team to whom the cupboard or drawer unit is allocated.

- Each team should have an established process to ensure that 'key safes' and team storage facilities (such as cupboards and / or drawer units) are locked each evening.

- All meeting rooms and touchdown areas should be cleared by the individuals using them of all papers, moveable media and any electronic equipment they have brought to the room/area after use. Informal meeting spaces, breakout and print areas should also be cleared of clutter and personal papers after use. Special care should be taken to ensure that no printed material is left at the print areas.

- Floors and window areas should be kept clear and not used for any form of storage. Evacuation routes to stairwells should be completely free of obstacle.

- Files and boxes should not be stacked on floors. When recalled from offsite storage, files should be securely locked in storage cupboards or drawer units. When no longer required they should be returned immediately. The offsite storage provider is instructed not to leave any files it is delivering in an unattended space. Staff will be held responsible for any files left unattended for collection by the offsite provider.

- The secure destruction consoles provided must be used for the disposal of all business, personal and confidential information. The disposal of business sensitive or personal information in non-

secure waste will be considered an information security breach.

- Any computer or laptop switched on and left unattended in the office (or elsewhere when being utilised for work purposes) must be "locked"'. PCs, screens and laptops should be switched off before leaving the office.

- Documents should be read on screen where possible to avoid generating increased amounts of clutter and to mitigate demand on the confidential destruction facilities wherever possible.

This list is not exhaustive. Common sense and due caution must be exercised when dealing with all personal, confidential and business sensitive information.