Confidentiality Policy

Publication: November 2016

Date for Review: November 2017

Version: 2

Contents

1. Policy Statement

1.1 This Confidentiality Policy sets out the principles that all staff must follow when managing personal or confidential information. The policy ensures that staff members are aware of their responsibilities in protecting confidential and personal information.

1.2 All employees working for SW9 Community Housing are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is a requirement of the Data Protection Act 1998.

1.3 It is important that SW9 Community Housing protects and safeguards personal and confidential information that it gathers creates processes and discloses, in order to comply with the law and to provide assurance to residents and stakeholders.

1.4 SW9 Community Housing will only collect, hold and process personal and confidential information that it needs for business purposes and it will not keep that data for longer than necessary.

2. Definitions

2.1 Personal data is defined as anything that contains the means to identify a person, e.g. name, address, postcode, date of birth.

2.2 Confidential information includes information that is private and not public knowledge or information that an individual would not expect to be shared. It can relate to residents, such as tenancy records or staff, such as employment records.

3. Scope of Policy

3.1. All staff members of SW9 Community Housing are within the scope of this document.

3.2 This policy sets out the requirements placed on all staff when sharing personal or confidential information within SW9 Community Housing, with other organisations and with residents. Specifically, it includes data sharing where personal or confidential information is requested in the following circumstances:

- Requests from individuals to access their own personal data.
- Requests for information from Community Trust Housing.
- Requests for information from other organisations.
- Requests for information from Councilors/MP's.
- Sharing information with the police, emergency services and external contractors.

4. Our Service Standards

4.1 We will respond to requests for access to information within 20 working days. Where we are unable to release information requested we will explain why.

5. Roles and Responsibilities

5.1 **The Executive Director**
The Executive Director has overall responsibility for strategic and operational management, including ensuring that this policy is followed, along with all legal, statutory and good practice guidance requirements.

5.2 **HR Manager**
The HR manager is responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that confidentiality is included in corporate inductions for all staff.

5.3 **Line Managers**
Line managers are responsible for ensuring that staff members comply with this policy and that any breaches of the policy are reported, investigated and acted upon.

5.4 **All staff**
Confidentiality is an obligation for all staff. Staff members are expected to participate in induction, training and awareness raising sessions carried out on confidentiality issues. Any breach of confidentiality, inappropriate use of resident or staff records, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract, and must be reported.

6. Corporate Principles

6.1 All staff must ensure that the following principles are adhered to:

- Personal or confidential information must be kept secure when it is received, stored, transmitted or disposed of.
- Access to personal or confidential information must be limited to those who need-to-know to be able to carry out their jobs effectively.
- Disclosure of personal or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure must be discussed with either the Line Manager or the Executive Director.

7. Keeping Data safe in the Workplace

7.1 All staff members have a legal duty of confidence to keep personal or confidential information private and not to share information accidentally. The following advice applies to all staff members who are associated with personal or confidential information:

- Before speaking about personal or confidential information, ensure that the information cannot be overheard by people who should not have access to it.
- Take care not to leave any personal or confidential information unattended.
- This includes computer printouts, reports and other documents, containing personal or confidential information.
- Lock computer terminals when away from the desk so that personal or confidential information cannot be accessed.
- Keep passwords secure and do not disclose them to unauthorised persons.
- Staff must not use someone else's password.
- Access to filing systems and information storage areas where personal and confidential information is stored must be locked and measures should be in place to prevent information being seen by unauthorised people.
- All staff should clear their desks at the end of each day. In particular they must keep all records containing personal or confidential information secure or locked away in recognised filing and storage places.
- Unwanted printouts containing personal or confidential information must be put into a confidential waste bin. Printouts must not be left on desks and must be filed and locked away when not in use.
- Personal and confidential information should be accessed by staff only where they need it for their work. Employees must not view any information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act.

8. Disclosing Confidential Information

8.1 SW9 Community Housing is responsible for protecting all the information it holds and must always be able to justify any decision to share information. To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it. It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary should be disclosed.

8.2 Information can be disclosed:

- When effectively anonymised.
- When the information is required by law or under a court order.
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their Line Manager or the Executive Director before disclosing.

- Any request for information from the police or emergency services must be made in writing. Requests must specify what information is required and provide justification for why the information is needed. See Appendix A for data request form.
- If staff members have any concerns about disclosing information they must discuss this with their Line Manager or the Executive Director.
- Care must be taken in transferring information to ensure that the method used is as secure as it can be.
- In most instances a Data Sharing Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer.
- A controlled disclosure is best achieved in writing in order to maintain an audit trail and avoid sharing too much.

9. Working Away from the Office

9.1 There will be times when staff may need to work from another location or away from the office and may need to carry confidential information with them e.g. on a laptop, USB stick or paper documents. Taking paper documents that contain personal or confidential information is discouraged. When working away from the SW9 Community Housing office, staff must ensure that their working practices comply with this policy.

9.2 Where it is essential to take personal or confidential information out of the office, staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations. Staff must minimise the amount of personal information that is taken away from the office.

9.3 If staff members do need to carry personal or confidential information they must ensure the following:

- Confidential information is kept out of sight whilst being transported.
- If staff members do need to take personal or confidential information home they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.
- Staff must NOT forward any personal or confidential information via email to their home email account.

10. Related Documents

- Complaints Procedure
- Information Sharing Agreement
- Data Protection Policy
- CCTV Cote of Practice

11. Legislation

We will meet our legal obligations under the following legislation:

- Data Protection Act 1998

12. Review

12.1 Processes shall be put in place to monitor compliance with this policy and both the policy and the processes will be health checked annually. A full review will be carried out if there are any significant changes to legislation and/or regulation, or if the health check shows there is evidence that the processes are not being followed and the policy is not being complied with.

13. Appendices

13.1 Request for personal/confidential data.

Appendix A – Request for personal/confidential data

RESTRICTED – WHEN COMPLETE
CONFIDENTIAL

Your details			
Name and contact details			
Your reference number			
By completing this form I confirm that I am making enquiries which are concerned with offences under the Theft Act 1968 and Social Security Administration Act 1992 as amended by the Social Security Administration (Fraud) Act 1997, Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) regulations 2013 or the Fraud Act 2006. Section 29(3) of the Data Protection Act 1998 states that where information is required to prevent or detect a crime, or for the apprehension of offenders, personal data is exempt from the Non-Disclosure Provisions of the Act. Please tick his box if you accept these terms: ☐			
Priority Please give justification if not routine. • **Urgent** ☐ Please state why:_____ • **Specific date response required** ☐ Please state why:_____ • **Routine** ☐ Please state why:_____			
Person / premises relating to this enquiry			
Last and Forename(s)		**Date of birth**	
Any other relevant information such as address or alias			

Telephone number	

Timescale of information required
Please provide justification for the timescale of data to be collated, which must be proportionate to the reason for requesting the information

Past month		**Last three months**		**Last six months**		**Last year**		**Over a year – please state time**	

Justification:

Information being sought

What information do you require?	
Why do you need this information? What are you trying to achieve?	
How is the information to be used?	

Please add any further information which may support this request:

Signature	
Date	