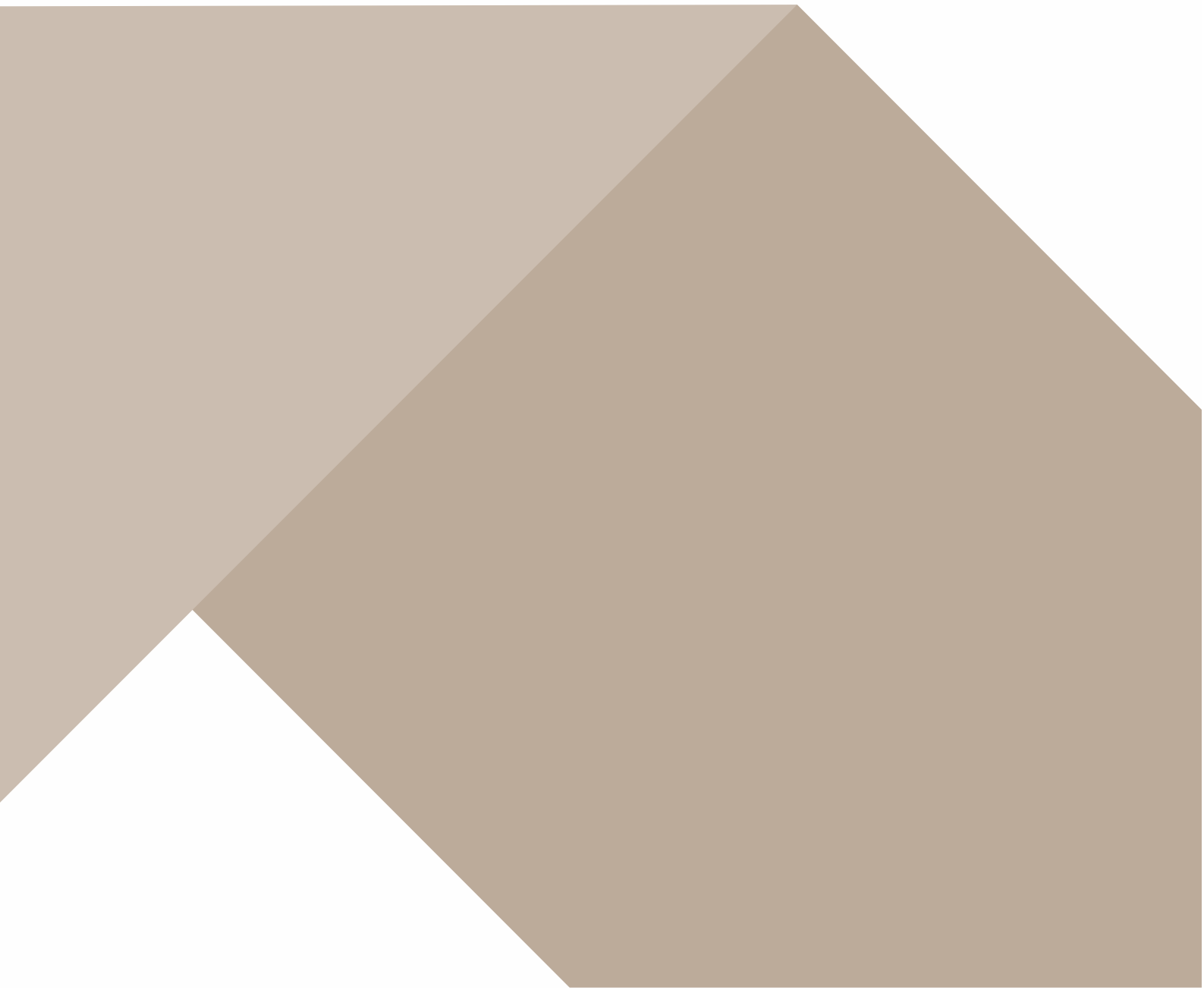
Wheatley Group

Making homes and lives better
wheatley-group.com

Wheatley Group Clear Desk Policy



We can produce information on request in large print, Braille, tape and on disk. It is also available in other languages. If you need information in any of these formats please contact us on Freephone 0800 479 7979.

如果你向我們提出要求，我們可以爲你提供本資訊的其他語言的版本，或者是盲文或磁帶。如果你需要本資訊的任何一種這些版式的版本，請聯繫我們，電話號碼是 0800 479 7979.

Si vous nous le demandez, nous pouvons vous remettre ces informations en d'autres langues, en braille ou sur cassette. Si vous souhaitez que ces informations vous soient fournies sous l'un de ces formats, contactez-nous en composant le 0800 479 7979.

چنانچه مایل باشید می‌توانید این مطالب را به فارسی یا زبان‌های دیگر و همچنین بریل و یا بر روی نوار کاست دریافت دارید. در صورت نیاز خواهشمندیم با شماره تلفن 0800 479 7979 با ما تماس بگیرید.

ਜੇ ਤੁਸੀਂ ਸਾਨੂੰ ਬੇਨਤੀ ਕਰੋ ਤਾਂ ਅਸੀਂ ਤੁਹਾਨੂੰ ਇਹ ਜਾਣਕਾਰੀ ਹੋਰ ਭਾਸ਼ਾਵਾਂ, ਬ੍ਰੇਲ (ਨੇਤ੍ਰਹੀਣਾਂ ਲਈ ਭਾਸ਼ਾ) ਵਿੱਚ, ਜਾਂ ਟੇਪ ਉਪਰ ਦੇ ਸਕਦੇ ਹਾਂ। ਜੇ ਤੁਹਾਨੂੰ ਇਨ੍ਹਾਂ ਵਿੱਚੋਂ ਕਿਸੇ ਰੂਪ ਵਿੱਚ ਚਾਹੀਦੀ ਹੋਵੇ, ਤਾਂ ਕਿਰਪਾ ਕਰਕੇ ਸਾਡੇ ਨਾਲ 0800 479 7979 ਨੰਬਰ ਤੇ ਸੰਪਰਕ ਕਰੋ।

Na Pana/Pani życzenie możemy zapewnić te informacje w innych językach, alfabetem Braille'a lub na kasecie. Jeśli chciał(a)by Pan(i) uzyskać te informacje w którejś z tych form, prosimy skontaktować się z nami pod numerem telefonu 0800 479 7979.

Haddii aad na weydiisato waxaanu warbixintan kugu siin karaa iyadoo ku qoran luuqad kale, farta ay dadka indhaha la' akhriyaan ama cajalad ku duuban. Haddii aad jeclaan lahayd in warbxintan lagugu siiyo mid ka mid ah qaababkaas, fadlan nagala soo xidhiidh telefoonka 0800 479 7979.

По вашей просьбе данная информация может быть предоставлена на других языках, шрифтом Брайля или в аудиозаписи. Если вам требуется информация в одном из этих форматов, позвоните нам по номеру 0800 479 7979.

Approval body	*Group Executive*
Date of approval	*30/11/2021*
Review Year	*2024*
Customer engagement required	*No*
Trade union engagement required	*No*
Equality Impact Assessment	*No*

Policy Statement

This Policy, which is approved by the Group Executive Team, is intended to support the Information Governance framework for the group comprising Wheatley Housing Group Limited and its subsidiaries ('the Group') for ensuring compliance with the relevant legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) and any subsequent or related laws. To this end, the Group will:

- Regard Information Governance and compliance with DPA 2018 and the UK GDPR 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 DPA 2018, the UK GDPR 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. To reflect the Group's operating model, this Policy should apply to both office and home based staff.

Signed: Ranald Brown

Title: Director of Assurance

Effective Date: 30 November 2021

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. This applies to both working in an office and home based environment.

1.2 The establishment of a Clear Desk Policy is recognised as good practice in line with data protection law.

1.3 This Policy covers the Group as a whole. All employees (whether permanent or temporary), office, home or field based, 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.

Aims

3.2 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 that employees are aware of their duty to keep personal information secure in compliance with the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulations (UK GDPR) ;
- 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.

Objectives

3.3 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.

4 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 **Director of Assurance** has responsibility for maintenance and implementation of this Policy to ensure that the Group complies with its legal and regulatory duties.

5.6 The **Information Governance Team** can provide advice and guidance on the requirements of data protection legislation and information governance queries.

6 Clear Desk Implementation

6.1 This Policy is intended to improve security and protect confidentiality of information. 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, where required to do so, 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 adheres to the DPA 2018 and the UK GDPR. The seventh data protection principle, 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. Compliance monitoring will be undertaken by the Information Governance Team with updates being disseminated to senior management.

10 Policy Review

10.1 We will review this Policy every three years 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 including (but not limited to):

- Wheatley Group Data Protection Policy;
- Wheatley Group Records Management Policy;
- Wheatley Group Records Retention Schedules;
- Wheatley Group Business Continuity Policy;
- Wheatley Group Risk Management Policy; and
- Unacceptable Actions Policy.

Appendix 1

Clear Desk Guidance

To implement the Policy the following steps should be followed for both office, field based, agile and home based staff.

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

- Documents should be read on screen, where possible, to avoid generating increased amounts of paper use and to mitigate demand on the confidential destruction facilities. Personal or business sensitive information should only be printed and/or taken out of offices where there is management approval to do so and there no practical means to work with this information electronically. Guidance around the types of information which can be printed and removed from offices will be given locally by managers driven by service requirements.

- Once confidential and/or business sensitive information is printed and/or removed from offices in paper format by staff, it becomes the staff member's reasonability to ensure that such materials are stored safely and securely. Staff members will be held accountable for any data losses of printed materials.

- Where confidential and/or business sensitive information is printed by a staff member or removed from offices in paper format, staff should ensure that the information is securely destroyed when no longer required. For example, staff may use the secure destruction consoles provided in offices to ensure secure destruction of information. The disposal of business sensitive or personal information in non-secure way will be considered an information security breach.

- If staff have been provided with access to pedestals and/or storage cupboards and/or locked folders in an office or at home, they must ensure that these are locked overnight or when leaving your desk or workspace for a major part of the day and the keys removed. 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.

- When working in an office environment, 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 at the end of each day. Floors and window areas should be kept clear and not used for any form of storage. All evacuation routes should be completely free of obstacles. 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.

- 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 stored securely before leaving your desk unattended for any significant period of time and / or before leaving your desk. Where possible, moveable media should be locked in a pedestal or a storage cupboard.

- 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 or public areas when working on an agile basis.

- 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 your workspace for a major part of the day.

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