

## **INFORMATION SECURITY POLICY REVIEW**

Report of the Chief Executive

### **1. SUMMARY**

In line with current policy, documents should be reviewed on a regular basis. This report documents the review of the Information Security Policy (ISP), Appendix 1, and the amendments made.

### **2. RECOMMENDATION**

That the Committee approves the amendments made to the ISP and agree the next review date be set for June 2014 in line with the current review policy.

### **3. MATTER FOR CONSIDERATION**

That the above mentioned policy has been reviewed and amendments have been made.

### **4. LEGAL AND CONFIDENTIALITY IMPLICATIONS**

The ISP outlines the legislation which surrounds data handling by Derby Homes' employees.

### **5. PERSONNEL IMPLICATIONS**

As outlined in the ISP in relation to responsibilities and potential sanctions for breach of the policy.

### **6. EQUALITIES IMPACT ASSESSMENT**

- Does this report affect the delivery of a service Yes
- Has an Equality Impact Assessment been completed Yes (attached as Appendix 2).

### **7. RISK IMPLICATIONS**

Derby Homes has highlighted the need for this ISP as part of its risk management strategy.

## 8. POLICY REVIEW IMPLICATIONS

This is a key policy of Derby Homes and is included in the Key Policy Review Schedule. In accordance with minute 10/51 this policy will be reviewed no later than 3 years from the date of this meeting.

The areas listed below have no implications directly arising from this report:

- Consultation
- Financial and Business Plan
- Environmental
- Health & Safety

If Board members or others would like to discuss this report ahead of the meeting please contact the author, or Phil Davies, Chief Executive, [phil.davies@derbyhomes.org](mailto:phil.davies@derbyhomes.org) – Phone: 01332 888528

Author: Mark Fairweather/IT Manager/01332888601/ [mark.fairweather@derbyhomes.org](mailto:mark.fairweather@derbyhomes.org)

Background Information: Previous ISP

Supporting Information: None.

Formatted: Centered



Formatted: Font: 24 pt

Formatted: Right

## INFORMATION SECURITY POLICY

Version 2.03.1

Document owner	<del>John Cornall, Assistant Director, ICT</del> <u>Mark Fairweather, IT Manager</u>
Document author and enquiry point	<del>Alison Jones</del> <u>Mark Fairweather, IT Security Officer</u> <del>Manager</del>
<del>Document authoriser</del>	<del>Mike Thompson, Head of ICT</del>
Date of document	September, 2003
Version	<u>2.03.1</u>
<del>Document classification</del>	<del>Internal</del>
<del>Document distribution</del>	<del>Internal</del>
Document retention period	Until date of next review
<del>Document approval date</del>	
Review date of document	<del>September, 2004</del> <u>June, 2011</u>
<del>Derby Homes edition</del>	<del>January 2004</del>
<del>Derby Homes Resources, Remuneration and Regeneration Committee</del>	<del>25 March 2004</del> <u>July, 2011</u>
<del>Derby Homes Board</del> <u>Date of next review</u>	<del>29 April 2004</del> <u>June, 2014</u>

Formatted: Font color: Auto

Formatted: Font color: Auto

Formatted: Font color: Auto

Formatted: Font color: Auto

Formatted: Font color: Auto

Document Review: ~~September 2003~~ June, 2011

### Summary of changes

Section <del>3</del> <u>Number</u>	<del>Scope</del> <u>Heading</u>	<del>3.3 Reference to Governing Bodies included</del> <u>Amendment</u>	<del>Requested by Corporate Personnel and Unions</del> <u>Reason For Amendment</u>
Section <del>5</del> <u>Various</u>	<del>Responsibilities and accountabilities</del> <u>Various</u>	<del>5.1 Reference to Assistant Director ICT included</del> <u>Removed Derby City Council References</u>	<del>Change in</del> <u>Policy now the responsibility of Derby Homes</u>
Section <del>7</del> <u>4</u>	<del>Virus protection</del> <u>Direction and Vision</u>	<del>Reference to public folders removed</del> <u>Re-Written to reflect Derby Homes' vision statement</u>	<del>To encourage use of Derbynet</del> <u>Council vision statement removed</u>
Section <del>13</del> <u>8.2</u>	<del>Other relevant policies, standards and procedures</del> <u>Sub section to 8 on Training</u>	<del>Updated list of documents. Reference to public folders removed</del> <u>Deleted</u>	<del>Self explanatory</del> <u>Awareness training reference not required</u>
Section <del>15</del> <u>10</u>	<del>Document version control</del> <u>Business continuity</u>	<del>Reference to public folders removed</del> <u>Re-written</u>	<del>To encourage use of Derbynet</del> <u>Plain English statement replaced longer complicated section</u>
Section <del>16</del>	<del>Version history</del>	<del>Updated</del>	<del>Self explanatory</del>



## CONTENTS

<b>1. Introduction</b>	<b>5</b>
<b>2. Definition</b>	<b>5</b>
<b>3. Scope</b>	<b>5</b>
<b>4. Direction and vision</b>	<b>5</b>
<b>5. Responsibilities and accountabilities</b>	<b>6</b>
<b>6. Compliance with legal and contractual requirements</b>	<b>6</b>
<b>7. Virus protection</b>	<b>7</b>
<b>8. Information security education and awareness training</b>	<b>7</b>
<b>9. Incident management</b>	<b>7</b>
<b>10. Business continuity and risk management</b>	<b>8</b>
<b>11. Compliance with the Information Security Policy</b>	<b>8</b>
<b>12. References</b>	<b>8</b>
<b>13. Other relevant policies, standards and procedures</b>	<b>8</b>
<b>14. Contact details</b>	<b>9</b>
<b>15. Document version control</b>	<b>9</b>
<b>16. Version history</b>	<b>9</b>

Formatted: Font: Bold, No underline,  
Font color: Auto

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

## 1. Introduction

The purpose of information security is to protect the highly valued information assets of Derby Homes, and the Council,~~and Derby Homes,~~. The objective is to reduce the risk of security incidents and be able to demonstrate to the citizens of Derby that we collect, handle and store their information securely. It also shows a commitment by Derby Homes, and the Council,~~and Derby Homes~~ to process information in line with relevant legislation and e-Government requirements.

## 2. Definition

2.1 The International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management defines Information Security as protecting three aspects of information:

- **confidentiality**- making sure that information is accessible only to those authorised to have access
- **integrity**- safeguarding the accuracy and completeness of information and processing methods
- **availability**- making sure that authorised users have access to information and associated resources when required.

2.2 Information Security is put into practice through appropriate controls, which will be a combination of policies, procedures, standards, guidelines and physical or hardware/software measures.

## 3. Scope

3.1 Information is in many forms. It can be:

- stored on computers, on removable media, on laptops and mobile phones
- sent across networks, including our partners and IT Companies
- printed out
- written on paper, published on the Web, our Intranet and other formats
- spoken.

3.2 Information Security covers the safekeeping of all forms of information to protect its confidentiality, integrity and availability.

3.3 The policy applies to all Derby Homes employees, including Board Members who may have authorized access to Derby Homes and Council IT systems.

## 4. Direction and vision

~~The Council's~~Derby Homes' vision ~~statement~~ is citizen-centred to enhance their participation in- "To secure the best future for Council

~~Housing tenants and services in Derby". and access to local and national government services. We want Derby's citizens, visitors, voluntary groups and businesses to be better informed, involved and, where possible, empowered by implementing electronic government. This means we must make sure our citizens in Derby".~~ Maintaining tenants information in a secure way is therefore a high priority. In so doing, tenants can have trust and confidence in the way we handle, store, share and use ~~our~~their information ~~assets~~.

## 5. Responsibilities and accountabilities

5.1 ~~The Council's Assistant Director for ICT~~ Derby Homes' IT Manager has responsibility for defining and setting ~~the Council's, and therefore~~ Derby Homes', security policies, standards and procedures. Every IT system user is responsible and accountable for putting into practice these policies, standards and procedures. Whilst these should be specific to Derby Homes, they must be broadly in line with those of Derby City Council (DCC), best practise and current legislation.

5.2 **Information Security is not an option.** We are all required to keep a minimum level of security to meet our legal and contractual obligations.

Formatted: Font: Not Italic, No underline, Font color: Auto

5.3 Derby Homes works with the Council and other partners to deliver its IT and Housing Services. All such partners are required to comply with Derby Homes' rules and policies on Data Protection and this requirement is included in any IT procurement process and contracts.

5.4 It will be the responsibility of the immediate line manager of any member of staff who leaves the employment of Derby Homes to notify the IT section so that the network access for that member of staff can be disabled. Any laptop, mobile phone and memory stick should be immediately returned.

## 6. Compliance with legal and contractual requirements

6.1 ~~The Council, and~~ Derby Homes, has an obligation to make sure that all information systems and processes meet the terms of all relevant legislation and contractual requirements, including the:

- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000.

6.2 If you are not sure of your responsibilities under any of these laws, contact the ~~Council's IT Security Officer~~IT Manager for further information.



- 6.3 The ~~Council's~~ IT ~~Security Officer~~ Manager has specific responsibility for the Data Protection Act ~~notification~~ Notification to the Office of the Information Commissioner.

## 7. Virus protection

Everyone has a responsibility to make sure that the ~~Council~~ Derby Homes and DCC network and IT systems, ~~and this includes Derby Homes,~~ stay virus free by complying with the ~~Council's and Derby Homes'~~ Homes Anti-Virus Policy.

To make sure you are using the current version of this policy please check on Derby Homes' ~~public folders in Outlook, at controlled documents site on DHnet and use the search word VIRUS.~~

Formatted: English (U.S.)

~~<Outlook://Public Folders/All Public Folders/DERBY CITY COUNCIL/Derby Homes/IT Unit/IT Policies/>~~

To ensure that data is further protected, Derby Homes will restrict the issue of memory sticks to devices capable of being encrypted. No unencrypted memory sticks will be allowed. Any document received via a third party should be virus checked prior to being opened.

## 8. Information security education and awareness training

- 8.1 All **line managers** must make sure that employees who have authorised use of ~~the Council's and~~ Derby Homes' IT systems have adequate and appropriate training on:

- operating the technology and information systems provided
- understanding the security risks to their information systems
- using the security features provided with their information systems
- choosing, managing and protecting passwords
- preventing the malicious spread of software and data, for example computer viruses and chain e-mails
- identifying and protecting important, sensitive, personal or confidential data or records from loss, destruction and error
- ensuring the physical security of their desktop, laptop and other information assets
- identifying and reporting ~~\*security incidents~~ (See in Appendix 1).

~~\*An Information Security incident is an event that compromises the confidentiality, integrity or availability of information or information assets, having an adverse affect on security, reputation, performance or ability to meet regulatory or legal obligations~~

- 8.2 The IT ~~Manager~~ Security Officer will continually review the level of awareness of Information Security within ~~Derby Homes~~ the Council and arrange awareness training when necessary.

## 9. Incident management

- 9.1 All security incidents must be logged with the IT ~~Unit and the IT Security Officer~~Manager. See Appendix 1 for examples of security incidents.
- 9.2 It is the aim of ~~the Council, and thereby~~ Derby Homes, to capture and record all incidents so they can be managed successfully and lessons can be learned.
- 9.3 All incidents will be monitored and investigated if necessary and the IT ~~Security Officer~~Manager will report to ~~the~~ Chief ~~Officers, Executive, Personnel and/or~~ Line Managers ~~and/or personnel~~ as appropriate.

## 10. Business continuity and risk management

~~The Council's, and therefore Derby Homes', critical business data must be identified, by way of a Risk Assessment, then restored and maintained as quickly as possible following a major disaster or failure that affects essential services or facilities. Anite have plans in place to recover Revenues and Benefits systems and Capita have plans in place to recover CODAS, SWIFT, AMPS and ACADEMY should a disaster occur, however, there are nominated officers responsible for making sure there are up-to-date **business continuity plans** in place in each department. The Council's Risk Management Officer can advise on individual departmental plans. Make sure you know what to do if a disaster or major systems failure occurs. Derby Homes' ability to recover data lost due to accident or malicious removal/alteration is covered in a service level agreement with their outsourced facilities management company.~~

## 11. Compliance with the Information Security Policy

- 11.1 The IT ~~Security Officer~~Manager is responsible for monitoring compliance with this policy.
- 11.2 If employees knowingly do not comply with Derby ~~Homes~~Homes' policies, procedures or guidelines, Derby Homes may take appropriate action under the Disciplinary Procedure.

## 12. References

ISO/IEC 17799:2000 Part 1-2 Code of Practice for Information Security Management, available from BSI Customer Services, 389 Chiswick High Road, London W4 4AL

## 13. Other relevant policies, standards and procedures

E-mail & Internet User Policy  
Data Protection Act Policy  
Anti-Virus Policy  
E-mail and Internet Monitoring Policy  
Software Licensing Policy

~~To make sure you are using the current version of these policies please check on Derby Homes' public folders in Outlook, at~~

~~<Outlook://Public Folders/All Public Folders/DERBY CITY COUNCIL/Derby Homes/IT Unit/IT Policies/>~~

#### 14. Contact details

~~Please contact the Council's IT Security Officer on 25 6262 or by email to [alison.jones@derby.gov.uk](mailto:alison.jones@derby.gov.uk), or anyone in the Central IT Unit with enquiries about this policy or any other referenced policy, procedure or law.~~

##### ~~Central IT~~

~~Head of IT 25 5565  
Business Analyst 25 6260  
IT Contracts Officer 25 6204  
IT Security Officer 25 6262~~

##### ~~Derby Homes IT~~

~~Systems Co-ordinator 71 1040  
Systems Co-ordinator 71 1165  
Systems Co-ordinator 71 1168  
Computer Projects Officer 71 1039  
IT Manager 71 1132  
Systems Administrator 71 1038  
**The IT Manager 888601**~~

#### 15. Document version control

To make sure you are using the current version of this policy please check on Derby Homes' ~~public folders in Outlook, at~~controlled documents site on DHnet and use the search word SECURITY.

Formatted: English (U.S.)

~~<Outlook://Public Folders/All Public Folders/DERBY CITY COUNCIL/Derby Homes/IT Unit/IT Policies/>~~

#### 16. Version history

Date Issued	Version	Status	Reason for change
4 Feb 2003	1.1	Issued	Section 5.1

19 Sept 2003	2.0	Issued	Reviewed and updated
<u>16 July 2009</u>	<u>3.0</u>	<u>Controlled</u>	<u>Controlled</u>
<u>22 June 2011</u>	<u>3.1</u>	<u>Draft for approval by RR&amp;R committee</u>	<u>Reviewed and updated</u>

Please tell useus if you need this in large print, on audio tape, computer disc or in Braille. You can contact the Equalities Unit IT Manager on 25 5384 ~~or on minicom 01332 258427~~ ~~or fax 25 6223888601~~.

## Appendix 1

### SECURITY INCIDENTS

An incident is defined as:

*'An information security incident is an event that compromises the confidentiality, integrity or availability of ~~the Council's~~ Derby Homes' information or information technology assets, having an adverse impact on ~~the Council's~~ Derby Homes', security, reputation, performance or ability to meet regulatory or legal obligations.'*

Incident reporting involves a variety of differing situations and two categories are described below.

**High level categories** would include such things as:

- system malfunctions
- loss of services, equipment or facilities
- degradation of the service
- access violations

- loss of Confidentiality, Integrity or Availability.

**Low level categories** would include such things as:

- virus infections
- loss or theft of PC/laptop or information
- password compromise
- misuse or abuse of the system
- backup failure and loss of data
- unauthorised access to premises or systems.

These lists are not comprehensive because, in reality, there may be a combination of any of the above categories – for example, the loss of a laptop and written notes detailing passwords would enable unauthorised access to systems and subsequent misuse or abuse.

If you can't decide if something falls within one of the categories, log it anyway.

# Equality impact, needs and requirements assessment form

Please use this form to record your findings, proposed actions, equality objectives and targets. Use the guidance notes to help you do the assessment or contact the Equality Standard Project Manager if you need some advice

## About the policy, practice, service or function you are assessing

Name of policy, practice, service or function: Information Security Policy

Assessment team leader name: Mark Fairweather

Date of assessment: 21/06/11

Department responsible: Derby Homes

Service Area: Derby Homes

Other members of assessment team:

Name	Position	Area of expertise	Comments

Question	Response/ findings
What are the main aims and objectives or purpose of the policy, practice, service or function that you are assessing?	To set out the Information Security Policy for Derby Homes
Who implements, carries out or delivers the policy, practice, service or function? Please state where this is more than one person, team, department, or body – and include any outside organisations who deliver under procurement arrangements	Derby Homes staff Capita Serco
Question	Response/ findings
Who is affected by the policy, practice, service or function, or by how it is delivered? Such as, who are the external and internal customers, groups, or communities?	All employees Tenants Capita Serco Staff from DCC including Revenues and Benefits Section and retained Housing
What outcomes do we want to achieve, why and for whom? For example, what do you want to be providing, how well, what changes or improvements, and what should the benefits be for customers, groups or communities?	Continuation of service to tenants
Question	Response/ findings
What existing or previous inspections of the policy, practice, service or function are there? For example, Best Value Inspections, policy reviews, research into the effects of a policy or practice.  What did they tell you?	This is the second review of this policy.

---

## Identifying potential equality issues and factors

Question	Response/ findings
What do you already know about the equality impact or need? For example, from research, feedback, consultation or any performance monitoring	Not applicable to this policy document
Question	Response/ findings
Is there any evidence of higher or lower take up under the policy or practice, or of the service or function for any particular groups? For example, who uses the service, who doesn't and why not?	Not applicable to this policy document.
Have there been any important demographic changes or trends locally? For example is the population changing, and if so, how and what might that mean for the service or function?	Not applicable to this policy document
Question	Response/ findings
Is there an indication that any of the policies or practices involved with the service or function creates particular problems or difficulties for any groups of customers or communities?	There has been one incident where a tenant enquired whether under the Data Protection act their data could be shared with third party IT companies. This is actually a condition of the tenancy agreement each tenant signs and Derby Homes ensures that any third party company handling data is bound by our policies and the data protection act.
What information or data exists? For example, statistics, customer feedback, complaints, research, monitoring – who keeps it and can you get hold of it?	Not applicable to this policy document



Question	Response/ findings
Does any equality or diversity objectives already exist? If so, what are they and what is current performance like against them?	Not applicable to this policy document
Is the service having a positive or negative effect on particular people in the community, or particular groups or communities?	Not applicable to this policy document

## Collecting the information and data about how the policy, practice, service or function, impacts on communities

Please record your information and data in this table and think about:

- what information or data you will need
- using both quantitative and qualitative data
- making sure that where possible there is information that allows all perspectives to be considered
- identifying any gaps in the information/ data and what it can tell you

Data or information	When and how was it collected?	Where is it from?	What does it tell you? You need to consider all six equality strands where you can	Gaps in information
Customer feedback and complaints	NA			
Consultation and community involvement	NA			
Performance information including Best Value	NA			
Take up and usage data	NA			
Comparative information or data where no local information	NA			
Census, national or regional statistics	NA			

<b>Data or information</b>	<b>When and how was it collected?</b>	<b>Where is it from?</b>	<b>What does it tell you? You need to consider all six equality strands where you can</b>	<b>Gaps in information</b>
Access audits or assessments such as DDA assessments	NA			
Workforce profile	Personnel			
Where service delivered under procurement arrangements – workforce profile for deliverers	NA			
Monitoring and scrutiny outcomes	Resource, Remuneration and Regeneration Committee	Minutes		

## Analysing the information and data and setting equality objectives and targets

Please give your detailed findings in this table

Service or function	Policy or practice	Findings	Which groups are affected and how	Whose needs are not being met and how?

## Objectives - process, impact or outcome based

Please give your proposed objectives/ targets in this table

<b>Objective/Target:</b>	<b>None Identified in this strategy document</b>
Specific	
Measurable	
Achievable	
Relevant	
Timed	

<b>Objective/Target:</b>	
Specific	
Measurable	
Achievable	
Relevant	
Timed	

<b>Objective/Target:</b>	
Specific	
Measurable	
Achievable	
Relevant	
Timed	

## Monitoring and reviewing - incorporating into performance management

Please summarise your objectives and targets in this table with your proposed monitoring and reporting arrangements

Objective	Planned action	Target performance			Responsible lead officer	Reporting cycle, for example, quarterly
Review	To be reviewed in line with next planned review of the strategy	<b>2014</b>			IT Manager	Every three years