Confidentiality and Data Protection Policy & Procedures

Policy Details	
Date Completed/Reviewed	August 2017
Next Review Date	TBA
Overall Responsibility	Chief Executive
Author	Chief Executive
Approved By	SMT
Date Approved	TBA

1. Introduction

1.1 This Policy and procedures set the framework within which personal and sensitive personal information (data) is to be processed - collected, edited, stored, viewed, handled and disclosed or shared - in compliance with the Data Protection Act (DPA) 1998 and, from 25 May 2018, the General Data Protection Regulation (GDPR).

1.2 Under the DPA the personal data of a living individual can only be used by an organisation for precisely specified objectives and in accordance with the rights of the individual to whom the information relates. We are required to:

- Be transparent and fair to the individuals whose personal information is being requested or held.
- Collect only the information necessary for a particular purpose.
- Make sure that only those who need the information and are legally entitled to have it, have access to it.
- Keep personal information private and securely stored, and delete it when no longer needed in relation to the purpose(s) for which it was collected.
- Comply with the law regarding the processing and disclosure of information.

The Data Controller and Data Processor

1.3 The Data Controller is an individual or an organisation who decides the manner and purpose of how personal data is processed. The Data Processor is an individual or organisation that processes personal data on behalf of, and under instructions from the Data Controller.

1.4 Data protection obligations mainly fall upon the data controller. In most cases Solon will act as a data controller when collecting and using tenants' personal data. However, in some cases, we may also act as a data processor, or we may share personal data with an external contractor who is acting as a data processor for Solon.

1.5 There are important implications for Solon in terms of compliance and legal liability, depending upon whether we act as a data controller or data processor and in relation to any data processors we appoint to act on our behalf.

1.6 The starting point is that, wherever personal data is processed, the Data Protection Act 1998 and GDPR will apply.

2. What constitutes information or data?

2.1 Information or data can be divided into two categories:

Personal information

This is information that relates to a living individual who can be identified from the information and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Examples may include a person's name and address, IP address, phone number, email address, date of birth, next of kin, details of support services provided and any expression of opinion about an individual subject relating to this person.

Where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data"

Sensitive personal information aka special categories of personal data

Sensitive personal data is defined as any information consisting of personal information such as racial or ethnic origin of the data subject, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, details pertaining to sexual life or sexual orientation, and the alleged commission of any offence or any proceedings for any offence committed or alleged to have been committed.

As this is sensitive personal data it must be treated very carefully. The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.

3 Definition of data storage and access

3.1 Non-sensitive and sensitive personal information may be stored and accessed in a number of ways:

- Stored on computer, including word, excel, UH2, email documents and other computer records.
- Faxes and phone system.
- Manual records which are structured and accessible, anything that becomes part of our filing system.
- Information processed and stored by a computer bureau.
- Information received from third parties including accessible records i.e.:
    - a health record that consists of information about the physical or mental health or condition of an individual, made by or on behalf of a health professional in connection with the care of that individual.
    - An accessible public record that consists of information held by a local authority for housing or social services purposes.

4 Definition of data subjects

4.1 Data subjects are likely to include:

- Tenants.
- Relatives of tenants (where their personal details are held by Solon).
- Other, non-tenant, occupants of the property
- Solon's staff.
- Individuals employed by suppliers or third parties who provide outsourced services e.g. payroll or secure waste disposal, for example.
- Consultants.
- Individuals who fall into the above category but who have moved on e.g. ex-tenants or staff who are still living but whose personal data is still held by Solon.

5 Definition of data processing

- Collecting.
- Editing.
- Retaining/storing.
- Disclosing or sharing.
- Deleting/erasing/destroying.
- Viewing (looking at data on screen or on paper).
- Archiving.
- Listening to

5.1 A comprehensive list of examples of the type of information housing associations can legitimately collect from tenants is set out at Appendix 1. This includes a wide variety of sensitive and non-sensitive data. It is noted that there is not an automatic right to collect all of this data. It must be treated as set out below.

6. How should Solon process data under the DPA and GDPR?

6.1 All personal and sensitive information relating to residents, applicants, staff and Board Members that is not a matter of public record will be handled in accordance with **Schedule 1** to the DPA which lists the data protection principles as follows:

1) To register with the UK regulator, (the information commissioner's office or ICO), to inform the ICO of our processing and pay the requisite fee.

2) To comply with the following data protection principles:

- Data should be processed lawfully, fairly and in a transparent manner and, in particular, shall not be processed unless (a) at least one of the grounds or conditions of Schedule 2 is met, (**for non-sensitive personal data**) and (b) in the case of **sensitive personal data**, at least one of the grounds or conditions in Schedule 3 is met **in addition** to a schedule 2 ground.

  See Schedule 2 and Schedule 3 grounds at **7.2** and **7.8** below.

- Personal data shall be collected only for specified, explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Personal data shall be adequate, relevant and limited to what is necessary in relation to purposes for which they are processed.

- Data is to be accurate and, where necessary, kept up-to-date. Every reasonable step must be taken to ensure that personal data that is inaccurate having regard to the purposes for which it is processed is erased or rectified without delay.

- Data is to be kept no longer than necessary for the purposes for which it was processed and destroyed when no longer required.

- Personal data shall be processed in accordance with the rights of data subjects under the DPA.

- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical organisational measures.

- Personal data is to be treated as confidential at all times.

- Data will not be transferred to a country outside the EEA, unless that country provides an adequate level of protection in the opinion of the Information Commission.

- Data will not be revealed to third parties without the authority of the person to whom it refers except to comply with a statutory requirement or a court order, or where there is a clear health and safety risk or evidence of fraud.

- The Data Controller will be responsible for, and able to demonstrate compliance with the above principles.

3) To be transparent to data subjects about the nature of the processing of their personal data.

6.2 When processing or disclosing any personal or sensitive personal information, staff must ensure that they meet these data protection principles, and the conditions and procedures set out below. Further guidance and information on the principles can be found on the Information Commission website: www.informationcommissioner.gov.uk

6.3 Any breach in the policy could have very serious consequences for an individual or for Solon and could be treated as a serious disciplinary matter.

7.0 The conditions for data processing

7.1 The first data protection principle requires that Solon satisfies one or more "conditions (grounds) for processing" in relation to our processing of non-sensitive and sensitive personal data. Many (but not all) of these conditions relate to the purpose or purposes for which we intend to use the information.

Non-sensitive personal data - (Article 6 GDPR)

7.2 Unless a relevant exemption applies, at least one of the following conditions must be met whenever we process non-sensitive personal data:

- The individual whom the personal data is about has given consent to the processing. This has been freely given, was fully informed, specific to circumstances and there was a positive indication of wishes, and this was confirmed by the completion and signing of an **Informed Consent Form**. See **8.0** below.

- The processing is necessary for the performance of a contract with the individual or taking steps at his/her request with a view to entering into a contract (i.e. a tenancy agreement)

- The processing is necessary to comply with a non-contractual legal obligation (e.g. data sharing with LAs under the Care Act 2014 in relation to vulnerable individuals).

- The processing is necessary to protect the "vital interests" of the individual or another person. This only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.

- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. This may be administering justice, or for exercising statutory, governmental, or other public functions (for example where a landlord collects data to fulfil a statutory duty)

- The processing is necessary for the purpose of **legitimate interests** pursued by the controller or third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

What is the "legitimate interests" condition?

7.3 The DPA recognises that we may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. For example as a landlord. The "legitimate interests" condition is intended to permit such processing, provided we meet certain requirements.

7.4 The first requirement is that we must need to process the information for the purposes of our legitimate interests or for those of a third party to whom we disclose it.

7.5 The second requirement, once the first has been established, is that these interests must be balanced against the interests of the individual(s) concerned. The "legitimate interests" condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual.

7.6 Our legitimate interests do not need to be in harmony with those of the individual for the condition to be met. However, where there is a serious mismatch between competing interests, the individual's legitimate interests will come first.

7.7 Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the wider data protection principles i.e. data is accurate, up-to-date and not excessive.

7.8 In determining if we have a legitimate reason for processing personal data, the best approach is to focus on whether what we intend to do is fair. If it is, then we are very likely to identify a condition for processing that fits our purpose.

Sensitive personal data - (Article 9 GDPR)

7.9 At least one of the conditions listed above must be met whenever we process personal data. However, if the information is sensitive personal data, at least

one of the following conditions must also be met before the processing can comply with the first data protection principle:

- The individual whom the sensitive personal data is about has given explicit consent to the processing, (unless reliance on consent is prohibited by law), and has signed an Informed Consent Form

Or where:

- The processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- The processing is necessary to protect the "vital interests" of the individual or another person where the data subject is physically or legally incapable of giving consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- For administering justice or for exercising statutory, governmental, or crown functions.
- Processing is necessary for reasons of substantial public interest on the basis of EU or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of EU or Member State law or a contract with a health profession.

Vulnerable tenants and the need for their consent

7.10 Some tenants will require more assistance in order to maintain their tenancies. Where we are providing additional services to vulnerable tenants we are likely to be processing much more sensitive personal data relating to social services data, health data or probation service data etc. This is a situation where the processing of tenants' sensitive personal data may require the explicit consent of those individuals.

7.11 Developing and maintaining the trust of vulnerable tenants will be vitally important in obtaining such consent which will, in turn, enable Solon to provide housing management and support services which are geared towards their needs. In addition, giving them the opportunity to give their informed consent in such cases is more likely to lead to a relationship with Solon built on trust.

Definition of consent

7.12 The European General Data Protection Regulation defines an individual's consent as:

"Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." (Article 4(11))

7.13 The ICO has said that the fact that an individual must 'signify' their agreement means that there must be some active communication between the parties. An individual may 'signify' agreement other than in writing, but organisations should not infer consent if an individual does not respond to a communication – for example, from a tenant's failure to return a form or respond to a leaflet. Consent must therefore be freely given, specific and informed. If tenants don't have a real choice about whether or not their personal data is processed, and if they aren't able to withdraw consent if they want to, without detriment, then any 'consent' they may have given will not meet the requirements of the DPA.

7.14 Being able to satisfy a condition for processing will not on its own guarantee that the processing is fair and lawful – fairness and legality must still be looked at separately. So it makes sense to ensure that what we want to do with personal data is fair and lawful before worrying about the conditions for processing set out in the Act.

8.0 Obtaining consent to process data – The Informed Consent Form

8.1 Where consent is required to process information, particularly non-sensitive personal information, this should be obtained at the point at which this data is collected. This will enable us to explain to the subject in detail what information is needed, how we will use it and who will see it. Consent should be signified in writing, via the completion and signing of Solon's Informed Consent Form (attached as Appendix 2)**.**

9.0 Transparency to data subjects about the nature of the processing of their personal data – The Privacy Notice

9.1 Whenever Solon collects new personal data from tenants or other data subjects, then provided that there are appropriate grounds to do so, such as consent, this can be done – as long as fair processing information is provided at this point, usually in the form of a Privacy Notice or statement. This is to ensure that tenants are informed of the following:

- Whether any personal or sensitive data is held.
- A description of the personal data.
- Identity of the data controller.
- Purpose of the processing and lawful basis for it.
- The legitimate interest of the controller or third party.
- Any recipient of the personal data.
- The anticipated retention period.

- Existence of each data subject's rights including right to access, complain, withdraw consent at any time, where relevant. (See 10 below).
- Source of the personal data and whether it comes from publicly accessible sources.
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data.

9.2 The above information should be provided via Solon's Privacy Notice. (Attached as Appendix 3) This is not an authorisation or consent form. Everyone being asked to provide, or offering personal information should receive or see a copy of this notice.

9.3 Solon should issue a Privacy Notice whenever personal data is collected and processed. The starting point of a Privacy Notice should be to tell people the points set out at 9.1 above. These are the basics upon which all privacy notices should be built. However, we should also tell them more than this where we think that not doing so will make our processing of that information unfair. This could be the case if an individual is unlikely to know that we use their information for a particular purpose or where the personal data has been collected by observation or inference from an individual's behavior.

9.4 To help us decide what we need to include, we should map out how our information flows through Solon and how we process it, recognizing that we might be doing several types of processing. We should work out:

- What information we hold that constitutes personal data.
- What we do with the personal data we process.
- What we actually need to carry out these processes - a privacy impact assessment can help us to answer this question (See section 20).
- Whether we are collecting the information we need.
- Whether we are creating derived or inferred data about people, for example by profiling them; and
- Whether we will be likely to do other things with the data in the future – this can be particularly important if we are undertaking large scale analysis of data, as in big data analytics.

9.5 When explained in sufficiently broad terms a Privacy Notice can allow for development in the way we use personal data, whilst still providing individuals with enough detail for them to understand what we will do with their information. However, we should not draw up a long list of possible future uses if, in reality, we do not intend to process personal data for those purposes.

9.6 Solon should also display a wider all-encompassing Privacy Statement on the website to give customers more information about the type of data we might need to process and why.

10.0 Rights for tenants (and others) under the DPA - See ICO guidance notes

10.1 Data subjects such as tenants have the following rights under the DPA in relation to their own personal data held by their landlord

- ***Right to be informed***

This is the information we should supply and when individuals should be informed, as set out at 9.1 above:

- ***Right of access to personal data***

Individuals such as tenants have the right to obtain:

- Confirmation that their data is being processed.
- Access to their own personal data so they are aware of and can verify the lawfulness of processing.
- Other supplementary information i.e. the information that should be provided in the privacy notice.

Tenants have a right to make a request in writing (including via email or social media) to obtain a copy of all of their personal data. This is called a 'subject access request'.

We will provide a copy of this information free of charge, unless a request is unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with requests for further copies of the same information.

Information will be supplied within one month of receipt of the request. This can be extended by a further two months where requests are complex or numerous. However, we must write to explain why the extension is necessary within the first month.

We can refuse to respond where the request is manifestly unfounded or excessive but where we do so, we must explain to the individual informing them of their right to complain to the supervisory authority (the Information Commissioner) and to a judicial remedy within one month.

We must verify the identity of the person making the request using reasonable means.

If the request is made electronically, we should provide the information in an electronic format.

The GDPR recommends that ultimately we would benefit from providing remote access to a secure self-service system.

Further details on handling a request for access to personal data is provided under the Procedures and Guidelines for staff below. See Section 4.

- ***Right of rectification***

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If we have disclosed the personal data in question to third parties, we must inform them of the rectification where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

We must respond within one month, extendable by two months where the request for rectification is complex.

Where we are not taking action in response to a request for rectification, we must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

- ***Right to erasure (right to be forgotten)***

The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the DPA/GDPR).
- The personal data has to be erased in order to comply with a legal obligation.

Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this threshold is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and we can refuse to deal with a request.

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- The exercise or defence of legal claims.

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments. See ICO guidance.

If we have disclosed the personal data in question to third parties, we must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment who make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

While this might be challenging, if we process personal information online, for example on social networks, forums or websites, we must endeavor to comply with these requirements.

- ***Right to restrict processing***

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data, but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in future.

We are required to restrict the processing of personal data in the following circumstances.

- Where an individual contests the accuracy of the personal data, we should restrict processing until we have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If we have disclosed the personal data in question to third parties, we must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

We must inform individuals when we decide to lift a restriction on processing.

- ***Right to data portability***

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe. This enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

The right to data portability only applies:

- To personal data an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

We must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge.

If the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible.

If the personal data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

We must respond without undue delay, and within one month. This can be extended by two months where the request is complex or we receive a number of requests. We must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where we are not taking action in response to a request, we must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

- ***Right to object***

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

If we process personal data for the performance of a legal task or our organisation's legitimate interests, individuals must have an objection on "grounds relating to his or her particular situation".

We must stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

We must inform individuals of their right to object "at the point of first communication" i.e. in our privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

10.3 The above rights must be set out in the Privacy Notice which must be signed by the resident.

11. Information to be kept confidential

11.1 All personal and sensitive information will be kept and handled confidentially, whether the information has been received formally, informally or discovered by accident. Broadly, this means:

- Anything of a personal nature (which includes racial/ethnic origin, physical/mental health and criminal record) that is not a matter of public record about a resident, applicant, staff member or Board Member.
- Sensitive organisational information which could be used to damage the association or threaten the security of property or buildings.
- Tenders and quotations for services and works.

12. Internal access to and use of personal information

12.1 Staff will generally have access to all information that they genuinely need to carry out their work, and are under a duty to respect the confidentiality of all personal information held by Solon.

12.2 Wherever possible, staff will explain the purpose of recording potentially sensitive personal information and the people likely to have access to it before it is disclosed, so that informed consent can be obtained. If this causes concern, special arrangements for recording and access will be made.

12.3 Residents will normally be referred to by reference codes rather than by name in board reports and at board meetings. Sensitive information about

properties, (such as occupancy by someone with HIV or where re-housed because of domestic violence), will be treated in the same way.

13. Disclosure – Sharing data with third parties: Landlord obligations

13.1 Solon may either receive a request from a third party or we may decide we wish to share personal data with that third party. The information shared could be that relating to any individual whose personal data is held by Solon e.g. a tenant, member of staff or a contractor or a business contact. In some cases, Solon will be required by law to share individuals' personal data and sometimes sharing can be essential to protecting a tenant from harm. In other cases, personal data is shared to gain insight into that data, for the benefit of the housing sector and/or society in general.

13.2 Sharing with third parties: examples *(NB: This is not an exhaustive list)*

- Local authorities, the police and other public bodies for the purposes of crime prevention/reduction i.e. Where there is evidence of fraud or criminal activity.
- HMRC for the assessment and collection of tax in relation to Solon's employees.
- Contractors, for example for the purposes of repairs to Solon's housing stock, i.e. the name, address, contact number and any other **relevant** personal information. Relevant personal information will be information required to ensure successful access, communication and health and safety of staff and residents.
- In connection with court proceedings or statutory action to enforce compliance with tenancy conditions (e.g., application for possession or for payment of HB direct).
- Debt collection agencies and tracing agents, to collect unpaid rent from tenants who have vacated property without paying rent due.
- Department of Work and Pensions (DWP) and local authorities for the purposes of universal credit claims.
- Local Safeguarding Authorities, for the purposes of making a safeguarding alert where there is a concern regarding the safety of a child or vulnerable adult.
- Where there is a clear health or safety risk to the resident or another person.
- To comply with section 115 of the Crime and Disorder Act 1998. This act gives organisations the power to share information with other agencies in order to tackle anti-social behaviour.
- The name of a resident and the date of occupancy to gas, electricity and water companies;
- Anonymously for bona fide statistical or research purposes, provided it is not possible to identify the individuals to whom the information relates.

13.3 Solon should, first of all, consider the capacity (under the DPA/GDPR) in which the recipient of the shared personal data is to receive the information. If the other party is a data processor, i.e. processing only on Solon's instructions and at its direction, this has significant legal implications.

- Solon will be legally responsible, not only for its own breaches of the DPA, but also for any breaches caused by the actions (or inactions) of its data processor.

- The sharing of personal data with the data processor will not, of itself, require specific legal grounds under the DPA in the same way as 'data controller to data controller' sharing. The landlord would, however, need to ensure that it has the legal grounds to process the personal data in the first place – in the way that it would need to have grounds for its own staff to process the information.

13.4 Further details are provided in the Procedures and Guidelines for staff. See Section 4.

14. Disposal of personal information

14.1 When no longer required, all personal information, including computer printouts of rent accounts and arrears, will be shredded or destroyed.

15. Supported housing projects

15.1 Residents in shared housing are likely to be aware of personal information about other residents and are expected to respect their right to privacy.

15.2 Special considerations may apply to projects providing sensitive services, e.g., with neighbours and media coverage. Everyone concerned with the project must ensure that confidentiality is not compromised.

15.3 Residents should be made aware that for management/health and safety reasons, information told to individual staff members could be shared within the project's staff teams. This may include volunteers.

15.4 Residents should also be aware that certain information they give to staff about other residents could, after a thorough and fair investigation, be acted on. This should be carried out in such a way as not to jeopardize the safety of the informant or discriminate against the residents concerned.

15.5 If a resident has an official visit which means disclosure is needed to comply with the law, or a court order, or where a search warrant is produced for the resident, the staff should co-operate with the officers in question and, if appropriate will mediate for both parties. Staff should be present during any searches.

16. Responsibility for implementation

16.1 It is the responsibility of all staff to ensure that they deliver their respective services in accordance with this policy and the associated procedures. Board Members are also expected to comply with this policy.

16.2 It is the responsibility of Solon's Directors and Managers to ensure that the policy and procedure guidelines are adhered to.

16.3 The Data Protection Officer (currently the Finance Director) is responsible for overseeing compliance with the policy and with the DPA and GDPR.

16.4 The Data Protection Officer is also responsible for ensuring that Board Members comply with the policy

16.5 All staff and Board Members will be informed of their duties and provided with practical procedural guidelines. Training will be made available on the operation of the policy to all staff responsible for handling confidential information. It will also be included as part of the induction programme for new staff. Ongoing training will be arranged, as updates and changes are made to the legislation.

16.6 All contractors and agents working for Solon will be bound by the policy in the same way as direct employees.

16.7 All staff, applicants, residents and agencies with whom Solon works will be informed about the policy.

17. Monitoring

17.1 Files will be monitored on an ongoing basis to ensure that they comply with this policy.

17.2 The policy and procedure will be reviewed every three years to ensure that it is effective and complies with current good practice. A review will be carried out sooner should there be any changes to statutory requirements.

18. Equalities

18.1 In all its work, Solon will take into consideration issues that may arise when working with people of different ethnicity, religion, language, culture, gender, sexuality, physical and mental abilities.

19. Access to records Policy – records held by staff

19.1 Solon has the absolute right to access records and information held by staff and to use this access to obtain any property belonging to the association including documents and office equipment, and to ensure that staff are adhering to the association's Confidentiality and Data Protection Policy.

19.2 Further details are provided at **5.1** and **20.1** of the Procedures and Guidelines set out below.

20. Accountability and governance

20.1 The GDPR elevates the significance of the principles of accountability and transparency.

20.2 We are expected to put into place comprehensive but proportionate governance measures. Good practice tools such as privacy impact assessments and privacy by design are now legally required in certain circumstances. Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean that we produce and comply with additional policies and procedures.

- **The accountability principle**

The new GDPR accountability principle requires us to demonstrate that we comply with the principles and state explicitly that this is our responsibility. To demonstrate that we comply we must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that we comply. This may include internal data protection policies, staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include data minimisation, pseudonymisation, transparency, allowing individuals to monitor processing; and creating and improving security features on an ongoing basis.
- Use data protection impact assessments where appropriate.

- **Records of processing activities (documentation)**

As well as our obligation to provide comprehensive, clear and transparent privacy policies, as an organisation with less than 250 employees, we are only required to maintain records of activities that are:

- not occasional
- could result in a risk to the rights and freedoms of individuals; or
- Involve the processing of special categories of data or criminal conviction and offence data.

We must maintain internal records of processing activities, recording the following information:

- Name and details of our organisation (and where applicable, of other controllers, our representative and data protection officer).
- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules
- Description of technical and organisational security measures.

- **Data protection by design and by default**

Under the GDPR, we have a general obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities.

- **Data protection impact assessments**

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help us identify the most effective

way to comply with our data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

We must carry out a DPIA when:

- Using new technologies; and
- The processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- Large scale processing of special categories of data or personal data relation to criminal convictions or offences.
- Large scale, systematic monitoring of public areas (CCTV).

See ICO guidance for what information a DPIA should contain.

- **When does a Data Protection Officer need to be appointed under the GDPR?**

Under the GDPR, we must appoint a data protection officer (DPO) if we:

- Are a public authority (except for courts acting in their judicial capacity)
- Carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- Carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

The DPO's minimum tasks are:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.

21. Notification of breaches

21.1 The GDPR introduces a duty to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected

21.2 A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

21.3 We have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on

individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

21.4 This has to be assessed on a case by case basis. For example, we will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

21.5 Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly. A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

21.6 See ICO guidance for the information a breach notification should contain.

21.7 See ICO guidance for how a breach should be notified. However, a notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases. If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

21.8 Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of our global turnover.

Preparing for breach reporting

21.9 We should make sure that our staff understand what constitutes a data breach, and that this is more than a loss of personal data. We should ensure that we have an internal breach reporting procedure in place. This will facilitate decision-making about whether we need to notify the relevant supervisory authority or the public.

21.10 In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.

Confidentiality and Data Protection Procedures and Guidelines for staff

1. Introduction

1.1. Everyone who has dealings with Solon has a right to privacy and to expect that all personal information about them will be handled sensitively and confidentially.

1.2. All staff have a duty to respect the confidentiality of all personal information held by Solon. Most breaches in confidentiality happen through lack of thought or awareness of the possible consequences, or lack of private or secure facilities. The best protection is to keep the number of people who have access to sensitive information to a minimum.

2. What information is confidential?

2.1. Any personal or sensitive personal information provided by a resident or applicant, or by a third party about a resident, staff member or Board Member, should be treated in the strictest confidence. Anything seen or overheard accidentally is still personal information.

2.2. Except in the specific circumstances outlined below, no personal information may be passed on without the permission of the person concerned. Be particularly mindful in situations like relationship breakdowns, domestic violence or neighbour disputes. Even where the person requesting the information is a joint tenant or spouse, information should not be given without the resident's permission.

2.3. Some information about Solon, its projects and buildings is also sensitive and could, if disclosed, have adverse implications for the association or future occupants.

2.4. Anyone worried or distressed by something they hear or read should seek guidance and support from their manager.

3 Requests by residents and others for their own personal information

3.1 By law all residents have the right to access personal data we hold about them. Residents should be encouraged to contact us for details. They will need to show proof of identity to be provided with the information. If they find the data is incorrect, they should tell us. Solon will give access to any personal information held about a current or former resident, applicant or staff member **to the person concerned** or their authorised representative, except where:

- The information is related to, or identifies a third party who has refused their consent to the disclosure (Solon must then consider whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual).
- The information was provided by a third party on the understanding that it would not be disclosed to the person concerned.
- There is a significant risk that disclosure would cause serious physical or mental harm to the individual or another person.

- The information is subject to legal professional privilege or a statutory requirement, or is likely to lead to legal proceedings being taken.
- Revealing evidence of the commissioning of any offence, other than an offence under the Act, exposes him/her to proceedings for that offence.
- Disclosures that may prejudice the commercial or financial interests of the association.

3.2 Solon is usually contacted by residents requesting confidential information about rent levels, arrears or credits on a rent account, repairs or other matters.

3.3 We can only divulge this information to a tenancy title-holder or to someone who has the consent of the resident, i.e. legal guardian or appointee.

3.4 To enable us to identify that the person we are talking to is the resident, we must ask the caller to confirm:

- Name.
- Address including post code.
- Either their telephone number or date of birth (these details can be found in UH2).

3.5 If they are a caller to the office, then if their photograph is held on the tenancy file, this should be checked. Otherwise, some form of identification may also be provided by asking to see photographic ID such as a passport or driver's license.

3.6 If we don't have the information to check their telephone number or date of birth, or if they can't provide photographic id, then we need to ask them some questions to which only they are likely to know the answer, for example, the date they last paid the rent or their normal method of rent payment.

3.7 If this information is correctly provided then they can be given the information they want, assuming that it relates to their application for housing, their tenancy or personal support issues.

3.8 If the caller is unable to confirm details, we need to find out what they want to know, explaining that we are unable to provide details over the phone or in person as we have to be sure we are only giving information out to the right person. General advice can be given but data about the subject cannot be given out.

3.9 We may then either:

- Send the requested information to their tenancy or usual contact address.
- Arrange to meet with them to provide the information, assuming they can confirm their identity when you next meet.

3.10 All the above, assumes that the caller is not sufficiently well known to you to allow you or to another member of staff to be comfortable about identifying them on the phone or in person.

4.0 Dealing with requests for information from third parties

4.1 External organisations such as contractors or supported housing agencies providing services on behalf of Solon are bound by the confidentiality policy in the same way as direct employees. Information may be passed to them with the informed consent of residents on a strictly need to know basis in line with this policy. These guidelines deal with requests for information from other external organisations and individuals.

4.2 In general, Solon does not give out information about a resident to third parties unless we have their express authority to do so. To obtain consent please complete the Informed Consent Form at Appendix One. There will however be some circumstances when disclosure will be permitted without informed consent. This is outlined in the guidance below:

4.3 Check that the request details the information required and explains why it is required.

4.4 Check that the resident's (or staff member's) consent to disclose has been given or the request falls into one of the categories detailed below. If not, explain Solon's policy.

4.5 Establish that there is a genuine need to know.

4.6 If an organisation or individual requests information on the phone, unless you are sure of their identity, ask for their name, address and ask them to send a fax with headed notepaper.

4.7 If an official caller to the office requests information on a resident, first verify the identity of the person making the request.

4.8 Except in the circumstances detailed below make your response in writing. Always ensure a copy of what has been disclosed, or a detailed note, is retained on file.

4.9 Remember that you must comply with the Data Protection Act at all times. Computerised information may only be disclosed to people or organisations listed in our Register of Notifications.

Contractors or other agents providing services on Solon's behalf

4.10 The name, address and contact number of a resident to contactors or other agents providing services on Solon's behalf; and any special access needs to be aware of to provide a tailored service.

4.11 Our contractors sign a Data Assurance clause before undertaking work with us which states that:

The Contractor shall:

- Not use Licensed Data for any illegal, deceptive, misleading or unethical purpose or otherwise in any manner which may be detrimental to the reputation of the Association or any person;

- Use its best endeavours to use adequate technological and security measures Solon SW Housing Association may reasonably recommend from time to time, to ensure that all Licensed Data, Login Details and any other similar information (such as user names and passwords) which the

Association provides the Contractor and which the Contractor holds or is responsible for are secure from unauthorised use or access;

- Notify the Association as soon as it suspects any infringement or any unauthorised use of Login Details and any other similar information (such as user names and passwords) and give the Association all reasonably required assistance in pursuing any potential infringement or remedying any unauthorised use.

General callers (residents' friends, relatives, partners or spouses if they are not on the tenancy agreement, debt collectors, etc.)

4.12 No matter how plausible the request is, explain that Solon does not give out any personal information about residents or staff members without the data subject's consent.

4.13 Offer to forward a letter or, in genuine emergencies, pass on a telephone message, if we know the person the caller is trying to contact.

Written requests and letters

4.14 Letters from lending institutions (banks, buildings societies or loan companies) requesting a reference must be accompanied by signed and dated authorization from the person concerned. If not, write to the firm explaining that written authorization is required before a reference can be given.

4.15 Forward letters to residents with a covering letter confirming that no information has been disclosed.

Housing Benefit and Government agencies or departments

4.16 Only provide the information necessary to process a claim.

4.17 After checking the identity of the caller (if in doubt), and being given the name and address of the claimant, the following may be disclosed:

- Tenancy start date;
- The weekly or monthly rent or council tax payable;
- Details of any HB direct payments received and other benefits;
- Resident's previous address if relevant to the history of the claim.

4.18 The level of arrears may also be disclosed where Solon is seeking direct payments.

4.19 Refer requests for other information (e.g., details of sub-tenants or lodgers) to the resident, unless Solon has general written authority from the resident to act on their behalf in respect of their claim.

4.20 At sign-up, residents are asked to sign a consent form so that we can discuss their claim with HB so this should avoid future problems

Utility services i.e. electricity and water companies, British Gas, Community Charge Registration Officer

4.21 Check the identity of the caller.

4.22 You may give the following information only: name of the resident, date of commencement of tenancy, name of any previous resident and date of commencement and termination of tenancy. Do not give particulars of other residents who are not the tenants.

4.23 Do not give any forwarding addresses, but forward mail, if we have an address with a covering note.

4.24 If a resident has died, you may say so but do not give the name and address of the executor. Offer to forward letters or suggest they write to the executor at the property.

The Police

4.25 While we wish to protect the confidentiality of personal information, we also have a duty to uphold the law and do not wish to obstruct the police in carrying out their duties.

4.26 Whenever the police ask for information about a resident, try to obtain the request in writing (by letter or fax) and establish what information is required and why it is required.

4.27 Generally, only the name and address of the resident and the household composition may be divulged without a court order. Requests for any other information must be channelled through a senior manager and a detailed note of what has been disclosed retained on file. If there is a court order, insist on seeing it. We are obstructing the course of justice if a court order for information is ignored.

4.28 The above does not apply where Solon is investigating fraud or criminal activities against the association, or where threats of violence, threats to the safety of staff, or criminal damage are involved.

4.29 Refer any requests for access to association property to a senior manager.

4.30 Where a personal relationship exists with local community police, care must be taken to avoid divulging information that the police would otherwise require a court order to obtain.

Solicitors and other legal advisers

4.31 If a solicitor or other legal advisor requires information which is necessary for legal proceedings or the provision of legal advice they are entitled to this information under *section 35 of the Data Protection Act 1998*. Staff members should ensure that only information necessary for these purposes is revealed. For example, a solicitor needing advice on possession proceedings for rent arrears would not need to see documents relating to harassment. Solicitors requesting information that will not be used for the purposes of legal proceedings or the provision of legal advice will need to provide the resident's written authorisation.

Social services departments

4.32 After checking the identity of the caller (if in doubt) and ascertaining the reason for the request, the names and address of residents may be given.

4.33 In cases of suspected abuse or neglect we may decide it is necessary to disclose information. You should consult with your Manager in deciding whether to pass information onto social services. Information should only be given in the best interests of the parties involved. It should also only be shared in line with Protocols around how and when to refer.

4.34 Information sharing protocols should be read fully before making a referral. The five key points from the South West safeguarding and Child Protection Group state that:

1. Explain to people openly and honestly what information you will share, with whom and why. The only time that you should not do this is, if letting them know, will leave someone at risk of significant harm.

2. You should respect the wishes of family members if they do not want information shared unless someone will be placed at risk of significant harm if you don't share the information.

3. If in doubt speak to your manager or have a general discussion with children's services, by which we mean, one where you do not necessarily share the name of the family.

4. Make sure that the information that you are sharing is accurate, up to date, necessary for the purpose for which you are sharing it and only shared with those who need to know it. The information should also be shared securely. Having decided to share information you need not tell everyone everything.

5. You should always record the reason for your decision; whether you shared the information or not.

   The full protocol can be found at: http://www.online-procedures.co.uk/swcpp/contents/policies/sharing-information-children/

   Best practice around sharing information relating to abuse of vulnerable adults applies the same principle- that you should explain to the person what you are going to do with the information and as clearly as you can what will happen next. Some people may wish to remain anonymous, but this should not prevent you from recording the details of the allegation or suspicion of abuse.

   The full protocol for reporting this type of abuse can be found at:

   http://www.bristol.gov.uk/sites/default/files/documents/health_and_adult_care/abuse_or_neglect/safeguarding_adults/Alerters%20%26%20Reporters%20Guide%202010%20%28amended%202012%29.pdf

Medical and psychiatric information

4.35 Information about a resident's medical condition is strictly confidential to the resident, the staff concerned and/or agency providing such information to the association.

4.36 Do not pass on any information about medical condition to another agency or third party without the resident's specific consent, except in exceptional circumstances where there is a genuine health and safety risk to the person or to anyone else if the information is not disclosed. In this case, seek the guidance of your Manager.

Requests for references

4.37 If we receive requests for references e.g. from banks, building societies, loan companies, ask them to provide the resident's or staff member's written consent.

4.38 Other associations or local authorities request references when a mutual exchange application is considered. Residents should provide consent for Solon to respond when signing the application for a mutual exchange.

4.39 Local authority homeless person's units may also contact Solon to find out information as to why a former resident has left or been evicted. Once again, the written authorisation of the former resident must be provided.

MPs or other advocates contacting Solon on behalf of a resident

4.40 Information cannot be provided to MPs or other advocates on behalf of residents without the written authorisation of the resident.

The press

4.41 Refer all press enquiries to the Chief Executive.

5. In the office and outside work

5.1 Your work is likely to bring you into contact with sensitive information that is personal to someone or is not yet ready for distribution. Always follow a few simple rules:

- Even in the most innocent of conversations, do not discuss any part of your work that will breach confidentiality or cause either an individual or the association embarrassment or harm.
- Be aware of who else may be listening, particularly in areas open to the public.
- Remember that information in the wrong hands can cause a lot of damage and unnecessary stress.

6 Written information

6.1 Ensure that notes of interviews with residents or staff are factual, observable and objective.

6.2 Do not record unsubstantiated opinions or derogatory remarks.

6.3 All written information must be accurate and justifiable. Remember that, with very few exceptions, residents and staff have a right to see all information held about them. ***See Policy on Access to Personal Information***.

6.4 Record the source of all information provided from an external agency or individual. We should, wherever possible, be able to identify the source of all written information about a resident. Again the resident has the right to be informed of the source of information held about them.

6.5 Be careful not to leave confidential information lying around for others to see. Check and clear work areas and lock desks and filing cabinets before leaving at the end of each day. It is acceptable to leave some work out, but lock away anything confidential or of limited circulation if practical. If someone comes near you while you are working on confidential matters, discreetly cover the material or ask the person to move away.

6.6 If confidential information is sent in the internal mail, seal the envelope and mark it private and confidential.

6.7 Take care when throwing information away - if necessary consider shredding paper.

6.8 Take care when providing paper to be used for scrap - check it does not contain confidential information.

6.9 If you need to take sensitive documents away from the office, seek permission first. Do not read or process documents on public transport. Do not leave documents unattended in cars; store them safely out of view at home and do not show them to other household members.

6.10 Should the need arise, Solon has the right to call at employees' residences to retrieve any of the association's documents that may have been taken there without permission, or that have not been returned within a reasonable timescale. Failure to comply could lead to disciplinary action.

7. Discussions and meetings

7.1 When discussing a resident's situation, only disclose information relevant to the case.

7.2 Be aware when discussing cases in the office that others with no involvement in the case may be able to overhear e.g. at reception, in an open plan area or corridors. Make sure discussions happen in an appropriate place.

7.3 In sheltered schemes do not discuss personal facts about one resident with another resident or in the presence of another resident.

7.4 Do not disclose the name of a resident making an allegation about another resident without the complainant's consent.

7.5 Do not discuss personal information about a staff or Board member without their specific consent.

8. Collecting and recording personal information

8.1 Offer a private interview

8.2 If the conversation is over the telephone and someone might hear, do not repeat aloud any personal information. If necessary, ask the person to say it again.

8.3 Obtain the individual's consent by first explaining why the information is needed and how it will be used. For sensitive information, also explain:

- Who will have access to it.
- The implications of not giving the information.
- Any special procedure for protecting particularly sensitive information.

8.4 If the individual does not agree, do not record or pass on the information. Explain this and its implications to the person.

8.5 Do not ask questions that are not relevant.

8.6 Ensure that any information you record is:

- *Factual and relevant* – concentrate on facts relevant to the application or conduct of the tenancy. Keep expressions of opinion to a minimum and make sure they are fully justifiable on the basis of the factual information.
- *Accurate* – wherever possible, take notes during interviews and conversations and use the resident or applicant's own words. Check the record with the resident or applicant if possible. Where appropriate, ask for and examine supporting documents and record this on file.
- *Comprehensive and clear* – another staff member might have to form a judgement from the information and residents may wish to read it.

9. Handling incoming information

9.1. Any envelopes marked 'confidential' or 'personal' should be passed to the addressee unopened.

9.2. If anything of a confidential nature is not in an envelope, put it in a sealed and appropriately marked envelope before passing it to the addressee.

9.3. If you open confidential correspondence by mistake, reseal it or use a new envelope and write your name and 'opened in error' on the outside before forwarding it to the addressee.

9.4. If information marked 'confidential' arrives generally addressed to the association or a department, pass it unopened to the Chief Executive or the appropriate head of department/Director.

10. Correspondence, messages and calling cards

10.1. Always use a sealed envelope for anything that is of a confidential nature (e.g., lettings, rent arrears, rent statements).

10.2. When leaving a phone message or calling card, keep any details about the reason to the absolute minimum – e.g., a request to contact you or Solon.

11. Typing and administration

11.1 The administration, typing, printing, photocopying, faxing and filing of confidential information must only be carried out by employees who are familiar with confidentiality procedures and who oversee the whole operation.

11.2 Take care to destroy all unused rough work and any spare copies.

11.3 When photocopying, do not let anyone else read the documents, make only the required number of copies and check that nothing is left in the machine afterwards.

11.4 When faxing, ensure the first page clearly shows the contents are confidential, the fax is sent by a designated person, and alert the recipient in advance to collect it from the machine immediately. Any incoming confidential faxes arriving when the recipient is not present should be placed in an envelope marked 'confidential' before being passed to the recipient.

12. Working with computers (see also email and Internet Usage Policy)

12.1 Personal information held on computer must be password – protected.

12.2 Lock away computer disks and USB sticks carrying confidential information.

12.3 Use automatic screen savers if there is any possibility of someone accidentally seeing confidential information on unattended computer screens.

12.4 Log out of the system when leaving your desk unattended.

12.5 Regularly delete old and out-of-date e-mails.

12.6 Generally, please refer to and follow the requirements of the data security section of the IT Policy and procedures.

13. Keys

13.1. All keys to Solon properties must be kept in a key cabinet that is kept locked.

13.2. Keys should be coded and address lists held separately.

14 Questionnaires/forms

14.1 When designing questionnaires (whether they are intended to be anonymous or not) or other forms for completion by residents or staff, where personal information is requested, staff shall include a clause that will state:

- Why the information is required.
- Who will have access to the information.
- How the information will be stored.
- How long it will be kept.

14.2 The following standard clause may be used, but can be amended to suit particular needs:

The information recorded here will be used by Solon South West Housing Association staff to assist in providing quality services to our customers. The information may be monitored to ensure equality of access to services and may be subject to audit. It may also be shared with Solon's Board Members and/or other departments or agencies in order to process the information given and/or improve our services. The information will be stored and kept in accordance with our Confidentiality and Data Protection Policy.

15 Promotional/Educational Material

15.1 Consent must be obtained if an image of a resident or other member of the public is used in any promotional/educational material. Use Informed Consent Form for this purpose. See Appendix 2.

16 Sensitive Information

16.1 Housing staff, Tenancy Support Officers and supported housing staff may have access to more detailed and private information on residents e.g. application forms, medical and health details, benefits and income information. This information qualifies as sensitive information. Particular care must be taken in keeping the minimum amount of information necessary and respecting the resident's right to confidentiality.

16.2 Informed consent is needed to process sensitive information. Use Informed Consent Form to record this. See Appendix 2.

16.3 Do not disclose the name of a resident making an allegation about neighbour dispute or harassment without the complainant's consent.

17. Avoiding putting staff and others at risk

17.1 In some cases, Solon will be aware that particular residents may present a risk to staff. For example where there has been threatening or violent behaviour in the past. Information about potential risks should be passed on to contractors and staff if they are visiting the residents concerned.

18. Breaches of confidentiality/damage limitation

18.1 Breaches often occur as a result of thoughtlessness and lack of awareness of the potential consequences of inappropriate disclosure. However, to the resident or staff member concerned the effect is the same whether the breach is intentional or accidental. All breaches will be taken seriously and are potentially a disciplinary issue.

18.2 If a breach of confidentiality occurs, you must inform your Manager or head of department/Director.

18.3 The Manager or head of department/Director will take immediate action to prevent further breaches.

18.4 Generally help to prevent accidental disclosures occurring by regularly pointing out that certain information is confidential and checking that people have understood.

19. Disposal of information that is no longer required

19.1 All confidential information that is no longer required should be shredded, including computer printouts or rent accounts and arrears.

19.2 Former residents' files are to be retained for four years, unless continuing action is being taken to recover outstanding debts. After that, the file is to be shredded except for the resident's name and address, names of other members of the household, date of commencement and termination of the tenancy, and forwarding address.

19.3 Former staff members' files are currently retained for six years. After that, the file is to be shredded except for the basic employment information such as date of commencement and end of the employment contract.

20. Access to records held by staff

20.1 Solon has the absolute right to access records and information held by staff and to use this access to obtain any property belonging to the association including documents and office equipment, and to ensure that staff are adhering to the association's Confidentiality and Data Protection Policy. This includes accessing staff e-mails, PC hard drives and desks and monitoring e-mail and internet access.

APPENDIX 1

Collecting personal data from tenants

Wherever landlords collect personal data from tenants for the first time it is important to pay careful attention to the following questions:

- Are you clear about exactly what items of personal data and sensitive personal data are needed (either now or in the future)?
- Are you clear about exactly why you need these items of information? You must have a 'real' reason for collecting information and for its further use and these should be defined at the outset.
- Are you likely to want to use the data again for something else? If you know it is highly likely that specific items of tenants' personal data will be needed later on for a slightly different reason, then include it and explain clearly why it is needed
- Are you clear about the legal grounds for the collection and further use of the tenants' data?
- Where the ground of 'consent' is to be used, have you provided clear details to enable tenants to give informed consent?
- Have you provided all the required fair processing information in a suitable privacy statement within the form where the information is collected? Does it clearly explain why information is being collected, how it will be further used and with whom it might be shared?

The tenancy application form

In this form, tenants typically provide a very wide range of personal data. Some of it will be personal data in the form of name and contact details. Other information may fall into the category of sensitive personal data e.g. information relating to health or disabilities, ethnicity and religion.

It is likely that where non-sensitive personal data is collected and is essential to the granting of the tenancy (such that if it wasn't provided, the tenancy could not be granted), then the collection of this kind of information could be legitimised on the basis of the 'contractual necessity' ground (i.e. tenant consent not needed – and not appropriate as any consent for this type of processing would not be 'true' consent).

With regard to sensitive personal data collected from tenants, landlords collect this kind of information for a variety of legitimate reasons including, for example, the need to ensure that they provide accommodation which is suitable for tenants' needs or to demonstrate compliance with statutory obligations. Where such sensitive personal data is collected in order to comply with a statutory duty, or a legal obligation, the DPA provides a legitimising ground for the collection and processing of this kind of personal data in this context.

Where a landlord needs to collect sensitive personal data from a tenant at the application stage and this information is not needed in order to comply with a statutory duty or legal requirement, the other legal grounds for processing which are available under the DPA will need to be examined.

If, after considering the grounds which are available, the most applicable one is that based upon the tenant's explicit consent, then that consent should clearly be sought

from the tenant. This could be achieved by providing the appropriate 'privacy statement/consent' section in the tenancy application form to explain to the tenant why that particular information is needed from them and how it will be used and providing a space for signature by the tenant for the tenant to indicate their explicit consent to this processing.

Landlords also need to consider carefully whether this information does in fact need to be collected from the tenant at all if the only ground upon which the processing can be legitimised is the 'explicit consent' ground.

However, it is necessary to point out that even where tenant consent is not actually needed in relation to the collection and further processing of any particular item of sensitive or non-sensitive personal data, it is very important that landlords ensure that they provide the fair processing information which would be given either in a privacy notice or statement with the tenancy application form when the information is first collected from the tenant i.e. it is explained clearly to the tenant why the information is needed and how it will be used.

Re-use of tenants' personal data at a later stage for a purpose other than the granting of the tenancy

It is sensible to design the tenancy application form, or any forms on which personal data is initially collected, very carefully with appropriate thought given to whether any of the personal data collected may be needed for other purposes, for example for research, direct marketing, or in the implementation of new products and services for tenants.

Ideally, these additional purposes should be specified clearly in the initial collection form (in the privacy statement section) and specific/explicit consents sought where needed at this point. Where, however, this has not been done and the new purpose is not covered in the initial privacy statement or notice, then this exercise will have to be carried out at the later stage. This will mean notifying tenants of the new purpose(s) and where appropriate to do so, obtaining their consent for example by sending out a new privacy notice/ consent form.

If the type of processing contemplated is to be done with the explicit consent of the tenant (this is going to be much more likely where the data required to be used is sensitive personal data) then the privacy notice to be sent to tenants should include a means of collecting consent e.g. the tenant's signature.

If this ground is used, it is important that the consent provided is 'true consent' and that tenants have the facility to withdraw consent for this processing at a later stage, if required.

Data landlords can legitimately request from tenants

The following are examples of personal data that can be held by landlords

- age
- title
- full name
- other name(s) may be known by
- marital status
- current and previous addresses

- alternative contact address
- landline/mobile phone contact details
- email address
- national insurance number
- nationality
- immigration / residential status
- ethnicity
- religious belief
- gender identification
- sexual orientation
- disability details – nature of disability, disabled access requirements
- aids and adaptations requirements
- medical information – physical and mental health
- vulnerabilities – e.g. sight, hearing impairments, drug/alcohol dependency issues
- employment status
- housing history
- household type
- economic status
- income details – wages and/or benefits
- financial commitments (expenditure and debts)
- bank details
- allowances, benefits and grants
- details of support being received or required from external agencies (name of support worker, name of external agency)
- unspent criminal convictions
- third-party authority and information (name, address, date of birth, contact details, nature of relationship to tenant.

Landlords can also collect personal data in the form of certain opinions and intentions, such as:

- staff case notes on tenants, including support worker diaries
- staff opinions on tenants in neighbour nuisance cases and their intentions on how to deal with tenants in such cases.

In addition, landlords might hold social service department case notes or information supplied by the DWP in relation to universal credit entitlement.

Summary of personal data that may be collected by landlords directly from third parties:

A landlord may obtain information about the tenant(s) from a third party, which may include information from social services, mental health agencies, benefit services such as the local council's housing benefit service, the job centre or DWP, money advice agencies, GP, hospital, support worker and/or external support services.

Information obtained may include:

- details of medical conditions, both physical and psychiatric
- details of medication and/or treatment
- hospital number
- name
- address

- national insurance number
- DWP reference number (universal credit)
- housing benefit claim number
- income details of tenant and family members (this information can be included on housing benefit entitlement notification letters or benefit letters)
- benefit entitlement information – this may include confirmation of the amount of benefit entitlement, the periods the benefit relates to, any backdated payment of benefits and periods it relates to.
- details of child protection, care or residency arrangements
- details of tenant(s)/household members' vulnerabilities

Types of forms used by landlords:

- housing application form
- pre-tenancy assessment form
- housing interview form
- sign-up form
- equality and diversity monitoring form
- income and expenditure / financial assessment form.

Types of documents obtained by landlords:

- proof of benefit letter (job seekers' allowance, employment support allowance, disability living allowance now in some instances referred to as personal independent payments).
- proof of income (wage slips, P60, child tax credit notifications)
- bank statement – for ID purposes, proof of bank account/means of receiving income or for money advice purposes
- council tax notifications – ID, money advice purposes or income and expenditure to consider rent arrears payment arrangement
- ID and proof of residence documents for tenant and family members (passport, driving licence, visa, immigration documents)
- housing benefit entitlement notification letters
- letters from DWP notifying of universal credit application or entitlement
- letters from money advice agencies
- medical letters (GP or hospital)
- expert medical report
- letters from social services or CPN
- direct debit form

Other information:

This is information a landlord may obtain from the tenant(s) about a spouse, partner, children, and/or relative(s) that will be residing with the tenant at the property or may come to reside with the tenant at some stage during the tenancy:

- title
- full name
- date of birth / age
- relationship to the tenant
- medical difficulties
- disability details
- vulnerabilities
- income details (employment income and/ or benefit income) – this may be obtained

for the purposes of completing housing benefit entitlement calculations and/or proof to be sent to the benefit services to process a housing benefit claim.

- bank statement – for the purposes of proof of income for housing benefit claim or Calculation.

APPENDIX 2

Solon South West Housing Association Ltd
Consent Form

Tenants Name(s)	
Address	
What information do we need your consent to hold?	
Why are we holding/ collecting this information?	
I consent to the personal information described above being held by Solon South West Housing Association Ltd.	**YES** ☐ **NO** ☐
If No – Please Specify what Information you do not want to us to hold.	

Please **sign** your name here to confirm your answers on this form.

Signed (Tenant)	
Date	

If you cannot sign here for any reason or have any questions, please ring or email to say yes or no to us holding your information on: **0117 916 7795** or: **james_naish@solonswha.co.uk**

APPENDIX 3

SOLON SW HOUSING ASSOCIATION
Privacy Notice – Short Form

What non-sensitive personal information may we hold on you? (See page 2 if you're unsure what this means)	We **normally** hold information such as your: Name(s), Address, Age(s), Contact details, Next of kin and their contact details, I.D, Sex, National insurance number, Employment details, Address history, Details of any support services, financial details, Photograph of you, Bank details and any complaints against you.
What Sensitive Personal Information may we hold on you?	We **normally** hold your: Ethnicities, sexual orientation, Health Details and your religion. We may **rarely** hold information on criminal offences and details of harassment or abuse (if we need it in order to support or protect you)
Who Holds Your Information?	**Solon** South West Housing Association Ltd
Why are we processing your Information?	To fulfil your **tenancy agreement**, to assess your housing need and provide you with a service, to fulfil our **legal obligations** to you.
Where did we get your data?	Directly from you, **the tenant**. Occasionally we may get some of your data from **3rd parties** such as the police or your former housing association.
Others who may have seen your personal information and why? (See Privacy Notice on website for full details of who may have seen your data)	Some of your personal information may have been shared with **contractors**, or **agencies** we work with, such as local authorities, social services, police, other social landlords and others when we think it is in your interests to do so.
How will your data be kept securely?	Your data is treated with the utmost confidentiality and security, as detailed in our data protection policy.
How long will your information be kept?	Normally, up to **6 Years** after Tenancy Ceases

It is PARAMOUNT that you tell us if any of the personal information changes so that we can keep this up to date or discuss it with you, it may affect your tenancy if you withhold any changes from us.

Your Rights and How You can Use Them

Right to Be Informed: We must provide you with a privacy notice to tell you how we are using your personal data, why we are using it and how long we are likely to use it for.
Right of access: You can ask us for access to any of the information we hold on you by contacting our Corporate Services team. Information will be given to you within one month of your request being received (or up to 2 if it's a complex request).
Right to rectification: You can change your personal data if it is inaccurate or incomplete. Please contact us if any of your personal information changes.
Right to erasure: You can ask us to delete or remove your personal data where there is no reason for us to keep it. Contact our corporate services team to request this.
Right to restrict data processing: Under certain circumstances, you can 'block' us from using your some of your personal data. We are then allowed to only store your personal data.
Right to data portability: You can ask us for your personal data if you wish to use it for another service. We will usually give you all the personal information that you have provided us (some conditions apply – see website for details)
Right to object: You can object to direct marketing – see website privacy notice for further details of what you can object to.
Right to Complain: You have the right to complain to a supervisory body (ICO) if you feel we have failed to meet our duties to you in any way in relation to your personal data.

Sensitive and Non-sensitive Personal Data: Information we hold on you is split into two categories; sensitive and non-sensitive.

Sensitive data is anything that relates to Race or Ethnicity, Political Opinions, Religious Beliefs, Physical/Mental Health and Sexual Life.

Non-Sensitive data is anything else we hold on you, including your Name, Date of Birth, Phone number and National Insurance Number. Criminal Offenses and Bank Details (and similar info) are not classified as sensitive data however they are treated with the same amount of security and confidentiality.

Contacting Us: Please contact our Corporate Services Team to make any requests in relation to your rights, or if you have any other queries about the Data Protection Act or Solon's Data Protection Policy please contact our data protection assistant using the following:

E-mail: solon@solonswha.co.uk

Phone: 0117 924 4071

For more detail on your rights and a more comprehensive privacy notice, please visit our website: www.solonswha.co.uk/SpecialPages/Privacy-Notice.aspx

Solon South West Housing Association: Privacy Notice for residents

Your contact with Solon generates records including personal information, some of which may be sensitive and all of which is subject to the Data Protection Act 2017. We respect residents' privacy. This privacy notice sets out Solon's approach to data protection and privacy as your data controller.

How we collect personal information

Solon collects information in a variety of ways including application forms and questionnaires, telephone conversations, the website, contracts, through ongoing contact and correspondence with you and with other support agencies which relate to you, occasionally from the police or other authorities and also from people associated with you such as family, friends and neighbours. We may also have CCTV cameras in public areas in some properties to record events in order to prevent anti-social behaviour.

It is paramount that you tell us if any of the personal information you have given to us changes so that we can keep this up to date or discuss it with you as it may affect your tenancy if you withhold any changes from us.

If you provide us with personal information relating to members of your family or your associates we will assume that you do so with their knowledge and consent.

Sensitive and Non-sensitive Personal Data: Information we hold on you is split into two categories; sensitive (or special categories of personal data) and non-sensitive. Sensitive data is anything that relates to Race or Ethnicity, Political Opinions, Religious Beliefs, Trade Union Membership, Physical/Mental Health, Sexual Life. Non-Sensitive information is anything else we hold on you, including (but not limited to) Name, Date of Birth, Phone number, E-mail Address and National Insurance Number. Bank Details (and similar info) are not classified as sensitive data however they are treated with the same amount of security and confidentiality as all other sensitive information. The Commission or Allegation of an Offense and the proceedings or sentencing of the offense are also not classed as sensitive personal data but are subject to even tighter controls.

What information we may collect, hold and use

- Your name and contact details for use across the organisation and by our suppliers and partners.
- Detailed personal information such as photo identification, age, sex, date of birth, ethnicity, income, National Insurance number, private expenditure data, employment status, contact details (telephone numbers and email addresses), relationship status, address history, any disabilities, religion, sexual orientation, nationality, caring responsibilities, details of your next of kin (address and contact details) access to financial services such as banks and credit unions, bank details, benefits, council tax, affordability information, eligibility for UK residency, details of those who you want us to communicate with on your behalf, how you prefer us to contact you, whether you have any literacy problems, your ability to speak English and language preferences, requirements for different communication formats, your

preferences for getting involved and the service areas that are of most interest to you.

- Simple Details on other occupants of your home such as their name, date of birth, sex, ethnicities, any health issues we may need to know about and their religion.
- Tenancy reference checks/references from other housing providers/private landlords.
- Your particular needs or preferences so that we can understand them better and offer care or support based on these needs.
- Details of Support Services may use.
- References/information from your mortgage lender (if you own/have owned your own home), When you apply to us for housing, we request information so we can understand your housing needs and assess your application. This may include references from other landlords, your mortgage lender (if you own/have owned your own home), the police and probation services, support workers, social workers, mental health workers and credit reference agencies.
- Medical and health information so that we can prioritise and assess a housing application. Your support needs so we know how we can support and assist you before and during your tenancy.
- Details of any harassment of abuse in order to support or protect you.
- Details of any complaints made against you or any anti-social behaviour.
- Details relating to the repair and maintenance of your home.
- Information that you provide to your relevant housing, maintenance or other dedicated team, including all emails and other forms of communication.
- Feedback from our contractors about their appointments with you.
- Information about allegations of anti-social behaviour.
- Voice and image (CCTV) recordings for safety, crime prevention and quality management which is used in accordance with our CCTV policies and procedures.
- We may collect information about individuals where they pose a substantial threat to our staff or contractor, such as criminal records or alleged offences.
- We may take pictures at residents' parties, meetings and other events, and these may be used in newsletters, annual reports, brochures or on the website or Facebook and they may appear in local newspapers. Whenever we take pictures we will always ask you for your written permission and give you the choice whether or not to be included in a photograph.
- We may also record calls to our customer service staff and some other departments, this is to help us identify how to provide you with a better service. These calls will be kept securely for 12 months then destroyed, unless they are part of a dispute – in which case we reserve the right to keep them for dispute resolution purposes.

How Long Do we hold your data for

In most cases we hold the majority of your tenancy data for up to 6 years after your tenancy ceases. However some data we may get rid of during your tenancy if we no longer have a purpose for keeping it. For full details on how long we keep your personal data you can contact us and ask to see our full retention policy.

Who the personal information relates to

We collect and hold personal information about:

Residents - This includes current, former and potential residents who live in our properties or access our support and other services, together with members of their families and people associated with them.

Visitors - Visitors to our offices

Anyone - who makes an enquiry to Solon.

Anyone - who makes a complaint to Solon.

How we use our records

We keep records to enable us to:

- Assess applications for housing and then allocate housing and provide tenancies.
- Manage housing and tenancies including collecting the rent and any service charges.
- Provide a repairs and maintenance service.
- Offer support, advice and help with debts and benefits.
- Provide support services where needed by residents including vulnerable residents.
- Keep in contact with residents, invite you to events etc.
- Prevent and detect crime and resolve disputes.
- Prevent and detect fraud and money laundering.
- Promote safety and the quiet enjoyment of houses and estates.
- Tackling Anti-social behaviour.
- Discuss services with residents to identify improvements.
- Provide information about services requested by you.
- Promote equal opportunities and fair treatment for all residents.
- Develop new products and services to meet the future needs of our communities.

- Meet our legal obligations to our regulators and funders.

- To fulfil our obligations to you as laid out in your tenancy agreement

The Data Protection Act requires us to minimise our holding and use of sensitive categories of personal information. This means that we will only collect and use it when it is necessary to provide special services, or to deal with special circumstances. Examples include when we receive applications from people with disabilities or with problems such as substance abuse, when there are anti-social behaviour issues involving actual or alleged criminal activity or when residents need access to care services.

Direct marketing

We may occasionally wish to provide you with information about events, services and other information which may be useful to you. We will send this by post, email or contact you by telephone. You can let us know at any time how you prefer to be contacted or if you do not want us to contact you with this information.

We will never provide any of your personal information to other companies for their marketing purposes.

Protecting and sharing information

Your personal information will be kept secure and confidential as per our data protection policy. Our staff only have access to your personal information when and if they need to have it to provide the service to you. We may share information with contractors, or agencies we work with, such as local authorities, social services, police, other social landlords and others when we think it is in your interest or in the public's interest to do so. We will also disclose information as required by law.

In particular, please be aware that:

- Current or forwarding addresses may be shared with utility companies and Council Tax offices to ensure billing details are correct.

- If you default on any tenancy or licence conditions, information about you may be provided to authorised debt recovery agencies, to enable them to recover the debt. This may affect future applications for tenancies, credit and insurance.

- We may discuss your financial situation, rent payments (including any arrears) and any claims made for welfare benefits with an external debt advice agency, welfare rights advisor, a council's housing benefit department or housing advice and homeless prevention team to ensure that benefits are paid correctly.

- We may pass data about your rent payment record to credit reference agencies. This will enable them to assist other organisations to assess your financial standing if you apply for products and services.

- We may pass your information to support services if we feel it is in your interests to do so or you ask us to do so.

- We may pass your contact information to a third party to conduct surveys and research on our behalf which allow us to gather feedback and improve the services we offer you. The third party will always be bound to strict terms and conditions outlined by us and will not share your data with other organisations. Should you choose not to participate in the surveys the third party will securely destroy your data.

- We may share your National Insurance number to verify your Universal Credit application and manage these payments.

- We may also share your National Insurance number in order to prevent and investigate tenancy and right to buy applications fraud.

National Fraud initiative

Solon may occasionally participate in the National Fraud initiative (NFI) data matching exercise carried out by the Government. Our participation in NFI assists in the prevention and detection of fraud against Solon and other public sector organisations.

Data matching involves comparing computer records held by one organisation with records held by another to see how far they match. This is usually personal information. Data matching allows fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

The use of data in this way is carried out with statutory authority and therefore does not require the consent of the individuals concerned under the Data Protection Act 2017.

Your rights under the Data Protection Act / GDPR

Right to Be Informed: We must provide you with a privacy notice to tell you how we are using your personal data.

Right of access: You have the right to obtain access to your own personal data at any time so you are aware of and can verify the lawfulness of processing. Information will be supplied within one month of receipt of the request. This can be extended by a further two months where requests are complex or numerous. This will be provided free of charge unless you ask for multiple copies or the request is manifestly unfounded or excessive. We can also refuse your request if it adversely affect the rights and freedoms of others or is manifestly unfounded or excessive. You can make a subject access request by contacting anyone at Solon, preferably someone on our corporate services team.

Right of rectification: You have the right to have your personal data rectified if it is inaccurate or incomplete. If we have disclosed this to third parties, we will tell you if this is appropriate and we will inform them of the rectification where possible.

We must respond within one month, extendable by two months where the request for rectification is complex.

Right of erasure: You have the right to request the deletion of personal data where there is no compelling reason for its continued processing or if we are processing it in an unlawful manner – for example if we are using it for a different purpose than originally stated.

Right to restrict data processing: Under certain circumstances, you have a right to 'block' or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data, but not further process it. We can retain just enough information about you to ensure that the restriction is respected in future.

Right to data portability: You can obtain and reuse your personal data for your own purposes across different services. This right applies where the processing is based on your consent or for the performance of a contract; and when processing is carried out by automated means.

Right to object: You have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

If we process personal data for the performance of a legal task or our organisation's legitimate interests, you must have an objection on "grounds relating to you particular situation".

We must stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defense of legal claims.
- The Personal Data is essential to the continuation of the tenancy or is in the 'vital interests' of the tenant.

Right to Complain: You have the right to complain to a supervisory body (ICO) if you feel we have failed to meet our duties or obligations to you under the DPA in relation to your personal data.

You Maintain the Right to Withdraw Consent at any Time: You may contact Solon to request this, conditions apply.

Contacting Us

Please contact our Corporate Services Team to make any requests in relation to your data rights, or if you have any other queries about the Data Protection Act or Solon's Data Protection Policy:

E-mail: solon@solonswha.co.uk.

Phone: 0117 924 4071