DATA SECURITY POLICY

Document Control

- Policy Reference: GF04
- Version Number: 03
- Author: Jess Cantrill
- Date of Last Review: Aug 2022
- Date of Next Review: Aug 2023

Revision History:

Version Number	Version Date	Nature of Change	Date Approved
01	Sep 2019	Implemented.	Sep 2019
02	July 2022	Revised branding & changes in line with current BCP.	25.7.2022
03	Aug 2022	Amended & further approved.	Aug 2022

Keystage Housing

Contents:

1. POLICY STATEMENT

1.1. This policy is to be read in conjunction with our Data Protection Policy and any other related policies or documents, including any Data Protection Privacy Notices supplied to individuals we deal with.

1.2. We have a commitment to ensuring that personal data is processed in line with GDPR and relevant UK law and that all members of staff, and people who have access to personal data and company systems, conduct themselves in line with this and other related policies. We have strict obligations to process personal data securely and to adopt sufficient procedural and technological safeguards.

1.3. This Data Security Policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

2. STATUS OF THE POLICY

2.1. The purpose of this policy is to set our rules on how to safely and securely deal with personal and confidential data.

2.2. Our Privacy Officer is responsible for ensuring compliance with GDPR and with this policy. Your manager can advise you who our Privacy Officer is. If we have cause to appoint a Data Protection Officer (an official appointment) or use a different title for a Privacy Officer, we will let you know and any reference to Privacy Officer shall include reference to a new title or a Data Protection Officer. Any questions or concerns about the operation of this policy should be referred in the first instance to the Privacy Officer.

2.3. If you consider that this policy has not been followed in respect of personal data you should raise the matter with either your manager or the Privacy Officer.

3. TERMINOLOGY USED IN THIS POLICY

3.1. Our Data Protection Policy sets out clearly the key principles of good practice and sets out definitions of the terminology commonly used.

3.2. Data is personal information about an individual who can be directly or indirectly identified from that information. Data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.3. Data Subjects for the purpose of this policy include all living individuals about whom we hold Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Data.

3.4. Data Controllers are the people who or organisations which determine the purposes for which, and the manner in which, any Data is processed. They have a responsibility to establish practices and policies in line with relevant laws. We are the Data Controller of all Data used in our business.

3.5. Data Users include employees whose work involves using Data. Data Users have a duty to protect the Data they handle by following our data protection and security policies at all times. All employees have a responsibility, when using Data, to comply with any security safeguards and procedures we put in place.

3.6. Processing is any activity that involves use of Data. It includes obtaining, recording or holding Data, or carrying out any operation or set of operations on Data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Data to third parties.

3.7. Special Categories of Data are sensitive categories of Data about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, or sexual orientation. It also includes genetic and biometric Data (where used for ID purposes). Special Categories of Data can only be processed under strict conditions, and may require the explicit consent of the person concerned.

3.8. Criminal Offence Data is Data which relates to an individual's criminal convictions and offences. It can only be processed under strict conditions and may require the explicit consent of the person concerned.

3.9. Confidential Information is information which is marked as confidential or information which is not marked confidential but when applying common sense it is clear that it is information we do not want an unauthorised person to see. For example, details of our products and services, lists of our customers and what they purchase from the company, individual and company customers, business information about us which if it got into the hands of a competitor or someone setting up in competition would give them an pecuniary advantage over us. If you are in doubt whether something is confidential, please ask your Manager.

3.10. Sensitive Data is Special Categories of Data, Criminal Offence Data and sensitive and valuable Confidential Information.

3.11. Confidential Data means Data and Confidential Information.

3.12. Equipment means computers, devices including, smartphones, tablets and storage devices, including USB sticks or remote hard drives, whether personal or owned by us.

4. WHAT DO WE EXPECT FROM YOU?

4.1. As Data Users, you are expected to understand the key principles of data protection contained in our policies relating to data protection and to understand the promises we are required to make to Data Subjects in our Privacy Notices. If you fail to meet your obligations as a Data User and/or unlawfully process Data and/or Sensitive Data, you may be held personally liable and may face legal action. If in doubt about how you can comply with our data protection policies, please do not guess but ask your manager or the privacy officer.

4.2. You are also expected to safeguard Confidential Information of all levels of sensitivity and take steps to ensure it does not fall into the wrong hands.

4.3. Your obligations include complying with any guidance we may give you on how you handle the information you will have access to, whether about the company, staff members, clients, customers, candidates or any other individuals.

4.4. If you feel you require training or guidance on any of our policies or any instructions we may give you, it is your responsibility to speak to your manager or the privacy officer.

5. RISKS TO CONFIDENTIAL DATA AND SENSITIVE DATA

5.1. You are required to consider and assess the security risks involved when working with Confidential Data and Sensitive Data. In cases of Sensitive Data, you will need to be even more vigilant.

5.2. The risks involved include:

5.2.1. Confidential Data being overheard by an unauthorised person.

5.2.2. Theft e.g. someone purposefully downloading customer records from the Company database before leaving.

5.2.3. Loss e.g. a database has been accidentally wiped and there is no back up, in order to prevent a potential breach, all data must be securely backed up upon the company's secure network.

5.2.4. Disclosure (intentional or unintentional) e.g. emailing the wrong recipient.

5.2.5. Hacking e.g. someone purposefully accessing the Company network via an individual's account.

5.2.6. Interception e.g. listening in to someone's phone calls or interception through hacking
5.2.7. Unauthorised storage e.g. backing up files onto a personal storage device of any description.

6. GENERAL CONFIDENTIAL DATA AND SENSITIVE DATA SAFEGUARDS

6.1. Do not process Confidential Data or Sensitive Data unless we have authorised you to do so.
6.2. If you are required to talk about Confidential Data or Sensitive Data, whether in the office, consider carefully whether you can be overheard by unauthorised persons. If you are in any doubt, consider delaying the conversation until you cannot be overheard or moving to a place you cannot be overheard.
6.3. Set your Equipment to 'sleep' or 'automatically lock' after a short-period of non-use.
6.4. Use a secure password on Equipment to prevent unauthorised access and change your password regularly. Do not share your password with anyone and do not use the same password for any other services or devices. We recognise that your passwords need to be memorable to avoid you needing to write them down, but we encourage you to use strong passwords which are hard to predict by ensuring that each password is at least 10 characters long and that each contains a mix of upper and lower case characters, numbers and symbols.
6.5. Ensure that passwords used to access any Confidential Data or Sensitive Data are not automatically electronically stored.
6.6. Ensure that any Confidential Data or Sensitive Data is not on display on your desk or your screen when not being used.
6.7. Ensure that you close down your work when you leave your desk and make sure you do not allow others to use your Equipment unless there is no risk involved.
6.8. Lock away any paper copies of Confidential Data or Sensitive Data when not being used.
6.9. It is expressly forbidden to use personal email accounts to send Confidential Data or Sensitive Data and could lead to disciplinary action been taken.
6.10. Unless it is absolutely necessary, and we have given you permission to do so, do not save Confidential Data or Sensitive Data on the local drive of Equipment, external storage devices or on external 'cloud' storage (e.g. drop box or iCloud). Use our system so that it can be securely held and backed up.
6.11. Unless it is absolutely necessary, and we have given you permission to do so do not store Confidential Data or Sensitive Data on any form of remote storage device. If you are given permission to use such a storage device, the files must be encrypted and password protected. The use of a storage device should only ever be a temporary measure and you should delete the files as soon as you no longer need to store it there.
6.12. Think carefully before sending any Confidential Data in the post and consider using special delivery options or using a courier. Always follow up to ensure that Data or confidential information has reached the intended recipient. Sensitive Data should not be sent in the post unless it is absolutely necessary and we have given you permission to do so.
6.13. If sending Confidential Data or Sensitive Data via email, check carefully that you have the correct email address, the recipient is authorised to process the information and consider encrypting and password protecting any files.
6.14. Securely dispose of paper copies of Confidential Data or Sensitive Data, for example, by shredding them.

6.15. Do not use any personal form of social media (Facebook, WhatsApp, Messenger etc) to process any Confidential or Sensitive Data, even if you think it is safe except in the instance of the company WhatsApp groups, but even then with consideration as to who may view the data or the content of the data been shared.

6.16. Always report any breaches of security or suspicions of breaches or potential breaches to the company privacy officer, HR department or your manager without delay and comply with any policies we may introduce in this regard.

6.17. If you feel you need to deviate from these specific rules, then speak to us so that we can assess the risks involved.

7. USING EQUIPMENT THAT WE DO NOT MANAGE

7.1. The general safeguarding rules above also apply to you using Equipment not owned by us and/or not managed by the company, for example 'Personal Equipment'.

7.2. As a general rule, we do not want you using Personal Equipment to process Confidential Data or Sensitive Data but if this is unavoidable or you feel there are benefits to doing so, please let us know so that we can assess the security risks involved and discuss the security measures you will need to take. We may require you to sign additional documentation relating to making your personal Equipment available for monitoring or agreeing to allow us to wipe its data in cases of security risks. By using your Personal Equipment, you agree to give us access to it in the event of any security issues and whilst we will not actively seek to access any personal files, eliminating the security issues may result in such access. If you are concerned about this, we recommend that you do not use Personal Equipment for work.

7.3. Most commonly, members of staff may wish to access our IT and communications systems via their smartphones or devices or home computers. We recognise the flexibility this can give to members of staff and the benefits to us. Please let us know you are doing this as information may still be at risk.

7.4. If you lend, borrow, sell or give Personal Equipment, you need to think carefully about whether the recipient could gain access to the work you were doing on it. If in doubt, please contact your manager, the IT department or the privacy manager and we will assess the risks involved, which may involve wiping its data.

7.5. If you are accessing our system via programs or apps, ensure that they are not accessible without a password. For example, if you are accessing outlook on your iPhone, ensure that you have a password to access your smartphone or tablet and that any apps or programs you are using to access information, are also password protected with a different password.

7.6. Ensure that passwords used in relation to work are not automatically remembered on Personal Equipment.

7.7. Always back up any work you do on your Personal Equipment prior to transferring to the company networks, please discuss this with your manager, if you are unsure what this involves.

7.8. If you wish to use your own personal computer or laptop, you should ensure that it can encrypt files and has the necessary security software. If in doubt, speak to us.

8. REMOTE/MOBILE/HOMEWORKING SAFEGUARDS

8.1. When you are mobile, keep equipment with you at all times, for example, do not use luggage racks on public transport and do not leave equipment unattended in vehicles or public places.

8.2. When you have finished using equipment, consider putting it in a locked cupboard or in a locked room.

8.3. If you are working from home, ensure that your home is secure.

8.4. If you are processing Confidential Data or Sensitive Data, consider who can see your screen whilst you are working (even if you are at home). If you are in a public place, e.g. on a train or whilst sitting in a café, take extra care that no one can see your screen and never leave a screen open on unattended equipment.

8.5. Consider discussing with your manager or the privacy officer any additional security measures that need to be taken, for example installing remote wiping agents so that Equipment can be wiped of all data in the event of loss or theft or installing software which prevents the hard-drive from being removed.

9. TRAINING

9.1. New employees must read and understand this policy as part of their induction and may, if necessary, have training on data security. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential Data Breach.

10. MONITORING AND REVIEW

10.1. We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

10.2. Line Managers and team leaders will be responsible for general monitoring of these guidelines. Transgressions will be reviewed with individual staff members, but in some cases, it may be appropriate to record examples for discussion as part of staff training or discussion at team meetings.

10.3. Significant and/or repeated breaches of this policy will lead to disciplinary action, up to and including dismissal.

11. RELATED POLICIES

GF02- IT & Communications Systems Policy
GF03- Data Protection Policy
GF05- Personal Data Breach Notification Policy
HR01- Disciplinary Procedure Policy