Wheatley Group

Making homes and lives better
wheatley-group.com

Wheatley Group Clear Desk Policy

We will provide this policy on request at no cost, translated, in large print, in Braille, on tape or in another non-written format.

We can produce information on request at no cost in large print, in Braille, on tape or in another non-written format. We can also translate this into other languages. If you need information in any of these formats, please call us on 0800 479 7979 or email info@wheatley-group.com

Możemy, na życzenie, bezpłatnie przygotować informacje dużą czcionką, w alfabecie Braille'a, na taśmie lub w innym niepisanym formacie. Możemy je również przetłumaczyć na inne języki. Jeśli potrzebujesz informacji w którymkolwiek z tych formatów, zadzwoń do nas pod numer 0800 479 7979 lub wyślij e-mail na adres info@wheatley-group.com

Podemos produzir informações mediante solicitação e sem custos, em impressão grande, Braille, cassete ou noutro formato não descrito. Também podemos traduzi-las em outros idiomas. Se precisar de informações em qualquer um destes formatos, contacte-nos através do número 0800 479 7979 ou envie um e-mail para: info@wheatley-group.com

يمكننا إنتاج معلومات عند الطلب مجانًا مطبوعة بأحرف كبيرة أو بطريقة برايل أو على شريط أو بتنسيق آخر غير مكتوب. يمكننا أيضًا ترجمة هذا إلى لغات أخرى. إذا كنت بحاجة إلى معلومات بأي من هذه التنسيقات، فيرجى الاتصال بنا على 0800 479 7979 أو إرسال بريد إلكتروني إلى info@wheatley-group.com

در صورت درخواست، می‌توانیم اطلاعات را در چاپ بزرگ، خط بریل، روی نوار یا در فرمت غیرنوشتاری دیگری ارائه دهیم. همچنین می‌توانیم اطلاعات را به سایر زبان‌ها ترجمه کنیم. در صورت نیاز به اطلاعات بیشتر در هریک از این فرمت‌ها، لطفاً از طریق شمارهٔ 0800 479 7979 با ما تماس بگیرید یا ایمیلی به info@wheatley-group.com ارسال کنید.

ہم درخواست پر معلومات کو بڑے حروف، بریل، ٹیپ پر یا کسی اور غیر تحریری صورت میں بغیر کسی لاگت کے مہیا کر سکتے ہیں۔ ہم اس کا دوسری زبانوں میں ترجمہ بھی کروا سکتے ہیں۔ اگر آپ کو ان میں سے کسی صورت میں یہ معلومات درکار ہوں تو برائے کرم ہمیں 0800 479 7979 پر کال کریں یا info@wheatley-group.com پر ای میل کریں۔

Approval body	*Executive Team*
Date of approval	*25 June 2024*
Review Year	*3 years*
Customer engagement required	*No*
Trade union engagement required	*Yes*
Equality Impact Assessment	*No*

Contents

1 Introduction and Background

The Wheatley Group Clear Desk Policy is intended to improve the security of documents and protect the confidentiality of information within Wheatley Housing Group 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.

The establishment of a Clear Desk Policy is recognised as good practice in line with data protection law including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) and any subsequent or related laws.

1.1 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

This Policy is designed to help us safeguard the physical security of information (such as papers and removable storage material such as USB sticks or CDs) and electronic information assets through.

Adhering to this Policy will 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

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

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 DPA 2018 and the 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

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;
- ensure that senior management take individual responsibility to effectively protect the security and confidentiality of information across the Group and within each subsidiary;
- measure training on data protection, which includes information about the importance of keeping information secure and out of sight;
- 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

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

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.

It is incumbent upon all teams and employees to:

- achieve and demonstrate an adequate level of general awareness of information security and confidentiality; and
- familiarise themselves with and adhere to the key guidance.

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

Directors/Managing Directors will be required to provide an annual confirmation that their teams within their directorate are aware of this policy.

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

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.

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

6 Clear Desk Implementation

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

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.

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.

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

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

We monitor performance of this Policy by measuring Group Data Protection Training which covers this Policy including the importance of protecting and storing securely data held by the Group and keeping information out of sight.

10 Policy Review

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

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; and
- Wheatley Group Risk Management 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 (either at home or in an office) 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,.

- Personal or commercially 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.

- Once confidential and/or commercially sensitive information is printed and/or removed from offices in paper format by staff, it becomes the staff member's responsibility to ensure that such materials are stored safely and securely.

  Where confidential and/or commercially 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.
- 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 their 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. . 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.