

ORIGIN HOUSING LIMITED

Data Protection Policy

1. INTRODUCTION

Purpose

- 1.1** This document sets out Origin Housing Limited's policy with regard to data protection and applies to all subsidiaries and associated entities. Origin recognises the importance of respecting the personal privacy of all our tenants, residents, customers and employees. We also recognise the need to build in appropriate safeguards during the collection, storage, processing and utilisation of personal data. This policy will be reviewed at least annually by the Company Secretary.
- 1.2** Origin Housing Limited is registered with the Information Commissioner (Registration No. Z6107036). Its registration can be viewed at <http://www.ico.gov.uk/ESDWebPages/DoSearch.asp>

Scope

- 1.3** This policy applies to all staff, but particularly those who deal with personal data.

2. REFERENCES

- 2.1** This policy must be read with other documents on the O Net, namely:
- Keeping Our Information Secure – Guidelines for Staff

- Subject Access Requests – Procedure Note for responding to requests from individuals to see their personal file
 - Origin's Document Retention & Archive Policy
 - Disciplinary Procedure
 - IT Induction Manual
- 2.2 The Information Commissioner's website also has useful guidance and good practice notes on the Data Protection Act, including guidance on disclosing information about tenants for landlords; outsourcing; employee references; privacy & electronic communications; information standards with examples, and the rights of individuals. Follow the link on the O Net/General Information.

3. DEFINITIONS

The legislation contains terms that have specific meanings which it is important that managers and staff are aware of. The relevant terms and definitions are set out below.

- 3.1** Data Subject - This is the person about whom the personal data relates.
- 3.2** Data Controller - This is the person or organisation who determines the purpose and manner in which personal data is processed. At Origin, the data controller is Origin Housing Limited.
- 3.3** Personal Data – This is data relating to a living person who can be identified
- a) from the data or
 - b) from the data and other information which we have in our possession or likely to have in the future.
- 3.4** Sensitive Personal Data – this is personal data about a person's
- racial or ethnic origin
 - political opinions
 - religious or other beliefs

- trade union membership
- health, physical or mental
- sexual life
- offences, committed or allegedly committed, or
- details of proceedings for offences

3.5 Data Processing – this means obtaining, recording or holding information (or data) or doing things with it, such as organising, adapting, altering retrieving, disclosing disseminating, erasing or destroying it.

3.6 Data Subject's Consent – the Act defines "the data subject's consent" as:-

"...any freely given specific and informed decision of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." The fact that the data subject must "signify" their agreement means that there must be some active communication between the parties. Therefore Origin cannot infer someone has given their consent if they have not responded to a letter, email, leaflet etc.

3.7 Explicit Consent – this means that the consent of the data subject must be absolutely clear. This is particularly important when processing sensitive personal data.

3.8 European Economic Area (EEA) – Countries within the EEA are Belgium, Denmark, Germany, Spain, France, Greece, Italy, Ireland, Luxembourg, The Netherlands, Austria, Portugal, Sweden, United Kingdom, Norway, Iceland and Liechtenstein. Switzerland and Hungary have been deemed by the European Commission to provide an adequate level of protection, but this list is subject to change. Please contact the Company Secretary for further advice.

3.8 Fair Processing Code – as far as practical, we shall provide data subjects with:

- the identity of the data controller (Origin Housing Limited)
- if it has nominated a representative for the purposes of the Act, the identity of that representative,

- the purpose(s) for which the data is intended to be processed, and
- any further information which is necessary, taking into account the specific circumstances, to enable the processing to be fair.

3.9 Third Party – another person or organisation apart from the data subject and the data controller. Third parties can include (but are not restricted to) suppliers and providers of goods or services to Origin, debt collection and tracing agencies, local authorities, health authorities, the police, Government departments including Her Majesty's Revenue & Customs, auditors, Housing Ombudsman, relatives, guardians or other people associated with the data subject.

4. THE POLICY

4.1 It is Origin's policy to comply with the legislation. All staff must be aware of the eight principles of the Act set out below and comply with them at all times. Any breach of the Act may result in disciplinary action being taken against the member of staff. For further information, please see Origin's Disciplinary Procedure.

4.2 **1st Principle: Personal Information must be fairly and lawfully processed.**

4.2.1 This means that Origin must have legitimate reasons for collecting and using personal data. We must process information in accordance with the Fair Processing Code (see definition in 3.8 above) and must not use the data in ways that would have an unjustified or adverse effect on the individual concerned. We will be open and honest about how we intend to use the data.

4.2.2 We shall give individuals appropriate privacy notices when collecting their personal data, handle their data only in ways they would reasonably expect, and make sure we do nothing unlawful with the data. We shall explain why we are collecting the information, who it will be shared with, and the

general circumstances where we will disclose without their consent (see 6 below) to specific third parties.

4.2.3 Origin Housing is registered under the DPA as a data processor. The register entry describes in general terms the purposes for which we collect data, who we collect data about, and who we share this data with. Our registration is reviewed annually. If there is any doubt about the legality of information collected, please check with the Company Secretary. Privacy statements must be emphasised when collecting personal information and there must be a statement detailing why data is being collected.

4.2.4 In general terms, if a third party asks for information, the third party must prove that they are authorised to do so, for example the data subject has given their explicit consent (see 3.7 above) in writing. Consent must also be obtained when taking photographs of people to use in brochures etc.

4.3 2nd Principle: Personal information must be processed for limited purposes

4.3.1 Information must only be processed according to the purposes set out in our registration. Our registration lists the following:

- Property management
- Research
- Staff, Agent and Contractor Administration
- Associated Welfare Services, Advice and Support
- Accounts and Records
- Crime Prevention and Prosecution of Offenders
- Fundraising
- Administration of Shareholders, Board Members and Loan Stock Holders

4.3.2 If in doubt, check with the Company Secretary.

4.4 3rd Principle: Personal information must be adequate, relevant and not excessive.

4.4.1 All files with personal information must be regularly reviewed (at least annually) to ensure compliance and the fact that a review has taken place documented with details of who conducted the review and when. Origin's Document Retention/Archive Policy on the O Net (General information/Data Protection) sets out how long information should be kept. Information must not be kept for longer than the agreed limit.

4.4.2 All Managers must ensure there are departmental procedures in place to review files on a regular basis, with responsible people identified.

4.5 4th Principle: Personal information must be accurate and up to date.

4.5.1 All files must be regularly reviewed to ensure accuracy and kept up to date. Historical information must be reviewed to ensure it is still correct. Where inaccurate records cannot be altered eg on Orchard, notes must be added to the record clarifying any inaccuracy in the record.

4.6 5th Principle: Personal information must not be kept longer than is necessary.

4.6.1 Origin's Document Retention & Archive Policy sets out how long information shall be kept.

4.6.2 All Managers must nominate a responsible person for archiving or disposing of departmental records and include this in their Success Factors' objectives.

4.7 6th Principle: Personal information must be processed in line with that person's rights.

4.7.1 An individual has a legal right to see what information we hold on them. Under the Act, a request to see their personal file must be in writing, together with the £10.00 administration fee. This is known as a "subject access request" under the legislation and there is a separate procedure note on the O Net (General information/Data

Protection/Subject Access Request Procedure) dealing with these requests. Any employee who receives a subject access request must notify the Company Secretary who will co-ordinate Origin's response.

4.7.2 Other rights under the Act include:

- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- right to object to decisions being taken by automated means;
- right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;
- a right to claim compensation for damages caused by a breach of the Act

4.8 7th Principle: All personal information must be secure.

4.8.1 Information held on computer must be secure, with passwords and only accessible to relevant staff. Information held in hard copy must be secure in a lockable cabinet. Separate guidance is available on the O Net to keep our information secure (General Information/Data Protection/Keeping Our Information Secure).

4.8.2 When outsourcing the processing of information on behalf of Origin, Managers must:

- choose a data processor providing sufficient guarantees in respect of security measures they take;
- take reasonable steps to ensure compliance with those measures (for example, a periodic audit), and;
- ensure the processing is undertaken under a written contract under which the data processor is to act only on instructions from Origin Housing Limited. The contract must require the data processor to comply with all the obligations imposed on Origin by the 7th Principle.

4.8.3 The Head of ICOS is responsible for ensuring that adequate security software is installed and operating to safeguard the

privacy of Personal Data held by the organisation in an electronic form.

4.8.4 Managers are responsible, working in conjunction with ICOS, for ensuring that only those members of staff who need access to Personal Data held by the organisation to perform their jobs have access to it.

4.9 8th Principle: Information must not be transferred to other countries without adequate protection.

4.9.1 Information shall not be transferred to other countries outside the European Economic Area. It can only be sent to a country outside the EEA if that country ensures an adequate level of protection for the rights and freedoms of individuals in relation to processing personal information. Any requests to transfer data to other countries regardless of whether they are within the European Economic Area or not must be referred to the Company Secretary.

5 Roles and Responsibilities

5.1 The Company Secretary is responsible for:

- Overseeing the Origin data protection system and ensuring compliance with the Act is monitored and maintained.
- Completing the organisation's Notification to the Information Commissioner and ensuring that operational processing of personal data is consistent with the Notified purposes.
- Conducting spot checks and reporting to the Risk Assessment Panel on process & procedural implementation and potential breaches.
- Receiving reports of potential breaches, weaknesses, concerns and requests for assistance.
- Maintaining a log of potential breaches
- Co-ordinating Origin's response to a subject access request.

5.2 Departmental Managers/Senior Management Team are responsible for:

- Ensuring processes are documented and include staff instructions/procedures that embed Data Protection obligations into working practices
- Ensuring all forms (electronic or paper) used within their department only collect personal data that is necessary for the service being provided, and that they contain approved Fair Processing Notices to the Data Subject. In particular to ensure that departmental forms do not collect excessive or irrelevant personal data, and not to allow that data to be used or disclosed to any third party, or for any additional or other purposes other than those previously advised to the Data Subject on collection. If in future additional processing becomes necessary, to ensure that the Data Subject is subsequently informed.
- Ensuring all completed forms used for the collection of personal data are signed to indicate the Data Subject's consent.
- Ensuring staff are fully aware of their obligations (see 5.3 below) and are appropriately supervised.
- Ensuring staff receive appropriate training to enable them to comply with this policy.
- Ensuring staff are only granted access to IT systems and manual files containing personal data required to perform their duties.
- Reviewing files on a regular basis (at least annually) and maintaining records of the review of the file.
- Nominating a responsible person for archiving or disposing of departmental records in line with Origin's Document Retention & Archive Policy.
- Assessing and approving home-working, mobile working or any work containing personal data to be performed outside of the normal office environment and ensuring that staff have appropriate IT equipment (eg encrypted laptops or secure remote access).
- Ensuring personal data used or acquired within their department is not input into any external databases, online systems or new data repositories without the recipient system having gained prior approval of the Head of ICOS.
- To seek written assurances that within supplier contracts that no aspect of processing, or support for systems utilised

for the processing, is performed from offshore locations outside of the EEA.

- Reporting any potential breach of the Act to the Company Secretary and, if the breach relates to personal information held in electronic form, to the Head of ICOS.

5.3 Staff are responsible for

- Reporting any incidents, concerns or suggestions for improvement to their Head of Department, or in confidence to the Company Secretary and Head of ICOS.
- Informing their Manager if they are unsure how to comply with departmental procedures, particularly when asked to disclose personal data to a third party.
- Being familiar with Origin's IT Security policies and acceptable use of IT systems, including restrictions on including/sharing personal data in unencrypted email attachments, protection of passwords and files.
- Obtaining their Manager's approval for any work involving personal data to be conducted outside the office unless this is performed using a Company encrypted laptop or via Secure Remote Access.
- Notifying the Company Secretary and Head of Department of any Subject Access Request.

6. Exemptions & Legitimate Grounds for Disclosure

6.1 Personal information can be shared without an individual's knowledge in cases where, for example, personal data is processed for:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; or
- the assessment or collection of tax or duty.

6.2 In these circumstances Origin would be exempt from the fairness requirements of the DPA, but only if, by telling the individual concerned, it would prejudice the investigation. For example, the police might ask Origin to give them information about an ex-employee who they suspect of being involved in a serious assault. If by informing the ex-employee that we have given the police this information,

Origin tips off the individual, this is likely to prejudice the investigation because the individual may abscond. In these circumstances, Origin does not have to tell the individual about the disclosure of information.

- 6.3 In some cases the sharing of data is required by law, for example under the Money Laundering Regulations 2007 – these allow financial institutions to share personal data with law enforcement agencies in certain circumstances. Such legal requirements override an individual's consent or objection.
- 6.4 The Company Secretary (and/or appropriate Executive Director?) shall be informed of all decisions taken to share personal information without the individual's consent, including reasons for the decision, so that the circumstances can be recorded in case of challenge.

APPENDIX 1

A summary of the legislation including the eight principles is set out below.

- 1** The Data Protection Act 1998 places a special responsibility on those obtaining data to ensure it is captured fairly and only used for the purpose for which it was collected.
- 2** There are eight principles in the Act which apply to all personal data processed by data controllers who must comply with them.
- 3** The first principle states that 'Personal Data shall be processed fairly and lawfully.' It also states that personal data shall only be processed if at least one of the following conditions is met:
 - The data subject has given their consent to the processing
 - For the performance of a contract to which the data subject is a party; or for the taking of steps with a view to entering into a contract (with the data subject's request).
 - To comply with any legal obligation.
 - To protect the vital interests of the data subject.
 - For the administration of justice, or exercise of any function relating to a government department or conferred by an enactment.
 - For the legitimate interests of the data controller.
- 4** Sensitive personal data shall only be processed if at least one of the above conditions is met, together with at least one of the following:
 - The data subject has given their explicit consent.
 - To comply with the law regarding employment.
 - To protect the vital interests of the data subject where consent cannot be obtained or has been unreasonably withheld.

- The processing is in relation to the activities of a political, philosophical, religious body or trade union and which is established or conducted not for profit; safeguards the rights and freedoms of data subjects; relates to members of that body or those with regular contact with it; it does not involve disclosure to third parties without the data subject's consent.
 - The information in the personal data has been made public as a result of steps taken by the data subject.
 - For legal proceedings, or obtaining legal advice, or establishing, exercising or defending legal rights.
 - For the administration of justice, conferred by or under any enactment or for the exercise of any function or a government department.
 - For medical reasons it is undertaken by a health professional or similar.
 - Consists of information about racial or ethnic origin that is to be used to promote or maintain equality of opportunity and is carried out with appropriate safeguards.
 - The processing is undertaken in circumstances specified in an order made by the Secretary of State.
- 5** The second principle 'Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes'.
- 6** The purpose for which data is obtained is defined in the Act as either by means of;
- a notice given by the data controller to the data subject in accordance with the fair processing code which gives the information needed to comply with the Fair Processing Information), or
 - a notification given to the Commissioner under the notification provisions of the Act. The purposes for which Origin obtains information is set out in the Information Commissioner's register.

- 7** The third principle states, 'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.'
- 8** The fourth principle states 'Personal data shall be accurate and where necessary kept up to date.'
- 9** It is the responsibility of the data controller to take 'reasonable steps' to ensure the accuracy of the data and that if the data subject updates the data this is corrected. This means that it is not enough to assume data accuracy by saying that because the information came from the data subject it is accurate.
- 10** The fifth principle states 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'
- 11** The sixth principle 'Personal data shall be processed in accordance with the rights of data subjects under this Act.'
- 12** A person will contravene this principal if they -
 - fail to supply information pursuant to a subject access request under the Act
 - fail to comply with various sections of the Act relating to the right to prevent processing likely to cause damage or distress; the right to prevent processing for the purposes of direct marketing; or the right in relation to automatic decision taking.
- 13** The seventh principle states that "Appropriate technical and organisational measure shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.' All personal information must be secure. " .
- 14** The Act states that appropriate security measures must ensure a level appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

- 15** The Act is specific regarding data processors, writing on behalf of the data controller. Data controllers must:
- choose a data processor providing sufficient guarantees in respect of security measures they take;
 - take reasonable steps to ensure compliance with those measures, and;
 - ensure the processing is undertaken under a written contract under which the data processor is to act only on instructions from the data controller.
- 16** The eighth principle 'Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.'

