Data Protection Policy

Department: Company Secretary

Author: Caroline Waterer, Company Secretary

Date Issued: February 2016

Date Last Updated: February 2016

Date of next review: February 2017

Version: 0.2

Approved by: Chris Trebilcock & SMT

Date approved: 3 February 2016

Version Control

Item	Reason for Change	Officer/Manager	Version	Date
1	New format & guidance on data sharing	Caroline Waterer	0.1	4/12/14
2	Additional purpose for CCTV use; Changes to O Net	Caroline Waterer	0.2	14/1/16
3	Reference to new CCTV Policy	Caroline Waterer	0.3	11/2/16

Related Documents

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
- CCTV Policy
- Origin's Document Retention & Archive Policy
- Origin's Supplier Compliance Questionnaire
- Disciplinary Procedure
- IT Induction Manual
- Disposal of Hardware & Software Policy and Procedure
- Records Management Policy

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. https://ico.org.uk/for_organisations/data_protection

Legislative and Regulatory Framework

This policy is in line with the principles set out in the Data Protection Act 1998

Appendices

None

1. Policy Statement

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, utilisation and destruction of personal data. Our policy is to comply with the eight principles of the Data Protection Act.

2. Scope of the Policy

This policy applies to all staff, but particularly those who process personal data. The policy applies to all subsidiaries and associated entities.

3. Definitions

The legislation contains terms that have specific meanings which it is important that managers and staff understand. 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 controllers are Origin Housing Limited and Origin Housing 2 Limited.

3.3 Data Processor – This is the person or organisation that processes personal information. This can be the Data Controller (Origin Housing or Origin Housing 2) or it can be a contractor or supplier who processes the information on our behalf (eg Gilmartins, Capita, Orchard Information Systems)

3.4 Personal Data – This is data which can identify a living person or data which, along with other information, can identify a living person. It includes information in electronic and paper form, photographs, recordings and CCTV images.

3.5 Sensitive Personal Data – this is personal data about a person's:-

- race or ethnic origin
- political opinions
- religious or other beliefs of a similar nature
- trade union membership
- physical or mental health
- sex life

- offences, committed or allegedly committed
- details of criminal proceedings

There is the potential for this type of personal data to cause damage or distress or prejudice to the rights of individuals if it is not processed correctly. However, there are times when sensitive personal information will be processed in everyday life, eg the need for a wheelchair, or special dietary needs.

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

3.7 Data Sharing – this is where various Data Controllers with their own database exchange information directly with other Data Controllers.

3.8 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.

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

3.10 European Economic Area (EEA) – Countries within the EEA are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK. 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.

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

- the identity of the data controller (Origin Housing Limited or Origin Housing 2 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.

3.12 Privacy Notice (or Fair Processing Notice) – this is the notice given to the Data Subject by the Data Controller when collecting personal information. As a minimum, it should tell people who we are (OHL or OH2), what we are going to do

with their information and who it will be shared with. A privacy notice should be genuinely informative and reassure people that they can trust us with their personal information.

3.13 The Act means the Data Protection Act 1998.

3.14 Third Party – another person or organisation apart from the data subject, the data controller, and the data processor. 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. Origin's Policy

4.1 It is Origin's policy to safeguard people's personal data and ensure that it is only used for the purpose intended. When recruiting staff, managers must take reasonable steps to ensure the reliability of any employee who has access to personal data.

4.2 Where processing is carried out by a data processor on Origin's behalf, the contract manager must ensure that:

- the data processor provides sufficient guarantees regarding their technical and organisational security measures governing the processing
- The contract manager takes reasonable steps to ensure compliance with those measures.
- the processing is carried out under a written contract where the data processor is to act only on Origin's instructions and the contract requires them to comply with Principle 7 Security (see below).
- The data processor has completed Origin's Data Protection Supplier Compliance form satisfactorily, (available on the O Net)

4.3 All staff must comply with the legislation and be aware of the eight principles of the Act which are set out below. Any breach of the Act may result in disciplinary action being taken against the member of staff. For further advice on data protection, please contact the Company Secretary.

4.4 **1st Principle: Personal Information must be fairly and lawfully processed.**

This means that Origin must have legitimate reasons for collecting and using personal data. Privacy notices must be provided to the data subject when collecting any personal data. We must not use or share the data in ways which are not specified in the notice, or which would have unjustified adverse effect on the person concerned. To process personal data lawfully, one of the following conditions must be met:

- the data subject has given their consent to the processing;
- the processing is necessary for the performance of a contract;

- the processing is necessary for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary to protect the vital interests of the data subject (life or death situation but could also extend to circumstances involving serious or substantial damage to an individual's property. For example if the property owner was on holiday and there was a strong smell of gas, therefore a need to enter the property without the knowledge or consent of the owner.)

In addition to the above, if the information being processed relates to sensitive personal information, one of the following conditions must also be met:

- the person's explicit consent must be obtained in writing and they must have been appropriately informed of all relevant information about the proposed processing before consent is given;
- the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on Origin in connection with employment;
- to protect the vital interests of the data subject or another person. This again refers to a life or death situation but this condition is extended to include the vital interests of another person, so potentially benefitting the wider community. An example is where a data subject has a communicable disease and another person is in danger of infection. This condition can only be invoked when (a) consent cannot be given by or on behalf of the data subject; or (b) Origin cannot reasonably be expected to obtain the consent of the data subject or (c) in the case concerning the protection of the vital interests of another person, consent by or on behalf of the data subject has been unreasonably withheld.
- The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

Origin Housing and Origin Housing 2 are both registered with the Information Commissioner under the DPA as data controllers. Origin Housing Limited's registration No. is Z6107036 and Origin Housing 2 Limited's is ZA003434. Both registrations can be viewed at http://www.ico.gov.uk/ESDWebPages/DoSearch.asp

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.

4.5 2nd Principle: Personal information must be processed for limited purposes

Information must only be processed according to the purposes set out in our registration. Our registration states that we process personal information to enable us to provide social housing accommodation and services which include:

- letting, renting and leasing properties
- Administering waiting lists
- Carrying out research
- Administering housing and property grants

- Providing associated welfare services, advice and support
- Maintaining our accounts and records
- Supporting and managing our employees, agents and contractors

We also process personal information using CCTV systems to monitor and collect visual images for the purpose of security and the prevention and detection of crime; and for the purpose of management of staff and volunteers.

When collecting personal information, we must be clear from the outset why we are collecting the information and provide appropriate privacy notices. We must process information in accordance with the Fair Processing Code and must not use the data for another purpose or in ways that would have an unjustified or adverse effect on the individual concerned. We must be open and honest about how we intend to use the data.

If you wish to use or disclose personal data for a purpose that was not contemplated at the time of collection (and therefore not specified in a privacy notice), you must obtain consent from the data subject for the additional purpose. If in doubt about the purpose, please check with the Company Secretary.

4.6 **3rd Principle: Personal information must be adequate, relevant and not excessive.**

Only relevant personal information must be collected in order to fulfil a specified purpose. This means that any information collected has to be adequate but not excessive – the minimum amount in order to meet the particular purpose.

4.7 **4th Principle: Personal information must be accurate and up to date.**

All files must be reviewed once a year to ensure accuracy and kept up to date. Historical information must be reviewed to ensure it is still correct. Where inaccurate historical records cannot be altered eg on Orchard, notes must be added to the record clarifying any inaccuracy in the record. It is the responsibility of staff to ensure that their personal information on CIPHR is accurate and kept up to date. Tenants should be reminded annually to keep their personal information up to date through the Self Service Portal.

4.8 **5th Principle: Personal information must not be kept longer than is necessary.**

Origin's Document Retention & Archive Policy sets out how long information shall be kept. Information must not be kept for longer than the agreed limit. If personal information has been obtained for validation purposes, you should consider whether it needs to be kept permanently on file. CCTV footage is generally kept for no longer than 30 days.

Departmental Managers must nominate a responsible person for archiving or disposing of departmental records and include this in their Success Factors' objectives. All Managers must ensure there are departmental procedures in place to review files at least annually, with responsible people identified.

4.9 **6th Principle: Personal information must be processed in line with that person's rights.**

An individual has the following legal rights:

- A right of access to their personal data
- A right to prevent processing likely to cause damage or distress
- A right to prevent processing for purposes of direct marketing
- Rights in relation to automated decision-making.

The damage or distress caused must be "unwarranted and substantial" and the right does not apply if the individual has given their consent to the processing, or if it is necessary for the performance of a contract, or to comply with any legal obligation. Individuals can only claim compensation if they can prove they have suffered damage (but not distress).

Data subjects should have the maximum visibility of the processing which relates to them – in other words, we should be transparent and open about what information is held and how it is processed.

All staff must be made aware of the procedure to be followed when an individual requests access to their personal data. This is known as a Subject Access Request and is co-ordinated by the Company Secretary. The individual must make the request in writing and pay the £10.00 administration fee. The procedure is on the O Net and is included in the Corporate Induction programme.

4.10 **7th Principle: All personal information must be secure.**

Personal data 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 (Guidelines for Keeping Our Information Secure).

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.

The Assistant Director of IT and Office Services 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. He must be informed

of any proposal to install any CCTV system which uses cloud-based storage in order that proper compliance checks on the security of the storage can be carried out and a decision taken by the IT Department on the suitability of the system.

Managers are responsible, working in conjunction with IT and Office Services, for ensuring that access to personal data is on a "need to know" basis. This means that only those employees who need access to personal data held by the organisation to perform their jobs have access to it.

Types of controls in use at Origin include:

- password protection
- encryption
- Access smart cards
- Lockable filing cabinets
- Reception staff checking ID to gain entry

4.11 **8th Principle: Information must not be transferred to other countries without adequate protection.**

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.

4.12 **Roles and Responsibilities**

4.12.1 The Company Secretary is responsible for:

- Overseeing the Origin data protection policy 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.

4.12.2 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 appropriate Privacy 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's consent is obtained prior to the processing.

- 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 Assistant Director of IT and Office Services. This would also cover cloud-based CCTV systems.
- 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 Assistant Director of IT and Office Services.

4.12.3 SMT and the Company Secretary are jointly responsible for deciding whether to disclose personal information to a third party without the data subject's consent.

4.12.4 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 Assistant Director of IT & Office Services.
- 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.

4.12.5 **Exemptions & Legitimate Grounds for Disclosure**

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.

4.12.5 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. The exemption also prevents a data subject who may be subject to a major criminal investigation from making a subject access request and getting access to criminal intelligence information about him. 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.

4.12.6 Any request from the Police to disclose personal information without the individual's consent must be made in writing from a senior police officer, Inspector level or above.

4.12.7 Any decision to disclose personal information without the data subject's consent must be taken by the appropriate SMT member and the Company Secretary. The appropriate Executive Director must also be informed. The Company Secretary will keep a log of all decisions taken to disclose personal information without the individual's consent, including reasons for the decision, so that the circumstances can be recorded in case of challenge.

4.13 Data Sharing

4.13.1 Origin has a number of Data Sharing protocols in place with other data controllers, eg local authorities. When deciding whether to enter into an arrangement to share personal data with another data controller, the following should be considered:

- What is sharing meant to achieve?
- What information needs to be shared?
- Who requires access to the shared personal data?
- When should it be shared?
- How should it be shared?
- How can we check the sharing is achieving its objectives?
- What risk does the data sharing pose?

- Could the objective be achieved without sharing the data or by anonymising it?
- Does the notification to the Information Commissioner need to be updated?
- Will any of the data be transferred outside of the European Economic Area?

4.13.2 Privacy notices must be given where:

- Sensitive personal data is being shared
- The data sharing is likely to be unexpected or objectionable
- Sharing the data, or not sharing it, will have a significant effect on the individual
- The sharing is particularly widespread, involving organisations individuals might not expect
- The sharing is being carried out for a range of different purposes.

4.13.3 Consent or explicit consent from the data subject for data sharing is most likely to be needed where:

- Confidential or particularly sensitive information is going to be shared without a clear legal basis for doing so; or
- The individual would be likely to object should the data be shared without his or her consent; or
- The sharing is likely to have a significant impact on an individual or group of individuals.

5 Equality and Diversity

Origin respects the differences of our individual residents, service users and staff, and will tailor communication to the individual needs and preferences of our customers.

6 Value for Money

Not applicable

7 Resident Involvement

Not applicable

8 Monitoring

The Company Secretary is responsible for overseeing the policy and for ensuring that compliance with the Act is monitored and maintained. Members of the Senior Management team sign an annual declaration to confirm that there are procedures and controls within their department to protect personal data and that spot checks have been performed to validate those procedures and ensure procedures and controls are operating effectively.

9 Communication of Policy

This policy will be stored on the intranet and communicated through The Source and Onet News.

10 Review

This policy will be reviewed at least annually by the Company Secretary.