SIX TOWN HOUSING

DATA PROTECTION FRAMEWORK

Date Approved: January 2015 via EBRM
Review Date: January 2016

Author: Danny Lansley
Governance and Compliance Lead

Contents		
Section		**Page No**

Section 1 - Policy Statement

This policy statement and framework sets out how Six Town Housing manages the data we collect and use in accordance with the Data Protection Act (DPA) 1998. As an organisation we collect and use information about the people with whom we deal. These are known as 'data subjects' and could be customers, current and former members of staff and suppliers.

In addition, we may be required by law to collect and use information in order to comply with the requirements of central government. All this personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by other means.

Six Town Housing regards the safe use and treatment of personal information as very important to successful operations and to maintaining confidence between the organisation and those with whom it carries out business.

However there are risks associated with the collection, holding and use of personal information, this framework includes all our organisational policies which aim to mitigate the risk of data protection issues and promote good information management. The framework should be read in conjunction with the following policies and strategies:

- ICT Security Policy
- Staff Code of Conduct
- Staff Safety Guidelines and Procedures (in development)

Our Commitments

In order to ensure that Six Town Housing meets its obligations under the DPA we will ensure that:

- There are key senior members of staff with responsibility for data protection.
- There is a central point of contact for advising and supporting all staff in implementing effective information management.
- Everyone managing and handling personal information understands that they are responsible for following good data protection practices.
- Everyone managing and handling personal information is appropriately trained to do so.
- Anyone wishing to make enquiries about handling personal information, whether a member of staff or customer is aware of how to make such an enquiry.
- Methods of handling personal information are regularly assessed and evaluated, either internally or via an audit function.

Roles within the Organisation

Senior Information Risk Owner (SIRO) – Sharon McCambridge

Has overall responsibility for information governance and compliance with data protection legislation across Six Town Housing. This role involves leading a culture of good information management through the development of key roles and responsibilities in the organisation, an effective support infrastructure, training alongside detailed and accessible policies and procedures in support of information governance.

Information Asset Owner (IAO) -

An identified member of staff who is the nominated owner for one or more information assets within the organisation. An information asset is customer, staff or corporate information, processed by Six Town Housing and held in either an electronic or manual format.

This could include:

- Tenant records
- House files
- Staff file
- CCTV recordings
- Contracts and service level agreements

Governance and Compliance Lead – Danny Lansley

Has operational responsibility for overseeing compliance with the Act, this includes developing and implementing this framework, provide information and guidance on the processing of personal data, give guidance to staff, deliver training to staff and process, co-ordinate and respond to all requests for information.

Fees and Charges

Six Town Housing charges £10 for processing any subject access requests received from customers or members of staff. The 40 calendar day limit of responding to requests does not commence until payment has been received.

In addition, Section 9A of the Act states that any public authority does not have to respond to any request under the DPA if it is estimated that the cost of complying with the request exceeds the appropriate limit. This has been set at £450 for organisations like Six Town Housing. Costs are estimated at £25 per hour and include any action by members of staff to:

- Determine if we hold the information.
- Locate the information, or a document which may contain the information.
- Retrieve the information, or a document which may contain the information.
- Extract the information from a document containing it.

Any decision on the cost will be made by the Governance and Compliance Lead, who is the organisation's Data Controller. On the rare occasion it is estimated that

a request may exceed this limit, Six Town housing will discuss with the requester whether they would prefer to redefine the request to reduce costs.

Overview of Policies and Roles

The following sections briefly describe the policies and procedures included in the framework along with when they are due to be reviewed:

Data Breach Policy and Procedure

This policy sets out how Six Town Housing will manage any actual or suspected breaches of data.

Subject Access Request Procedure and Form

Under the DPA tenants or members of staff are entitled to request all of the information which we hold on them. This procedure helps staff identify what is a subject access request and ensures that it is responded to within the 40 day limit.

Records Management Schedule

An essential part of information management is the ability to ensure that the records we have are not kept for longer than is necessary. This schedule helps staff identify where records can be deleted, the full schedule is at Section 6.

Section 3 - Data Breach Policy

1 Policy Statement

Our information assets and the systems that support them must be adequately secure to protect our customers' data and to ensure that Six Town Housing (STH) l can deliver its services and meet its legal and contractual obligations. This includes liaising with key partners who share data and information systems such as Bury Council on information security issues. Six Town Housing will ensure that it reacts appropriately to any actual or suspected breaches of that security which may jeopardise its information assets and systems.

2 Purpose

The purpose of this policy is to ensure that any breach in the security of our information assets is dealt with appropriately. This means that:

- a record is made of all such breaches
- the breach is investigated thoroughly
- appropriate actions are taken to address the problem
- reports are made to external bodies as required
- there is proper monitoring and oversight
- lessons are learned and our information security is improved.

3 Scope

This policy applies to all information assets held Six Town Housing, regardless of format. It encourages a risk-based and proportionate approach to handling information security breaches. Six Town Housing evaluates all breaches on a case-by-case basis and makes decisions on actions through the information gathered.

This policy applies to all employees, Board Members and contractors working on behalf of Six Town Housing.

The procedure needs to be applied as soon as information assets are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

Due to the nature of information and data sharing arrangements with partner organisations, such as Bury Council or Greater Manchester Police, there may be occasions when a data security breach has to be reported to other organisations because they hold the information. In these instances the procedures at Appendix 1 details how they will be dealt with.

4 Risks

Six Town Housing recognises that there are risks associated with accessing and handling information in order to deliver services. Risks are indentified as part of our risk management procedure and recorded in Operational or Strategic Risk Registers.

This policy aims to mitigate the risks by:

- Reducing the impact of information security breaches by ensuring events and incidents are investigated and resolved appropriately and that those affected are informed immediately **(see Appendix 3)**
- Identifying areas for improvement to decrease the risk and impact of future breaches.
- Protecting the Confidentiality, Integrity and Availability of our information assets at all times

5 Protection Roles – Overview

All employees,board members and external contractors are responsible for protecting our information assets from misuse, loss or unauthorised access, modification or disclosure. This does not mean that information cannot be used or shared, but that appropriate steps must be taken to ensure that information is protected and is in line with this and other policies such as the Information Security Policy and Data Protection Policy. Different staff however have different roles in relation to information security and these responsibilities are outlined below:

Senior Information Risk Owner (SIRO): Will act as an advocate for information risk. They are the representative at the Exec Team level and understand the business goals of STH and how these may be impacted by the failure of information assets. The SIRO is responsible for ensuring that management of information risks are weighed alongside the management of other risks facing the organisation such as financial, legal and operational. The SIRO is responsible for the decision to report a data protection breach to the ICO.

Within STH this is the Chief Executive. In the event that the Chief Executive is unavailable for an extended period another member of the Executive Team will make the decision about reporting a breach to the ICO.

Information Asset Owners: Each system that we use should have an information asset owner. This will usually be a Business Manager. Their role is to understand what information is contained in that system, how it is accessed, who has access to it in order for business to be transacted with an acceptable level of risk.

Governance and Compliance Lead: Is responsible for the management of this policy and its supporting procedures, including reviewing Information Security Incident Reporting Forms and escalating incidents to the SIRO. The GCL is the only person in STH responsible for reporting data protection breaches to the ICO, with the knowledge and approval of the SIRO.

Security Officer: Responsible for the overall security of our assets, including information. In their dual role as Strategic ICT Co-ordinator and Security Officer they maintain the technology used for storing our information assets, ensuring that confidentiality, integrity and availability of information is maintained at all times.

6 Protection Roles – Contact Details

Abbreviation	Protection Role	Person	Contact

		Responsible	Extension
Six Town Housing			
STHCE (SIRO)	Chief Executive and Senior Information Risk Owner	Sharon McCambridge	8111 or 8141
BICFBM	Business Improvement and Customer Focus Business Manager	Ailsa Dunn Business Manager BICF	8129
GCL	Governance and Compliance Lead	Daniel Lansley	8134
BM	Business Managers (Information Asset Owners)	See list below for IAOs	
SIC	Strategic ICT Co-ordinator	Mike Nixon	8041

7 Procedure for Incident Handling

Six Town Housing have a procedure for reporting and monitoring such breaches, these are detailed at Appendix 1. These procedures must be followed in the event of an information security breach.

All breaches or possible signs of a breach must be reported at the earliest possible stage to your line manager and to the Governance and Compliance Lead (GCL) see 6 above for contact details. The GCL will liaise with other organisations if appropriate for that breach. The Strategic ICT Co-ordinator must always be informed of any incidents involving lost, stolen or hacked IT equipment. If necessary this will be forwarded to Bury Council.

Examples of such breaches are given in Appendix 2.

8 Policy Compliance and Monitoring

All Six Town Housing employees and Board Members, contractors and other third parties who may have access to our information assets are responsible for ensuring the safety and security of that information and the systems that support it, refer to Six Town Housing's ICT Security Policy.

In the event of any breach of security such as:

- Loss or theft of data or equipment on which data is stored

- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Security failures
- Unforeseen circumstances that leave equipment / data vulnerable
- Hacking
- 'Blagging' offences where information is obtained by deception

You must follow the procedure detailed in Appendix 1.

Non-compliance with this policy could have a significant effect on our efficient operation and may result in reputational damage to us, and significant harm to those whose personal data has been lost, prosecution and financial penalties. As a result data protection issues are regularly reported to the monthly Executive Business Review Meetings (EBRM) and by the Audit, Standards, Risk and Performance (ASRP) Committee.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Governance and Compliance Lead, see contact details at 6 above.

9 Review and revision

This policy will be reviewed at least annually by the Governance and Compliance Lead with any changes being reviewed by the SIRO.

10 References

ICT Security User Guide – this document is currently under review.
http://www.sixtownhousing.org/documents/ICT%20Security%20user%20guide.doc

Bury Council Information Security Policy -
http://intranet/CHttpHandler.ashx?id=13627&p=0

ICO Guide to the Data Protection Act

http://intranet.bury.gov.uk/NR/exeres/B644E894-04F5-4AAD-AD8A-6C8BACA855F4.htm?NRMODE=Unpublished&WBCMODE=PresentationUnpublished

ICO Data Sharing Code of Practice

http://intranet.bury.gov.uk/NR/exeres/892F69D3-2E40-471B-8EB7-20EA74FA28FE.htm?NRMODE=Unpublished&WBCMODE=PresentationUnpublished

Guidance on Subject Access Requests:

http://intranet.bury.gov.uk/NR/exeres/DD2B2700-6DF6-49AE-822F-BC81C4C8AF61.htm?NRMODE=Unpublished&WBCMODE=PresentationUnpublished

Information Commissioner's Office Guidance on data security breach management

11 Discplinary

IMPORTANT!

It is extremely important that information is disclosed to relevant parties to enable the effective operations of Six Town Housing.

But you must remember that

If you knowingly or recklessly disclose information to others without authorisation or misuse or allow others to misuse any IT hardware or software you are committing a disciplinary offence and you may also be committing a criminal offence for which you may be personally liable.

12 Links to other Policies

- Information Security Policy
- Data Protection Policy

Appendix 1

Procedure for incident reporting

You should immediately report the following:

- Any incident that seems to threaten the security of the Six Town Housing, Council network or any Council Information Systems
- Any incident that seem to threaten the security of confidential or sensitive personal information held by Six Town Housing, the Council or partner organisations particularly information relating to people.
- Any malfunction of IT hardware or software , such as a virus infection, this must be reported to the STH ICT Team or the Council Service Desk without delay because it has the potential to affect our IT systems and cause further data loss.

The following abbreviations are used in this procedure:

Abbreviation	Protection Role	Person Responsible	Contact Extension
Six Town Housing			
STHCE SIRO	Chief Executive also Senior Information Risk Owner STH	Sharon McCambridge	8111 or 8141
BMBICF	Business Manager – Business Improvement and Customer Focus	Ailsa Dunn	8129
GCL	Governance and Compliance Lead	Danny Lansley	8134
CMA	Communications Advisor	Laura Conrad	8018
BM	Business Managers (Information Asset Owners)	As arranged	
SIC	Strategic ICT Coordinator	Mike Nixon	8041

Other Contacts:

Bury Council ICT Help Desk – 0161 253 5050 or servdesk@bury.gov.uk

Step 1

Recognising a Breach: Is the information missing or has it been sent to the wrong person? If the answer is yes to one or both of the above questions then a potential breach may have been identified.

Step 2

Reporting the Incident: Immediately inform our GCL and your BM on discovering there has been an information security incident i.e. there has been a loss or disclosure of personal identifiable or confidential data. The GCL/BM-BICF in consultation with senior colleagues will make a risk assessment of the breach. Details will be recorded on the ISIR Form within 24 hours, included at Appendix 4.

Step 3

Mitigation: Following the assessment appropriate steps will be taken to recover any losses and limit reputational damage. Steps might include; efforts being made to retrieve the data which has been disclosed; Informing the CMA about the incident if any press enquiries arise.

All of these actions will be recorded on the ISIR Form, within 7 days, included at Appendix 4.

Step 4

Review and Evaluation:

If the data is owned/controlled by Six Town Housing

GCL and/or BM will immediately report the breach through to the following employees.

Chief Executive	Sharon McCambridge	8111 or 8141
Director of Assets	Emma Richman	8175
Director of Neighbourhoods	John Merrick	8038

Along with the appropriate Director any BMs whose area of the business has been affected must be informed.

Within 7 days of the incident being reported the GCL will check to see that the Information Security Incident Report Form at Appendix 4 has been completed in full, and pass to the SIRO. The purpose of this form is to create a record of the incident which will be used to:

- Record details of the nature of breach
- People affected and potential consequences
- Check what remedial actions are being taken and when they are completed
- Form the basis of reports to the SIRO and to external bodies such as the Information Commissioner's Office as required
- Allow patterns and trends in security breaches to be identified so that the state of information security can be improved.

The GCL will ensure the form has been saved electronically.

The completed form will be passed through to the SIRO for decision, with a decision being made within 10 days.

If the data is owned/controlled by the Council

Head of Internal Audit	Andrew Baldwin	5084
Information Security Manager	Kevin Amos	5163
Data Protection Lead Officer	David Hipkiss	6677

The GCL will report the breach to the following employees of the Council. Other colleagues at STH may be required to liaise with the investigators.

What if the breach involves personal sensitive data about our customers, staff or other people?

If the breach involves personal data about customers, staff or others it may be necessary to inform them. See Appendix 3 for further information/guidance on this.

Step 5

If found that there has been a breach?

If there is found to be a breach at STH, the SIRO-STH will consider if it needs be reported to the Information Commissioners Office (ICO) and the completed form will be stored by the GCL. In the event that the SIRO is unavailable for an extended period another member of the Executive Team will make the decision about reporting a breach to the ICO.

Step 6

The GCL and BMBICF will periodically review any ISIR forms to ensure that any corrective action has been implemented and monitor as necessary.

Appendix 2

Examples of what should be reported

As a general rule to be classed as an incident under the Data Protection Act personal information must have been disclosed. The following are some examples of events which should be recorded using the breach reporting procedure. It is for guidance only and it is not an exhaustive list; any event which potentially jeopardises the security of our information assets should be recorded.

- Theft or loss of any STH/Bury Council IT equipment
- Theft or loss of memory sticks, CDs or other devices containing personal or confidential data, whether encrypted or not.
- Computer infected by virus or other malware
- Use of unapproved or unlicensed software on STH/Bury Council equipment.
- Unauthorised access to databases containing personal or confidential information
- Finding that data has been changed by an unauthorised person
- Personal or confidential data appearing on our website
- Theft or loss of hard copy files containing personal or confidential data
- Break-ins or other unauthorised access to buildings where personal or sensitive data could have been viewed
- Disclosing data verbally, in writing or electronically to someone who should not have access to it
- Not storing confidential information correctly so that it could be viewed by unauthorised people.(i.e. information left on desks, leaving files in your car, not locking computer allowing people to access your desktop).
- Any waste that has been disposed of incorrectly that contains personal or confidential information.

Appendix 3

Notifying people affected by security breaches

Where the security breach involves the loss or compromise of personal data, whether of customers, staff or other people, you will need to consider whether to inform the individuals concerned. There should be a clear purpose for notifying individuals.

Where the breach affects a large number of individuals or involves sensitive data about a small number of individuals the decision as to whether and how to notify individuals will be made by the Business Manager – BICF and Governance and Compliance Lead in consultation with the relevant Director. If the breach is of council controlled data the Executive Directors in discussions with SIRO, Assistant Director of Legal & Democratic Services and the Caldicott Guardians will make the decision.

Issues to consider before notifying individuals:

Risk Mitigation – Could notification help the individuals concerned to mitigate any risks, for example by being alert for unsolicited emails or other correspondence, or by cancelling a credit card or changing a password.

Who should be notified? - If a breach has only affected a small number of people on a particular database, notifying everyone on the database may cause disproportionate enquiries and work.

How the communication will be made - e.g. letter, telephone call, email, statement to the media. This will depend on the number of people affected, whether they have particular needs e.g. children or young adults, and the nature of the information. It is important that advice/guidance is sought from appropriate experienced officers to deal with this type of situation. In all cases the Caldicott Guardians will oversee management of breaches affecting personal identifiable information that relate to health or social care affecting adults or children.

If people are aware that their data has been compromised they may contact the media or complain to the Information Commissioner. If they have suffered damage or distress they may also take legal action against the Council for compensation. This is more likely to happen if we have not notified them and they discover by other means that the breach has occurred.

When notifying individuals:

- Give specific and clear advice on the steps they can take to protect themselves and on what we are willing to do to help them.
- Provide a contact number and /or email for people to contact you and ask any questions about what has occurred.
- For further advice please contact Governance and Complaince Lead, or Caldicott Guardian for Adult Care and Children Services.

Appendix 4: Information Security Incident Report (ISIR) Form

- This form MUST be completed in all occasions where there has been a breach in security that has resulted in the loss of confidential, personal sensitive data. As defined in the Information Security Policy and Reporting Procedure.
- The Governance and Compliance Lead is available for additional advice and will facilitate and co-ordinate the completion of this form until the incident is resolved or concluded including the monitoring of any corrective actions.
- For Council related breaches the Information Security Group monitor all ISIRs and report to the SIRO and AD of Legal & Democratic Services
-

General Information **Part 1 – This form must be completed within 24 hours if there is a potential data breach**					
ISIR Reference Number:			**Today's Date:**		
Department:					
Brief Description of the incident:					
Incident Location:					
Date / Time detected?			**Date / Time reported?**		
Name person reporting incident:			**Name of Departmental DP Lead Officer:**		
Information Asset Owner Name/Job Title and Telephone No:			**Contact Telephone Number:**		
Incident Type (if other please state)	Lost ( ) Stolen ( ) Other ( )		**Identifiers** (e.g. asset number, make, model, phone number, case/file reference/s, system name)		
Who's been informed? STH	**Yes / No**	**Date & Time**	**Who's been informed? Bury Council**	**Yes / No**	**Date & Time**
Governance and Compliance Lead/BMBICF			SIRO		
Relevant Director and Business Manager?			AD Legal & Democratic Services?		
STH Chief Executive?			Head of Audit?		
Comms and Marketing Advisor (if applicable)			Information Security Manager		
Who's been informed? Other	**Yes / No**	**Date & Time**	Data Protection Officer?		

Police			Corporate Communications Manager?		
Other:			Caldicott Guardian ACS or CS?		
			Council Leader?		
			Insurance Section?		
			Line Manager?		

Part 2 – Incident Details and remedial actions

Description as to what happened leading up to the event?

Was the data electronically held or was it hard copied – give details?

On what was the data stored – give details?

If electronically held was it encrypted – give details?

Clear description of the data that has been breached?

Whose data has been breached?

Impact of Breach?

Actual

Potential

Is the data defined as confidential? / Personal? / Personal Sensitive?
Have all those affected by this breach been informed?
What immediate actions are being taken to:
Protect all remaining data?
Get back the lost data?

Part 3 – Incident Review

This needs to be completed within 7 days of the incident being reported

Remedial and future Actions being undertaken to prevent this incident from re-occurring?

What actions are being taken?	Date actioned	Date planned	Lead Officer	Completed Date

Describe what lessons have been learnt:	
Head of Service / Service Managers Name:	
I agree that the above is a true and correct record of the incident and accept to undertake corrective actions as specified	Signed: Date:

Part 4 – Sign off and Completion

This should be completed within 10 days of the incident being reported

	Name	Signature	Date
GCL/BM			
Director			
STHCE			

Version Control

Version Number	Date	Comments	Author
1.0 (Draft)	July 2014	First draft for review	AD

Section 4 - Subject Access Request Procedure and Form

This guidance aims to assist staff to deal with requests for information covered by the Data Protection Act 1998.

Individuals have a right under the Act to make a request in writing for a copy of the information that we hold about them on computer and in our manual filing systems. This is called a subject access request (SAR). They are also entitled to be given a description of the information we hold, what we use it for, who we might pass it on to, and any information we have about the source of the information.

All subject access requests received by Six Town Housing should be passed immediately to the Governance and Compliance Lead.

Six Town Housing have produced a Subject Access Request Form and explanatory notes that can be issued to anyone who wishes to make request for their personal information (these people are identified as the Data Subject under the legislation). However, other forms of written request may be accepted if sufficient details are provided to enable us to recognise it as a Subject Access request.

This procedure should help you to deal with any subject access requests, as always if unsure, speak to Danny Lansley (ext. 8134) for advice.

1. Is this a Subject Access Request?

Once an enquiry is received a decision needs to be made about whether the person's request will be treated as a routine enquiry or as a subject access request. Any enquiry that asks for information citing the Data Protection Act or Freedom of Information Act, is in some cases a simple request for service.

Examples of such requests might be:

- Can you tell me what payments I have made this year on my rent account and how much I owe?
- Can you tell me the date that my introductory tenancy is due to change to a secure tenancy?
- When am I due to have new windows fitted?

The following requests are more likely to be treated as formal subject access requests:

- I don't agree with the amount of rent arrears you say I have. Please can you provide me with a detailed print out of my rent account including details of any telephone calls and home visits made?
- Please send me copies of all letters sent to me regarding ASB over the last twelve months.
- I am a solicitor acting on behalf of my client and request a copy of his house file. An appropriate authority is enclosed.

If you are in any doubt how to respond you can go back to the individual or their representative to clarify the situation. Alternatively you can speak to the Governance and Compliance Lead for guidance.

No Handle the query as part of your normal course of business.
Yes Go to 2.

2. Do you have enough information to be sure of the requestor's identity?

Often you will have no reason to doubt a person's identity. For example if a person with whom you have regular contact sends a letter from their known address it may be safe to assume they are who they say they are.

No If you have good cause to doubt the requestor's identity you can ask them to provide any evidence you reasonably need to confirm it. For example you may ask for a piece of information held in your records that the person would be expected to know (such as those used by the contact centre). Once satisfied go to 3.
Yes Go to 3.

3. Do you need any other information to find the records that they want?

No Go to 4.
Yes You need to ask the individual promptly for any other information you reasonably need to find the records that they want. You might need to ask them to narrow down their request. For example if they are asking for records of their house file, you could ask if it is relating to something specific such as rent arrears, ASB or re-housing. However, they do have a right to ask for everything we have about them and this could mean a lot of information and a very wide search. We have 40 calendar days to respond to a subject access request after receiving any further information we need. Go to 4.

4. Do we hold any information about the person?

No If we hold no personal information at all about the individual we must tell them this.
Yes Go to 5.

5. Will the information be changed between receiving the request and sending the response?

No Go to 6.
Yes We can still make routine amendments and deletions to personal information after receiving a request. However, we must not make any changes to records as a result of receiving the request, even if there is inaccurate or embarrassing information on our files. Go to6.

6. Does it include information about other people?

No Go to 7.
Yes We will not have to supply the information unless the other people mentioned have given their consent, or it is reasonable to supply the information without their consent by redacting their names or references to them. Go to 7.

7. Are we obliged to supply the information?

There may be circumstances in which we are not obliged to supply certain information. Some of the most important exemptions apply to:

- Crime prevention and detection;
- Negotiations with the requestor;
- Confidential references given by us;
- Information covered by legal privilege.

No If all the information we hold about the requestor is exempt, then we can reply stating that we do not hold any of their personal information that we are required to reveal.
Yes Go to 8.

8. Does the information include any complex codes or terms?

No Go to 9.
Yes We need to make sure that these are explained so that the information can be understood. E.g. explain all the abbreviations used on QL if sending copies of computer records. Go to 9.

9. Prepare the response

A copy of the information should be supplied in a permanent form except where the individual agrees or where it is impossible or would involve undue effort. This could include very significant cost or time taken to provide the information in hard copy form.

If there is a large amount of sensitive information, normal protocol is that the requester comes into STH to pick up the documentation and signs/dates an acceptance form. If the information is being sent via email it should be password protected.

An alternative would be to allow the individual to view the information on screen. We have 40 calendar days to comply with any request starting from when we have received all the information necessary to deal with the request.

DATA PROTECTION ACT 1998

SUBJECT ACCESS REQUEST FORM

This form is used by Six Town Housing to help you receive the information we hold and process about you, the data subject (i.e. the person whose information Is held). Six Town Housing charges an administration fee of £10 to facilitate subject access requests.

To enable us to respond efficiently to your request, please complete all of the relevant sections of the form and enclose the fee. If you are requesting the data on behalf of someone else also enclose proof that you have the authority to act on their behalf.

If you are the data subject complete sections A, B and C. If you are acting on behalf of the data subject complete sections A, B and D.

Section A – Data Subject Details

Data Subject: .....

Current Address: .....

.....

.....

.....

Post Code: .....

Email Address: .....

Contact Number: .....

Previous Address: .....

If you have moved since your details were given to Six Town Housing

.....

.....

.....

Post Code: .....

Section B – Personal Data you are Requesting

Tell us what personal data you would like to see including any relevant dates, specific information or documents:

Section C – Data Subject Declaration

I can confirm that I am the data subject and that the information provided on this form is correct:

Signed: ..... Date: .....
Name: .....

Section D – Requests made on behalf of Someone Else

Name: .....
Address: .....
.....
.....
.....
Post Code: .....
Email Address: .....
Contact Number: .....
Relationship to Data Subject: .....

I can confirm that I have been given the authority by the data subject named in section A to act on their behalf and that the information provided on this form is correct:

Signed: ..... Date: .....
Name: .....

Send the completed form and fee to –

Danny Lansley
Governance and Compliance Lead
Six Town Housing
6 Knowsley Place
Angouleme Way
Bury
BL9 0EL

Alternatively the form can be emailed to enquiries@sixtownhousing.org and payment sent to the address below or presented at the reception.

There may be occasions when we request proof of identity. An original copy must be presented to the employee dealing with your request to ensure that no data is being unlawfully disclosed.

Notes – Six Town Housing reserves the right to redact information related to third parties under Section 7 of the Data Protection Act 1998. Personal information used on this form is required to enable your subject access request to be processed, and will only be used in connection with this request.

Six Town Housing have 40 days to respond to the request from the day it is received. If clarification is sought in relation to the request this time period is deemed to have started from the day a satisfactory response is received.

Office Use Only –

Date Received: ----------
By Whom: ----------
Fee Enclosed: ----------

Section 5 - Six Town Housing – Records Management Schedule

Aim

The aim of this schedule is to determine what information should be held and how long it should be held for. It also identifies who is responsible for reviewing the information Six Town Housing holds and making arrangements for appropriate disposal.

Good records management helps us to comply any legislative or statutory requirements and fulfil our commitment to our customers as a processor of their data by only keeping what is necessary and justifiable in line with the principle of the Data Protection Act.

This schedule is based on the model schedule published by the National Housing Federation in 2013 and is not intended to be an exhaustive list of all the records, whether paper or electronic, which Six Town Housing holds but represents the most common records we hold and should dispose of on a routine basis. If the information is not listed consideration should be given to whether it 'feels right' to keep or dispose of the information and also what impact this decision will have on storage whether physical or digital.

Each member of staff is responsible for ensuring that any data they is store is, as far as possible, accurate and complete. Staff are also responsible for bringing it to the attention of their Coordinator or Business Manager when they notice that information is incorrect or incomplete.

Storage of Documents

As a provider of social housing we hold a wide range of data on our customers, properties and staff. Keeping someone's personal data for longer than needed contravenes one of the data protection principles. Therefore being proactive is managing this data is the responsibility of every member of staff as it helps to keep the organisation compliant with the Act and make the most of the physical and digital storage we have.

Email

Having a large number of emails clogs up our servers, costing the organisation money in extra storage. The configuration of Microsoft Outlook automatically erases any emails which are in your deleted items when the programme is closed but it is recommended staff routinely delete emails that are not necessary to keep (all user messages, setting up meetings, out of offices). Bear in mind that emails are also subject to Freedom of Information legislation!

Disposal of Information

All paper records which are confidential must be disposed of using the secure waste bins provided on each floor. If in any doubt air on the side of caution.

Electronic records which are deleted are done so securely. The IT infrastructure of Bury Council, of which we are a part of, has enhanced security features which protect this data once it is erased.

Abbreviations Used

CIPD – Chartered Institute of Personnel and Development

DPA – Data Protection Act 1998

IEE – Institute of Electrical Engineers

NHF – National Housing Federation

RMS – Records Management Society

Links to Other Policies/Strategies

- Data Protection Statement
- ICT Security Policy

Contact Details

For any advice about records management please speak to the Governance and Compliance Lead, Danny Lansley, who is based on 4th Floor. Email – d.lansley@sixtownhousing.org or 0161 686 8134.

Records Management Schedule

Governance Documents

Information	Information Type	Owner	Retention Period	Justification	Disposal Method
Certificate of Incorporation	E/P	Governance and Compliance Lead	Permanent	Implied by CA, Sec. 15	N/a
Memorandum and Articles of Association (Original)	E	Governance and Compliance Lead	Permanent	Best Practice	N/a
Articles of Association (Current)	E	Governance and Compliance Lead	Permanent	Best Practice	N/a
Governance Framework	E	Governance and Compliance Lead	Permanent	Company Policy	N/a
Certificate of Registration with Housing Regulator	E/P	Governance and Compliance Lead	Permanent	Best Practice	N/a
Board Member Documents – Appt Letters, Personal Details	E/P	Governance and Compliance Lead	6 Years after Board membership ceased	DPA 5th Principle Companies Act	Via Confidential Waste
Notices of Meetings	E	Governance and Compliance Lead	6 Years	In case of challenge to validity of meeting resolutions. Notice of meeting is the agenda.	Deletion
Board and Committee Minutes	E	Governance and Compliance Lead	10 Years	Companies Act 2006 s. 355 Signed copies scanned and stored electronically.	Deletion
Written Resolutions/Chair's Decisions	E	Governance and Compliance Lead	10 Years	Companies Act 2006 s.355 Signed copies scanned and stored electronically.	N/a
Management Agreement	E	Governance and Compliance Lead	Permanent	Company Policy	N/a

Registrations and Statutory Returns

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Annual Returns to the Regulator	E	Governance and Compliance Lead – Recorded through Companies House Website	5 Years	Best Practice	
Audited Company Returns and Financial Statements	E	Business Manager – Financial Services	Permanent	Best Practice	N/a
Register of Directors and Secretaries	E	Company Secretary	Permanent	Best Practice	N/a
Register of Use of Company Seal	E	Company Secretary	Permanent	Best Practice	N/a

Strategic Management

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Business Plans	E	Respective Business Manager	6 years after completion	RMS Guidelines	Via Confidential Waste
Annual Delivery Plan	E	Business Manager - BICF	6 years after completion	RMS Guidelines	Deletion
Annual Reports	E	Communications and Marketing Advisor	6 years	RMS Guidelines	Deletion

Insurances

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Current and Former Policies	E	Insurance Section – Bury Council	Permanent	Limitation can commence from knowledge of a potential claim and not the cause of the claim.	N/a
Annual Insurance Schedule	E	Insurance Section – Bury	6 Years		

		Council			
Claims and Related Correspondance	E/P	Insurance Section – Bury Council and Governance/Compliance Lead	2 Years	Zurich Municipal Recommendation	Via Confidential Waste
Indemnities and Guarentees	TBC	TBC	6 Years after Expiry	Limitation for legal proceedings is 12 years related to land.	
Employer's Liability Insurance Certificate	E	Governance and Compliance Lead	40 Years	NHF Recommendation. 2008 Regulations removed time requirement but have to be mindful of industrial disease claims.	Via Confidential Waste

Finance, Accounting and Tax Records

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Accouting Records for Limited Company	E/P	Business Manager – Financial Services	6 Years		Via Confidential Waste/Deletion
Balance Sheets and Supporting Documents	E/P	Business Manager – Financial Services	6 Years		Via Confidential Waste/Deletion
Loan Account Control Reports	E/P	Business Manager – Financial Services	6 Years		Via Confidential Waste/Deletion
Social Housing Grant Documentation	E/P	Business Manager – Financial Services	Permanent		Via Confidential Waste/Deletion
Budgets and Internal Financial Reports	E/P	Business Manager – Financial Services	3 Years	STH Financial Regulations	Via Confidential Waste/Deletion

Tax Returns and Records	E/P	Business Manager – Financial Services	10 Years	TMA. Sec. 20 may require any documents relating to tax over 6 years.	Via Confidential Waste/Deletion
VAT Records	E/P	Business Manager – Financial Services	6 Years	Customs and Excise requirements for VAT registered bodies.	Via Confidential Waste/Deletion
Orders and Delivery Notes	E/P	Business Manager – Financial Services	6 Years	Customs and Excise requirements for VAT registered bodies.	Via Confidential Waste/Deletion
Copy Invoices	E/P	Business Manager – Financial Services	6 Years	Customs and Excise requirements for VAT registered bodies.	Via Confidential Waste/Deletion
Credit and Debit Notes	E/P	Business Manager – Financial Services	6 Years	Customs and Excise requirements for VAT registered bodies.	Via Confidential Waste/Deletion
Journal Transfer Documents	E/P	Business Manager – Financial Services	6 Years	Customs and Excise requirements for VAT registered bodies.	Via Confidential Waste/Deletion
Creditors, Debtors and Cash Income Control Accounts	E/P	Business Manager – Financial Services	6 Years	Customs and Excise requirements for VAT registered bodies.	Via Confidential Waste/Deletion
Cheques	E/P	Business Manager – Financial Services	6 Years	Limitation for legal proceedings.	Via Confidential Waste/Deletion
Paying in Counterfoils	E/P	Business Manager – Financial Services	6 Years	Limitation for legal proceedings.	Via Confidential Waste/Deletion
Bank Statements and Reconciliations	E/P	Business Manager – Financial Services	6 Years	Limitation for legal proceedings.	Via Confidential Waste/Deletion
Instructions to Bank	E/P	Business Manager – Financial Services	6 Years	Limitation for legal proceedings.	Via Confidential Waste/Deletion

Contracts and Agreements

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Contracts under seal and/or executed as deeds	TBC	TBC	12 years after completion including any defect liability period.	Limitation for legal proceedings.	TBC
Contracts for the supply of goods or services including professional services	TBC	TBC	6 years after completion including any defects period.		TBC
Documentation relating to one off purchases of goods and services where there is no continuing maintenance or similar requirement	TBC	TBC	3 Years		TBC
Loan Agreements	TBC	TBC	6 years after expiry	Limitation for legal proceedings.	TBC
Rental and Hire Purchase Agreements	TBC	TBC	6 years after expiry	Limitation for legal proceedings.	TBC
Indemnities and Guarantees	TBC	TBC	6 years after expiry	Limitation for legal proceedings.	TBC
Tender Documentation – Successful tenders and associated evaluation	TBC	TBC	6 years after end of contract. 12 years after for contracts under seal	Statutory Limitations Act 1980.	TBC
Tender Documentation –	TBC	TBC	2 years after	NHF Recommendation	TBC

Unsuccessful tenders			notification.		
Service Level Agreements	E/P	Relevant Director/Business Manager	6 years	Company Policy	TBC

Application and Tenancy Records

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Applications for Housing Register	E/P	Housing Options – Bury Council	6 years after offer accepted	NHF Recommendation	
Housing Benefit Notifications			2 years	CIH Recommendation	
Rent Statements	E via QL	Rent Team Co-ordinator	6 years	Company Policy	Deletion from system
House Files	E/P	Business Manager - Neighbourhoods	6 years after tenancy ends	NHF Recommendation	Via Confidential Waste or Deletion

Vehicles

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Mileage Records	E – Trent P – Submitted on paper	Business Manager - HR	2 years after disposal	NHF Recommendation	Via Confidential Waste
Maintenance records, MOT Tests	P – Staff File	Business Manager - HR	2 years after disposal	NHF Recommendation	Via Confidential Waste

Human Resources

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Staff Records inc. Retirement Benefits	P – Locked Filing Cabinets	Business Manager - HR	During and 7 years after employment ends	Company Policy	Via Confidential Waste
Terms and Conditions of Service – Both general and those applying to individuals	P – As part of Staff File E - Trent System	Business Manager - HR	During and 7 years after employment ends	Company Policy	Via Confidential Waste
Service Contracts for Directors	P – As part of Staff File E - Trent System	Business Manager - HR	During and 7 years after employment ends	Company Policy	Via Confidential Waste
Remuneration Package	P – As part of Staff File E - Trent System	Business Manager - HR	During and 7 years after employment ends	Company Policy	Via Confidential Waste
Training Records	P – Staff File	Business Manager - HR	During and 7 years after employment ends	Company Policy	Via Confidential Waste
Shortlists, Interview Notes and Application Forms – Successful Candidates	P – Staff File	Business Manager - HR	During and 7 years after employment ends	Company Policy	Via Confidential Waste
Application Forms of Non-shortlisted Candidates	P – Locked Filing Cabinet	Business Manager - HR	6 Months	NHF Recommendation	Via Confidential Waste
CRB/DBS Clearance Documentation – Names of	E	Business Manager - HR	During and 7 years after	Company Policy Can be held longer under	Deletion

those who hold clearance			employment ends	Section 122(2) of Police Act 1997	
Employer/Employee Committee Minutes	E	Executive Support	Permanent	CIPD Recommendation	N/a

Information relating to payroll/tax is held by Bury MBC under a service level agreement.

Health and Safety

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Medical Records Relating to the Control of Asbestos	E – Q Drive P – Staff File	Business Manager - HR	40 Years	NHF Recommendation. See note in Insurance Section	Via Confidential Waste
Health and Safety Assessments (Corporate)	E	Health and Safety Advisor	Permanent	NHF Recommendation	Delete
Health and Safety Assessments (Individual Staff)	P – Staff File	Health and Safety Advisor	During and 7 years after employment	Company Policy based on NHF Recommendation.	Via Confidential Waste
Health and Safety Policy Statements	E	Health and Safety Advisor	Permanent	NHF Recommendation	
Accident Records and Reports	P – Staff File	Business Manager - HR	During and 7 years after employment	Company Policy and RIDDOR	Via Confidential Waste
Sickness Records	E – Trent HR System P – Staff File	Business Manager - HR	During and 7 years after employment	Company Policy	Via Confidential Waste
Health and Safety Statutory Notices	E	Health and Safety Advisor	6 years after compliance	NHF Recommendation	Deleted from Drive

Strategies and Policies

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Company Policies	E	Relevant Business Manager	5 Years for previous versions	RMS Guidelines	Deletion
Company Strategies	E	Relevant Business Manager	5 Years for previous versions	RMS Guidelines	Deletion

ASB and Enforcement Action

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
ASB Case Material	E/P	ASB Coordinator	TBC	TBC	TBC
High Level Domestic Violence Cases (MARAC)	E/P	ASB Coordinator	TBC	TBC	TBC
Court Documents for Rent Arrears	E/P	Rent Team Coordinator	Until tenant evicted	No longer needed after eviction	Deletion or Via Confidential Waste
Notice Seeking Possession	E	Rent Team Coordinator	12 Months	Not valid after this period.	Deletion or Via Confidential Waste

Complaints, Compliments

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Stage 1 Complaints	E	Customer Involvement, Regulation and Improvement Lead	5 Years – unless vexatious	Company Policy	Deletion
Stage 2 Complaints	E	Customer Involvement, Regulation and Improvement Lead	5 Years – unless vexatious	Company Policy	Deletion

Information Security

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Subject Access Requests	E	Governance and Compliance Lead	Destroy when no longer needed	Company Policy – Judgement to be made depending on circumstances of request	Deletion
Freedom of Information Requests	E	Governance and Compliance Lead	6 Years	Company Policy	Deletion
Data Security Breach Forms	E	Governance and Compliance Lead	Permanent	Company Policy in case of any legal action resulting.	N/a
Information Sharing Protocol's	E	Governance and Compliance Lead	6 years after scheme to which ISP relates has finished.	Data Sharing Code of Practice 2011	Deletion

Leaseholders

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Leases and Service Charge Data	E/P	Business Manager – Financial Services	6 Years	Company Policy	Via Confidential Waste/Deletion
Leasehold Property Information	E		Permanent	Part of Housing Management System	

New Housing Development

Information	Electronic or	Owner	Retention	Justification	Disposal

	Paper		Period		Method
Documents relating to building of new homes	E/P	Director of Assets	12 Years after settlement of all issues	Limitation for legal action relating to land or contracts under seal	Via Confidential Waste

Property Records

Information	Electronic or Paper	Owner	Retention Period	Justification	Disposal Method
Repairs Information	E	Business Manager – Repairs Direct	6 years	Limitation for legal proceedings	Deletion
Asbestos Survey Records	E	Business Manager – Sustainability and Investment	Permanent	Good practice	N/a
Asbestos Removal Records	E	Business Manager – Sustainability and Investment	Permanent	Good practice	N/a
Void Inspection Records	E	Business Manager – Repairs Direct	6 years after tenancy ends	Held as part of house file	Deletion
Cyclical Maintenance Records	E	Business Manager – Sustainability and Investment	Permanent	Good practice	N/a
Gas Safety Certificates	E/P	Contract Coordinator - Heating	Min 3 years	Gas Safety (Inst. & Use) Regulations 1998 ** Also held by Sure Group contractor*	Deletion or Shred
Building Regulation Certificates	TBC	TBC	TBC	TBC	TBC
Electrical Inspections	E – Written certificates scanned to Q Drive or submitted to NIC EIC cloud system	Contract Coordinator - Electrical	10 Years	IEE Guidance Note 3	Deletion if stored on Q Drive

Property Adaptations	E	Business Manager – Sustainability and Investment	Permanent	Good practice	N/a
Fire Safety Checks – Communal Blocks	TBC	TBC	TBC	TBC	TBC
Fire Risk Assessments – Communal Blocks	TBC	TBC	TBC	TBC	TBC
Legionella Checks – Sheltered Housing	TBC	TBC	TBC	TBC	TBC
PAT Testing Records for Furnished Properties	E	Tenancy Sustainment Advisor	3 Years	Electrical Regulations	Deletion

Section 6 – Advice for Staff/Tenants

What is the Data Protection Act 1998?

This is an Act that came into force on the 1st March 2000. It protects personal data about individuals (that is you and me) whether processed by computer or manually, what the data is processed for and who processes it.

How does it protect your personal data?

The Act sets out rules and conditions which Six Town Housing, as a user of personal data, must obey when obtaining and using information about you. The Act also provides you with certain rights that Six Town Housing must respect.

What are your rights?

- to ask Six Town Housing if it holds personal information about you
- to ask what Six Town Housing uses the information for
- to be provided with a copy of the information
- to be given details about the purposes for which Six Town Housing uses the information and details of other organisations or persons to whom the information is disclosed
- to ask for incorrect data to be corrected
- to ask Six Town Housing not to use personal information about you
    - for direct marketing
    - if it is likely to cause damage or distress
    - to make decisions about you based on the automatic processing of the data
- to be compensated for damage or distress should these be caused by Six Town Housing's failure to comply with certain requirements of the Act

Why does Six Town Housing keep personal information?

Personal data is required so that we can provide you with the services you require or that Six Town Housing is required to undertake. Examples of these include collection of rents, calculation of benefits and maintaining a record of services provided.

Does Six Town Housing need your consent to use data about you for any of these purposes?

Six Town Housing needs your consent if we are going to process personal data about you for purposes other than required by law or where we intend using the data required for one legal purpose for another purpose. Application forms and requests for information explain why we require the information.

How do you make a request to see information about you?

Six Town Housing has a standard application form that sets out what information you need to provide to make a request for information. We may upon receipt of this form ask you for further detail to either enable us to locate the information or verify that you are the person to whom the data relates.

What information will be provided?

All information that Six Town Housing holds about you both on computer and in manual files in respect of the purpose(s) you requested will be provided together with a list of others to whom the data is disclosed and information about sources of the data.

How will you be given the information

The information will be provided in the form of either a computer print out or photocopies of records and provided to you in the manner requested in the Declaration section of the Subject Access Request Form.

The information will be provided within 40 days of receipt of your application or the date that Six Town Housing received adequate information to locate the information.

What do you do if the information is incorrect?

You must advise Six Town Housing in writing advising them which information is incorrect and request that it be corrected. We must, within 21 days, tell you whether we have amended the data or if we do not agree that the original information was incorrect. In the latter instance you can

- ask Six Town Housing to record your disagreement on your record
- appeal to the Information Commissioner
- appeal to the Courts if Six Town Housing does not correct the information

What do you do if you think you have not been given all the information?

You can advise Six Town Housing in writing requesting that we re-examine your request and be provided with an amended reply. You can if you are still not satisfied appeal to the Information Commissioner who will examine the matter on your behalf.