Data Protection Policy and Procedure

If you need any information in a different format, for example large print, Braille, audio file or another language, please email Communications@housing21.org.uk

Version number	7.0
Issue date	October 2025
Review date	October 2028
Board approval required?	Yes
If yes, date approved by Board	September 2025 (Audit and Assurance Committee) October 2025 (Board)
Author's name and job title	Sonia Hawley, Information Governance Manger and Data Protection Officer (DPO)
Policy owner and job title	Annabel Ellin, Director of Audit Assurance and Governance
Policy Steering Group approval date	October 2025

Summary

The Data Protection Act 2018 (DPA18) governs data protection in the UK and incorporates the relevant provisions set out in the UK General Data Protection Regulation (UKGDPR). The DPA18 provides individuals with the right to know what personal information is held about them and how it is processed and protected. It also sets out requirements for organisations to adhere to when collecting and processing personal data and includes additional provisions for processing special category 'sensitive' personal data.

This Data Protection Policy sets out how Housing 21 protects the personal data it collects and processes as an organisation in compliance with the GDPR and DPA18.

This policy aims to set out clear guidance on:

- Employee obligations in the protection of personal data and breach reporting
- Data Controller obligations in the protection of personal data

- Individuals' rights in relation to their personal data

Compliance with this policy is mandatory for all employees. Related policies, privacy guidelines, glossary and terms are available to help you. Any breach of this policy and the related mandatory information governance eLearning training provided to all employees, may result in disciplinary action.

Personal data breaches can result in harm to residents and employees as well as possible action form the data protection regulator, the Information Commissioners' Office (ICO), who can impose significant fines to business and individuals for failing to process personal data securely and in line with the law. This can result in reputational damage for both Housing 21 and employees.

This policy applies to all Housing 21 Board Members, Executive Directors, Senior Management Team, and employees whether permanent, part-time, fixed term, casual employees, and volunteers of Housing 21. The policy also applies to any temporary employees, consultants, or contractors, including suppliers or 3rd party agents working on Housing 21's behalf. All of whom are expected to always act with honesty and integrity in safeguarding the resources for which it is responsible.

The policy includes clear guidance on roles and responsibilities and highlights how to comply with the legislation and regulation and who to liaise with when processing an information rights request and/or reporting an actual or suspected data breach. Further information on reporting data breaches and managing information rights requests are documented within the Information Rights Procedure and Form and the Information Governance and Security Policy and Procedure.

The Director of Audit, Assurance and Governance is responsible for ensuring that this policy and associated policies and procedures are adhered to. The Senior Information Risk Officer (SIRO) takes overall responsibility for Housing 21's risk approach.

Equality, Diversity, and Inclusion

Housing 21 aspires to embed diversity and inclusion within all our organisational activities to enable these principles to become part of our everyday processes.

Policy Contents

1.0 Data Protection

1.1 Data Protection applies to all personal data, processed and/or stored electronically[1] and manually (paper based) files.[2] It aims to protect and promote the rights of individuals, ('Data Subjects') and Housing 21 (the 'Data Controller').

1.2 '**Personal Data**' is any information which relates to a living individual who can be or may be identified from that information, (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access: for example: (this list is not exhaustive)

- An individual's name, address (postal and email) or date of birth
- A statement of fact and/or any expression/opinion communicated about an individual's actions or behaviour
- Minutes of meetings and reports which refer to an individual
- Emails, file notes, handwritten notes, sticky notes in relation to an individual
- Individual identifiable CCTV footage
- Lettings, sales, and employment application forms
- Care support plans and housing files
- Spreadsheets and/or databases with any list of individuals set up by code, tenancy number, NI number etc.

1.3 Personal data may **only** be processed provided:

- The individual has given their explicit consent to the processing

[1] This list is not exhaustive: Desktop PC's, Laptops, Tablets, and Mobile Phones.
[2] Manual records are paper based and structured, accessible (filed by subject, reference dividers or content), where individuals can be identified, and personal data easily accessed.

- It is necessary for the performance of a contract with the individual
- It is required under a legal obligation
- It is necessary to protect the vital interests of the individual
- It is to carry out public functions
- It is necessary to pursue the legitimate interests of Housing 21 or certain third parties (unless this is prejudicial to the interests of the individual)

1.4 '**Special Category Data**' is any information relating to an individual's:

- Race or ethnicity
- Sexual orientation
- Sex life
- Religious or philosophical beliefs
- Membership of a Trade Union
- Health, physical or mental health conditions
- Biometric data
- Genetic data
- Political opinions

1.5 Special category data may *only* be processed provided:

- The individual has given their explicit consent (i.e., signature)
- The individual has already made this information public
- It is to protect the vital interests of the individuals or other individuals
- It is necessary for the purposes of, or in connection with legal proceedings or for obtaining legal advice and for the administration of justice or any enactment, function of the Crown
- It is for medical purposes and is undertaken by a health professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to a health professional
- It is necessary for the purposes of exercising or performing any right or obligation as Data Controller in connection with employment

1.6 A '**Data Subject**' is an identified or identifiable **living** individual who is the subject of personal data. The provisions set out in the DPA18 and GDPR do not apply to the records of the deceased.

1.7 Requests for personal data on deceased individuals may be covered by the Access to Health Records Act 1990. **Employees always consult with the Data Protection Officer (DPO),** as these cases are managed on a case-by-case basis.

1.8.1 If Housing 21 is processing personal data relating to criminal convictions and offences it shall implement suitable measures including a policy document that satisfies the requirements of the Data Protection Act 2018 Schedule 1 Parts 3 and 4.

2.0 Data Protection Principles

There are six (plus one) principles under the GDPR and DPA18 which Housing 21 employees must ensure they abide by when processing personal data:

2.1 **Principle 1** Personal Data shall be obtained and processed fairly, lawfully, and transparently. (Lawfulness, Fairness and Transparency)

2.2 **Principle 2** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. (Purpose Limitation)

2.3 **Principle 3** Personal Data shall be adequate, relevant, and limited to only what is necessary for the purpose for which it is obtained. (Data Minimisation)

2.4 **Principle 4** Personal Data shall be accurate and, where necessary, kept up to date. (Accuracy)

2.5 **Principle 5** Personal Data shall not be kept in a form which permits identification of Data Subjects for longer than necessary for the purposes for which the data is processed. (Storage Limitation)

2.6 **Principle 6** Personal Data (manual and electronic) must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage. (Security, Integrity, and Confidentiality)

2.7 Accountability We are responsible for and must be able to demonstrate compliance with the data protection principles listed above. (Accountability)

2.7.1 Housing 21 must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

2.7.2 Housing 21 has implemented adequate resources and controls to ensure compliance including:

- Appointing a suitably qualified DPO and an executive accountable for data privacy.
- Implementing Data Protection by Design and Default when processing personal data and completing DPIAs where processing presents a high risk to rights and freedoms of Data Subjects.

- Integrating data protection into internal documents including this Policy, related policies, privacy guidelines, Privacy Notices or Fair Processing Notices.
- Regularly training employees on data protection and data protection matters including, for example, Data Subject's rights, consent, legal basis, DPIA and personal data breaches.
- Maintaining a record of training attendance by employees.
- Regularly testing the privacy measures implemented; and
- Conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

2.7.3 All employees must follow these Principles and maintain data security by protecting the confidentiality, integrity, and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users can access the personal data when they need it for authorised purposes.

2.8 Where the lawful grounds are legitimate interests a legitimate interests assessment (LIA) will be undertaken and documented. Where the lawful grounds are a task carried out in the public interest or in the exercise of official authority vested in the organisation, a public interests assessment (PIA) will be undertaken and documented. Where the lawful grounds are a legal obligation, the relevant legislation shall be cited and appropriately documented.

2.8.1 Where the lawful basis is consent or explicit consent the organisation shall ensure the consent is valid and that the data subject is able to withdraw their consent should they choose to.

2.8.2 Consent shall not be valid unless:

- there is a genuine choice of whether or not to consent;
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of personal data relating to them;
- the consent was given through statement made by the data subject or by a clear affirmative action undertaken by them;
- the organisation can demonstrate that the data subject has been fully informed about the data processing to which they have consented and is able to prove that it has obtained valid consent lawfully; and
- a mechanism is provided to data subjects to enable them to withdraw consent and which makes the withdrawal of consent in effect as easy as it was to give and that the data subject

has been informed about how to exercise their right to withdraw consent.

2.8.3 The organisation recognises that consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject. The organisation recognises that consent cannot be considered to be forever and will determine a consent refresh period for every instance where consent is the lawful condition for processing.

2.8.4 Where consent is the lawful basis for processing, the Data Protection Officer shall ensure that consent is properly obtained in accordance with the conditions above.

Transparency - The organisation shall ensure that transparency is engrained the processing undertaken. Before any processing of personal data begins, the privacy information provided to data subjects will be considered and will be updated where necessary to ensure it accurately reflects the processing being undertaken.

Purpose Limitation – The organisation shall ensure personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data Minimisation – The organisation shall ensure personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The organisation will strive to use a minimum of personal data in its data processing activities and will periodically review the relevance of the information that is collects.

Accuracy - The organisation will use its reasonable endeavours to maintain data as accurate and up-to-date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date.

Storage Limitation - The organisation will ensure that it does not retain personal data for any longer than is necessary for the purposes for which they were collected and will apply appropriate measures at the end of data's useful life such as erasure or anonymization.

Security - The organisation will ensure that any personal data that it processes or commissions the processing of is 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 or organisational measures.

In particular, an information security management policy (ISMP) will be maintained setting out specific policies in relation to ensuring the confidentiality, availability and integrity of personal data.

The management will implement sufficient controls to ensure that it is able to demonstrate compliance with the Data Protection Legislation including the keeping of sufficient records of data processing activities, risk assessments and relevant decisions relating to data processing activities.

3.0 Employee Obligations

3.1 Employees will not gain access to information that is not necessary to hold, know or process. All information which is held will be relevant and accurate for the purpose for which it is required. The information will not be kept for longer than necessary and will always be kept secure.

3.2 Employees will ensure that all personal or special category personal information is anonymised or pseudonymised, where appropriate e.g., for equality and diversity reporting.

3.3 Employees who manage and process personal or special category personal information will ensure that it is kept secure and where necessary, confidential.

3.4 Employees are responsible for notifying their line manager or the Data Protection Officer, if they believe or suspect that a conflict with this policy has occurred or may occur. This includes notification of any actual or suspected data breach.

3.5 Where employees do not comply with this policy, Housing 21 may also consider acting in accordance with our disciplinary processes. Where it is found that an employee has knowingly (with intent), or recklessly breached our data protection and security policies, guidance and/or the legislation, Housing 21 and the ICO will also consider taking direct legal action against the employee. This will be the case regardless of whether a data breach has been found to have caused actual or potential distress to our residents or employees.

4.0 Data Controller (Housing 21) Obligations

4.1 Housing 21 will follow the Code of Practice issued by the ICO when developing policies and procedures in relation to data protection compliance.

4.2 When contracting out services and processing to third parties ('data processors[3]') Housing 21 will ensure that Data Processing and/or Data Sharing Agreements, where Housing 21 is the Data Controller, clearly outlines the roles and responsibilities of both the Data Controller and the Data Processor.

4.3 Housing 21 will adhere to and follow the seven Principles of the GDPR and DPA18 and the Privacy and Electronic Communications Regulations (PECR) when conducting surveys, marketing activities etc. and where the organisation collects, processes, stores, and records personal data.

4.4 Housing 21 will not transfer or share personal information with countries outside of the UK unless that country has a recognised adequate level of protection in place in line with the

[3] 'Data Processor' in relation to personal data, means any person (other than an employee of the Data Controller) who processes data on behalf of the Data Controller.

recommendations outlined in the legislation. Please refer to the International Transfer Policy for further details.

4.5 Housing 21 will conduct Data Protection Impact Assessments (DPIAs) where processing personal data may result in a high risk to data subjects or where we are processing information that relates to many individuals

4.6 Housing 21 will ensure all employees are provided with data protection training and promote awareness of the organisation's data protection and information security policies, procedures, and processes.

5.0 Individuals ('Data Subjects') Rights

5.1 Housing 21 acknowledges individuals (data subjects) rights when it comes to how we handle their data. This includes rights to:

- withdraw consent to processing at any time.
- receive certain information about the data controller's processing activities.
- request access to their personal data that we hold.
- prevent our use of their personal data for direct marketing purposes.
- ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data.
- restrict processing in specific circumstances.
- challenge processing which has been justified based on our legitimate interests or in the public interest.
- object to decisions based solely on Automated Processing.
- prevent processing that is likely to cause damage or distress to the data subject or anyone else.
- be notified of a personal data breach which is likely to result in high risk to rights and freedoms.
- make a complaint to the supervisory authority (ICO); and
- in limited circumstances, receive or ask for personal data to be transferred to a third party in a structured, commonly used, and machine-readable format.

5.2 You must verify the identity of an individual requesting data under any of the rights listed above **(Do not allow third parties to persuade you into disclosing personal data without proper authorisation).**

5.3 Housing 21 recognises that individuals have the right to make a request in writing to obtain a copy of their personal information, if held on our systems and files. These rights are known as 'information rights'. A formal procedure needs to be followed in relation to this matter, therefore please refer to Housing 21's **Data Subject Access Request Procedure,** for more

detailed guidance. Where an individual requests access to personal data held by Housing 21, always contact the organisation's Data Protection Officer (DPO), dataprotection@housing21.org.uk. The information rights form and procedure can also be made available in an accessible format, for example large print, Braille, audio file or another language, please email Communications@housing21.org.uk.

5.4 Housing 21 recognises that individuals have the right to prevent data processing where it is causing them damage or distress, or to opt out of automated decision making and to stop direct marketing at any time, under the DPA18 and the Privacy and Electronic Communications Regulation (PECR).

5.5 Housing 21 will only share information in accordance with the provisions set out in the DPA18 and where applicable, Housing 21 will inform individuals of the identity of third parties to whom we may share, disclose, or be required to pass on information to, whilst accounting for any exemptions which may apply under the legislation. We will not share third-party data in SARs unless provided with consent.

5.6 Each corporate department, Extra Care and Retirement Living scheme is responsible for the personal data which it collects and processes. This responsibility extends to personal data that is processed by any third parties on behalf of Housing 21.

5.7 Housing 21 recognises and understands the consequences of failure to comply with the requirements of the DPA18 may result in:

- Criminal and/or civil action
- Fines and damages
- Personal (e.g., employee) accountability and liability
- Suspension/withdrawal of the right to process personal data by the ICO
- Loss of confidence in the integrity of Housing 21's systems and processes
- Irreparable damage to Housing 21's reputation

5.8 Alongside this, Housing 21 recognises the right to complain internally, introduced by the DUAA 2025. If you have any complaints about the way your data is being handled/request, you are requested to complain to the data protection officer, who can be contacted at: dataprotection@housing21.org.uk.

6.0 Record Keeping

6.1 Housing 21 must keep and maintain accurate corporate records reflecting our processing including records of data subjects' consents and procedures for obtaining consents. These records should include, at the very least, the name and contact details of the Data Controller, the Information Asset Owner and the DPO. It should also include, clear descriptions of the personal data types, data subject types, processing activities, processing

purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

6.2 Each Corporate and Operational business area has an Information Asset Register (IAR) which accurately details this information. Please contact your Data Protection Champion (DPC) or Data Protection Officer (DPO) at dataprotection@housing21.org.uk.

7.0 Training and Auditing

7.1 Housing 21 are required to ensure all employees have undergone mandatory data privacy related training to enable them to comply with data privacy laws. This training is available in employees' learning pathways on our internal learning and development platform.

7.2 All employees must regularly review all the systems and processes within their remit to ensure they comply with this Policy and check that adequate information governance controls and resources are in place to ensure proper use and protection of personal data.

7.3 To further support the understanding of data protection and data security compliance, the following processes are in place:

- Coverage of data protection principles and a summary overview of the information governance framework as part of the corporate induction process for all new starters, which also includes focus on cyber security
- Supporting guidance on Housing 21s intranet covering all elements of data protection and overall information governance legislation, how to implement in day-to-day roles and best practice examples
- Regular workshops (at least every quarter) with business areas where there is high data processing or recent risks of data breaches
- Quarterly liaison with Heads of Service to identify gaps and support their information governance security profiles.
- Regular communications on the intranet, using recent data breach case studies and general good practice tips.
- We also regularly conduct assurance audits to ensure our information governance framework and associated polices and training remain compliant and fit for purpose.
- The newly formed Data Protection Champions (DPCs) will also support to deliver further information governance and awareness within their teams.
- The SIRO takes overall responsibility for the organisations data risk approach with support from the Information Governance Steering Group (IGSG) and the DPO.

8.0 Data Protection Impact Assessments (DPIAs) (Data Protection by Design and Default)

8.1 Housing 21 are required to implement Data Protection by Design and Default measures when processing personal data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with the data protection principles.

8.2 You must assess what Data Protection by Design and Default measures can be implemented on all programs/systems/processes that process personal data. This can be achieved on most projects by conducting a DPIA which helps you to consider, the nature, scope, context, and purposes of processing; and the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

8.3 The level of support/input from the DPO, when implementing major system or business change programs involving the processing of personal data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- large scale processing of sensitive data; and large scale, systematic monitoring of a publicly accessible area.
- a description of the processing, its purposes and the data controller's legitimate interests if appropriate.
- an assessment of the necessity and proportionality of the processing in relation to its purpose.
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

9.0 Artificial Intelligence (AI)

9.1 Artificial Intelligence (AI) has brought about transformative changes offering efficiency, automation, and improved decision-making capabilities. However, like any technology AI is not immune to risks. Employees are required to complete a DPIA and/or consult with IT Security, prior to implementing any system or process which involves the processing of any personal identifiable data of employees or residents.

9.2 Employees should be aware that AI tools can make errors, and human interaction is essential to quality check any content created by generative AI tools. There should be no loss of accountability when a decision is made with the help of, or by, an AI system, rather than solely by a human. Where an individual would expect an explanation from a human, they should instead expect an explanation from those accountable for an AI system.

9.2 Employees are to consider the ethical impact of using AI. The data which generative AI uses to create content comes from large, often uncontrolled data sets which may include biased

or harmful material, as the tools can only work with the information they are given, which can lead to bias.

9.3 Employees are reminded to stay in control and remember that if you put information into an AI tool you lose control of where it goes, and it can be used by the machine learning (ML) tool as 'training' for future responses, outside of Housing 21's control. This can lead to confidential information becoming public and result in personal data breaches or targeted cyber-attacks.

9.4 Where employees choose to use AI in a work capacity, ensure this is referenced to make individuals aware. This can be achieved by using a simple line such as 'content created by AI'. This is necessary if the content you use has been taken directly from an AI tool.

9.5 AI offers a lot of potential but comes with significant risks. If you are using AI tools like ChatGPT please do so cautiously and never input Housing 21 data that has not previously been made public.

9.6 Before conducting any further processing with AI, you must ensure that you conduct a DPIA if you are using this service in the long-term e.g for a project, as this constitutes as a high-risk activity.

9.7 **Employees are reminded not to input any Housing 21 personal identifiable data (or confidential business data) into these tools. To do so would be in breach of our data governance rules and may result in disciplinary action and/or legal or regulatory action.**

10.0 Privacy and Electronic Communications Regulation (PECR) (Direct Marketing)

10.1 All organisations are subject to certain rules and privacy laws when marketing to customers. This is captured under the PECR, which underpinned by the DPA18. A large proportion of fines issued by the ICO are because of grossly inappropriate marketing practices. The right to object to direct marketing must be explicitly offered to data subjects in an easy-to-understand form of words, so that it is clearly distinguishable from other information.

10.2 A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future. Failure to action such requests can result in a breach of PECR and the DPA18.

11.0 Sharing, Processing and Retaining Information

11.1 Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put into place. or we have sufficient legal basis for the processing/sharing. In this case a DPIA is required to be completed.

11.2 Personal data we hold may only be shared with another employee or agent if the recipient has a job-related need to know the information.

11.3 Personal data may also be shared with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services.
- sharing the Personal Data complies with the Privacy Notice provided to the data subject and, if required, the data subject's consent has been obtained.
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains GDPR approved third party clauses has been obtained.

11.4 If organisations such as Local Authorities request personal information about a customer you need to find out:

- why do they need the information?
- what will be done with the information?
- who else will they share the data with?
- inform the third-party agency of Housing 21's policy on confidentiality
- if the agency has their own robust policy on data protection and confidentiality which aligns with ours and is data protection compliant

11.5 Before sharing and disclosing personal information, it is important to ensure you seek the consent of the individual(s) concerned (if this has not been given) and provide limited identifiable information to meet the request for disclosure.

11.6 In certain circumstances, information may be disclosed without consent. The disclosure must be authorised by the Regional Director and/or Head of Department and advice should *always* be sought from the Data Protection Officer, dataprotection@housing21.org.uk.

11.7 These circumstances can include:

- Where Housing 21 has a statutory duty to disclose information, e.g., tax office, council tax office.
- Where the police are investigating a criminal matter.
- Information of a non-personal nature may be released. Personal information or requests to search premises must not be agreed without prior legal authority.
- Where public health or national security issues are involved (The Public Interest Disclosure Act 1998).

- When housing benefit is paid direct, Housing 21 has a duty to provide certain information, e.g., commencement of tenancy date, changes in rent and service charge etc.
- Where information relating to tenancy dates is requested in respect of statutory services such as gas and electricity supplies.
- Where information relating to tenancy dates is requested in respect of statutory services such as gas and electricity supplies.

12.0 Data Sharing

12.1 The organisation will only share personal data where we have a lawful basis, and it is necessary to do so. Where we share data with third parties / processors we shall carry out appropriate due diligence and ensure there is an adequate Data Sharing Agreement/Data Processing Agreement in place prior to any sharing of personal data with third parties.

12.2 The Data Protection Officer shall maintain a record of who data is shared and all data processors and is responsible for ensuring that appropriate agreements are in place.

12.3 The Data Protection Officer shall be responsible for maintaining the Data Sharing Procedure and the Selecting, Appointing, Managing and Decommissioning Data Processors Procedure and for ensuring that all relevant people are made aware of them.

13.0 Processing and Sharing Personal Data (Manual Records)

13.1 When confidential and sensitive personal data is being sent by post, wherever possible, the information should be checked by another employee/colleague before sending it, to ensure it is being sent to the correct recipient.

13.2 Internal and external mail containing personal information must be placed in a sealed envelope and, if possible, placed in a secondary envelope. The envelope and enclosed data must be clearly marked 'Private and Confidential'. Sealing paperwork twice provides an additional layer of security to manual records as a second barrier to the information being incorrectly opened by the wrong person.

13.3 External mail of an extremely confidential nature should always be sent by Special or Recorded Delivery, or by Courier, where possible.

13.4 When printing personal data, employees should always use the secure printing facility operated in all offices requiring the user to use their ID card to release print jobs. Personal data should not be left on printers and should be collected at the time of printing.

13.5 Maintaining a 'clear desk policy' further reduces the risk of unauthorised access to or loss of personal data. When you are not using files or paperwork of a personal and sensitive nature, always clear these away and store them securely. Never leave personal data unattended on

a desk once you have left the office at the end of a working day or if you know you will be attending a lengthy meeting, particularly if you are a home-based worker and have booked a hot desk for the day. N.B. This does not affect office-based employees from reasonably personalising their workspaces.

14.0 Processing and Sharing Personal Data (Electronic Records)

14.1 Employees sending personal data via email or other electronic media (e.g., Text, Workplace Chat, MS Teams Chat, Jabber etc.) should always take extra precautions to ensure information is sent to the correct individual. This is particularly relevant when emailing individuals outside of the organisation. ***Always*** ask the individual to spell their email address out for you as the same name can have many alternative spellings, for example, Sonia, Sonja, Sonya, etc.

14.2 All emails of a confidential nature and which contain personal data must be marked as 'Confidential' and should only be sent using the encrypted email software 'Mimecast', which is available on all employee email accounts. Please contact IT Service Desk (24999 or ITServiceDesk@Housing21.org.uk) for details on how to use this facility. Where a document containing personal data is sent, always password protect this and provide the password to the recipient in a separate email or telephone them.

15.0 Data Protection Compliance when Working from Home

15.1 It is important to maintain the integrity and security of the personal data that we process daily for our customers and employees.

15.2 All employees must ensure they continue to adhere to this policy and IT security policies, procedures, and processes, when working from home. Employees must:

15.2.1 Keep up office protocol. Lock your screen and clear your workspace at the end of your working day. The most common way of doing this is by simultaneously pressing 'control, alt, delete' and then clicking 'Lock' or simultaneously pressing the 'windows' key and letter 'L' key on your keyboard.

15.2.2 Continue to save files on SharePoint only, as this is the most secure place for them. Do not save any business personal data or business confidential data onto your desktop. Files saved on the desktop are not secure and your teams will be unable to access anything you have been working on if you are absent.

15.2.3 Be wary of hacking, scams and viruses which can result from phishing emails. Keep your wits about you and always remember 'don't trust, verify'. If it doesn't seem right, trust your instincts, and don't buy into the scam!

15.2.4 Always use the Mimecast facility to send emails/attachments to third party organisations as this ensures that they are transferred securely. **ALL** employees have this facility on their Outlook email.

15.2.5 Keep all paper-based files you have taken home with you as secure as you would in the office. Return all paperwork to your offices and if it is no longer required, only dispose of it when you return to the office, in the secure confidential waste bins. If you have a cross shredder, this can be used, ensuring it is separated at the time of disposal.

15.2.6 Reporting of compliance with the policy takes place as part of an annual review of the information governance framework and the policy framework. The review being carried out by the Information Governance Manager and reported to the Information Governance Steering Group, the Executive and the Audit and Assurance Committee.

16.0 Video Conferencing

16.1 The following guidance for video conferencing, if followed, will assist in mitigating data protection risks that may arise.

16.1.1 Separate work and social communication channels. Social and work-related communication channels should be separated to ensure that personal (and potentially sensitive) information is not captured on Housing 21 systems and equally that business-related communications are recorded on Housing 21 systems and not employee devices. Accordingly, employees should:

- **avoid unofficial channels** such as WhatsApp or other personal platforms or devices (i.e., iPads and other Android personal and tablets phones) when video calling for work-related purposes.
- Where possible only use Housing 21 approved platforms such as Microsoft Teams Chat.
- use an alternative video conferencing platform to that provided by Housing 21, for social calls; and
- ensure any device used has **all available system updates** and **antivirus software**

16.1.2 Exercise caution when subscribing to platforms. When subscribing to and using video conferencing platforms for social calls, employees should:

- be aware of the personal information being requested, assess **whether the information is necessary** and what its purpose is; and
- note any permissions granted to the platform and, ask whether they are necessary.

16.1.3 Be conscious of your physical environment. One of the more invasive features of video conferencing is that it is essentially opening a lens into your home. Accordingly, employees should:

- **be careful of what is being captured by the camera and microphone.** When finishing a video call make sure the camera and microphone are turned off/muted; and
- take into consideration and respect the **rights and interests of call participants** and those that may feature in the background of the call. Sharing a screenshot **o**r video taken during a video call may interfere with the individual's privacy rights (particularly given the relative ease and speed with which this material can be further disseminated).

16.1.4 Continue to stay alert to phishing emails or texts.

16.1.5 Know what to look out for in a video chat: The 'live chat feature' can be used by malicious people to spread phishing messages. Be vigilant. Don't click on links or attachments you were not expecting or from meeting attendees you do not recognise.

17.0 Personal Data Breach

17.1 The organisation will maintain a Data Breach Reporting Procedure and will ensure that all employees and those with access to personal data are aware of it and this personal data breaches policy can be found in the Information Governance and Security Policy and Procedure.

17.1.1 All employees and individuals with access to personal data for which the organisation is either data controller or processor must report all personal data breaches to an appropriate individual as set out in the Data Breach Reporting Procedure as soon as they become aware of the breach (whether this is actual or suspected).

17.1.2 The organisation will log all personal data breaches and will investigate each incident without delay. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data protection near misses will also be recorded and investigated in the same manner as data protection breaches.

17.1.3 The Personal Data Breach Procedure sets out responsibilities, decision-making criteria and timescales for notifying data subjects, the Information Commissioner and the media about a personal data breach.

17.1.4 The Data Protection Officer shall be responsible for maintaining the Data Breach Reporting Procedure and for ensuring that all relevant people are made aware of it.

17.2 A data breach can occur in many ways, for example (this list is not exhaustive)

- Theft or accidental loss of personal data
- A deliberate attack on the organisation's systems
- The unauthorised use of personal data by an employee
- Mistakenly sending personal data to an unintended recipient
- Accidentally sharing your screen (when third party personal data is visible) during a video call

17.3 The legislation requires Housing 21 to notify any Personal Data Breaches to the ICO and, in certain instances, to the Data Subject within 72 hours of becoming aware of the breach.

17.4 If you know or suspect that a Personal Data Breach has occurred, **do not** attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches (Data Protection Champion), the Data Protection Officer (DPO) the IT Helpdesk and follow the Security Incident Event Management (SIEM) Procedure. You should preserve all evidence relating to the potential Personal Data Breach.

17.5 The penalties for breaching the Act can be severe as the ICO has regulatory powers to:

- Impose monetary penalties of up to, approximately £18 million, or 4% of total worldwide annual turnover, whichever is the higher (dependent upon the severity of the data breach);
- Issue an Undertaking or Enforcement Notice requiring an organisation to take remedial action and update procedures and train employees; and/or
- Criminally prosecute organisations and in some circumstances individuals or employees of the organisation.

17.6 If personal information has been lost, stolen, or otherwise dealt with in contravention of this Policy, it must **immediately (within 24 hours)** be reported to Housing 21's Data Protection Officer or in the case of an electronic data breach the IT Service Desk/. IT Security Manager who will inform the Data Protection Officer. This will allow for the appropriate reporting to the ICO and expedient mitigating actions to be carried out.

17.7 The Data Protection Officer (DPO) is responsible for overseeing this Policy and, as applicable, developing related policies and privacy guidelines. The post is held by the Information Governance Manager.

18.0 Data Retention

18.1 Housing 21 shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

18.2.1 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

18.2.2 For full details of the Housing 21's approach to data retention, including retention periods for specific personal data types held by the us, please refer to our Data Retention Policy which is available on request.

19.0 Related Policies, Procedures and Legislation

- Data Protection Glossary and Terms
- Data Subject Access Request Guidance
- Document Retention Policy and Procedure
- Information Governance and Security Policy and Procedure
- Equality, Diversity, and Inclusion Policy
- Reasonable Adjustment Policy
- Safeguarding Policy and Procedure
- IT Acceptable Use Policy and Procedure
- Work Location Policy and Procedure
- UK General Data Protection Regulation (UKGDPR)
- Data Protection Act 2018 (DPA18)
- Crime and Disorder Act 1998
- The Human Rights Act 1998
- The Public Interest Disclosure Act 1998
- The Access to Medical Reports Act 1988
- Access to Health Records Act 1990
- Privacy and Electronic Communications Regulations (PECR)

Appendix A

Data Protection Procedure: Glossary and Terms

This document has been produced to enable employees to gain a better understanding of the terms used within the data protection legislation and regulation and should be read in conjunction with Housing 21's Data Protection Policy.

Data Protection Act 2018 (DPA18)	Consent Explicit Consent
General Data Protection Regulation	Artificial Intelligence
European Economic Area (EEA)	Automated Processing
Information Commissioners' Office	Automated Decision Making
Data Protection Principles	Purposes (Data Classes)
Data Controller	Privacy by Design
Data Processor	Data Privacy Impact Assessments
Data Processing	Privacy Guidelines
Data Processing Agreements	Privacy Notices
Data Subjects	Data Breach
Data Recipients	Recording Information
Third Parties	Relevant Filing System
Data Subject Access Request (DSAR)	Storing and Securing
Disclosure	Transfers
Data Protection Officer (DPO)	Security Statement
Personal Data	Information Notice
Special Category Data (Sensitive)	Enforcement Notice
Pseudonymisation/Pseudonymised	Information Tribunal

Data Protection Act 2018 (DPA18)

The Data Protection Act 2018 (DPA18) is the UK's implementation of the General Data Protection Regulation (GDPR). The DPA18 and GDPR provide individuals with the right to know what personal and sensitive (special category) information is held about them, how it is processed and safeguarded and sets out requirements for organisations to adhere to when collecting and processing personal data.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area, which replaces the Data Protection Directive. When the UK left the EU on the 31 December 2020, we adopted the UK GDPR alongside the Data Protection Act 2018, to ensure that we remain compliant with the EU Data Protection Regulation (EU GDPR 2016/679).

European Economic Area (EEA)

The UK was a part of the EEA until we left on the 31 December 2020. The EEA includes EU countries in addition to Iceland, Liechtenstein, and Norway. It allows them to be part of the EU's single market. Switzerland is neither an EU nor EEA member but is part of the single market, this means Swiss nationals have the same rights to live and work in the UK as other EEA nationals. More guidance will follow here once we have been provided steer from the Government and the ICO.

Information Commissioners' Office (ICO)

The ICO is an independent office holder appointed by the Crown to administer and enforce the data protection legislation, the Freedom of Information Act 2000, the Environmental Information Regulations (EIR) and the Privacy and Electronic Communications Regulations (PECR). The ICO's role in terms of data protection is providing advice, promoting good practice and enforcement. They have the powers to issue fines to organisations for severe breaches of data protection and/or PECR. The ICO is independent of the Government and reports directly to Parliament.

Data Protection Principles

There are seven Principles under the GDPR and DPA18 which Housing 21 employees must ensure they abide by when processing personal data:

Principle 1 Personal Data shall be obtained and processed fairly, lawfully, and transparently. (Lawfulness, Fairness and Transparency)

This means personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. Therefore, we may only collect, process, and share personal data fairly and lawfully and for specified purposes. The DPA18 restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process personal data without adversely affecting the Data Subject. The legislation allows processing for specific purposes, some of which are set out below:

- the Data Subject has given their consent.
- the Processing is necessary for the performance of a contract with the Data Subject.
- to meet our legal compliance obligations.
- to protect the Data Subject's vital interests; or
- to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices

Employees must identify and document the legal ground being relied on for each processing activity before a new project or disclosure involving the collection and processing personal data is considered.

With regards to transparency Housing 21 are required to provide detailed, specific information to data subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we must provide the data subject with following information: the identity of the Data Controller and DPO; how and why we will use, process, disclose, protect and retain their personal data through a Fair Processing Notice which must be presented when the data subject is first requested to provide their personal data.

When personal data is collected indirectly (for example, from a third party or publicly available source), you must provide the data subject with all the information required by the legislation, as soon as possible after collecting/receiving the data. You must also check that the personal data was collected by the third party in accordance with the legislation and on a basis which contemplates our proposed processing of that personal data.

You must comply with Housing 21's guidelines on drafting Privacy Notices/Fair Processing Notices.

Principle 2 Personal Data shall be collected for specified, explicit and legitimate purposes, for which consent is recorded. (Purpose Limitation)

This means personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot use personal data for new, different, or incompatible purposes from that disclosed when it was first obtained unless you have informed the data subject of the new purposes and they have consented where necessary.

Principle 3 **Personal Data shall be adequate, relevant, and limited to only what is necessary for the purpose for which it is obtained. (Data Minimisation)**

This means personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

You may only process personal data when performing your job duties requires it and you cannot process personal data for any reason, unrelated to your job role/duties.

You may only collect personal data that you require for your job duties: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.
You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the company's data retention guidelines.

Principle 4 **Personal Data shall be accurate and, where necessary, kept up to date. (Accuracy)**

This means personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. You will ensure that the personal data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which it was originally collected. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy and/or amend inaccurate or out-of-date personal data.

Principle 5 **Personal Data shall not be kept in a form which permits identification of Data Subjects for longer than necessary for the purposes for which the data is processed. (Storage Limitation)**

This means personal data must not be kept in an identifiable format for longer than is necessary for the purposes for which the data is processed. This means personal data must not be retained in a format which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected, including for the purpose of satisfying any legal, accounting or reporting requirements.

Housing 21 will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time, in compliance with the organisations Records Management Policy and Records Management and Retention Schedule.

You will take all reasonable steps to destroy or erase, from our systems, all personal data that we no longer require in accordance with Housing 21's Records Management and Retention Schedule, Policy, and Procedure. This includes requiring third parties to delete such data, where applicable.

You will ensure data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

Principle 6 **Personal Data (manual and electronic) must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. (Security, Integrity, and Confidentiality)**

This means Housing 21 must protect personal data and must secure it by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

We will develop, implement, and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable).

We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. Employees are responsible for protecting the personal data we hold.

You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.

You must exercise particular care in protecting special category personal data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity, and availability of the personal data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users can access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of our Information Governance and Security Policy and Procedures, and you must comply with and not attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain in accordance with the DPA18 and relevant standards to protect personal data.

Accountability Principle
Housing 21 and their employees are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability)

Data Controller
A Data Controller can be a person or an organisation responsible for all personal information/data which relates to living, identifiable individuals. A Data Controller determines when, why and how any personal information is processed, managed, stored, and made secure. It is responsible for establishing practices and policies in line with the DPA2018 and GDPR.

A Data Controller is required to pay an annual fee to the Information Commissioners Office (ICO) unless they are exempt. In addition to the fee, a Data Controller is also required to register a Data Protection Officer (DPO) with the ICO on an annual basis with the following detail:

- Purposes (for processing personal data)
- Data Subjects (whose personal data is being processed)
- Data Classes (the type of personal data processed)
- Recipients (the receivers of personal data)
- Transfers (define any overseas transfers of personal data)
- Security Statement (how are we are keeping the personal data secure)

Housing 21 is a Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes. Our ICO Registration Number is: **Z5515259.** The registered Data Protection Officer for Housing 21 is: Sonia Hawley, Information Governance Manager and Data Protection Officer (DPO).

Data Processor
A Data Processor is any person (*other than* an employee of the Data Controller) who processes personal data on behalf of the Data Controller, these can include: (this list is not exhaustive)

- Agency employees as they are employed to process information and are not employed directly by the Data Controller
- Confidential Waste Companies
- Document Management System providers

Data Processing
This refers to any actions either verbal (when recorded), manual or electronic that involve the use of personal data. Processing can be any function which is carried out on personal information such as: receiving; recording; adapting; altering; retrieving; consulting; disclosing; transmitting and disseminating; making available; aligning or combining; blocking, erasing, or destroying; dictating; emailing; inputting; writing. Processing also includes transmitting or transferring personal data to third parties.

Data Processing Agreements
Data Processing Agreements should be in place between a Data Controller and any person, organisation and/or body when they are going to carry out processing duties on behalf of the data controller. Always seek advice from the Procurement Department and the Data protection Officer when embarking on a new project which will involve the processing of personal data by a third-party provider/supplier.

Data Subject
A Data Subject is any living, identifiable individual (the legislation does not extend to the personal data of the deceased**)** who is the subject of personal data and refers to any person who can be identified directly or indirectly, via an identifier such as:

- Name
- ID Number (e.g., payroll number, employee number)
- Location data

Or via factors specific to a person's physical, physiological, genetic, mental, economic, cultural, or social identity.

Examples of Data Subjects at Housing 21 are: (this list is not exhaustive)

- All employees; current, past, or prospective
- Employees including volunteers, agents, consultants, contractors, temporary, casual, and fixed term employees
- All residents; current, past, or prospective
- Board Members

Data Recipients
This refers to any person to whom the personal data is disclosed to while processing the data for the data controller and can include the following:

- Employees of the data controller
- Data processor acting on the instruction of the data controller
- Agents or employees of the data processor

Third Parties
A third party in relation to personal data is any person or organisation other than the:

- Data controller
- Data subject
- Data processor
- Any employee or authorised person of the data controller or data processor

The following are some examples of third parties:

- An agent acting on behalf of the data subject e.g., Solicitor
- An employee who has left the company, but the data controller still holds information they have processed in the course of their duties
- A relative, friend, or agent of the data subject asking for information on them

However, third parties can also be the Police, Solicitors, Health, and Social Work agencies and Regulatory or Government bodies. These third parties can be entitled to information if it is in connection with a particular inquiry made in the exercise of a statutory power:

- **Crime:** Police activity involving the detection of or the prevention of crime, the apprehension or prosecution of offenders.
- **Taxation:** The assessment or collection of any tax or duty, or any imposition of a similar nature.
- **Court Proceedings:** A legal step or action taken at the direction of, or by the authority of, a court or agency with the intention to prosecute or defend.
- **Health and Social Work:** Liaising with agencies, health authorities in cases such as safeguarding, for example.
- **Regulatory Activity:** Care Quality Commission (CQC) assessments and audits.

Data Subject Access Request (DSAR)
Data protection legislation gives individuals who are subject of personal information a general right of access to the personal information which relates to them. These rights are known as 'subject access'. A formal procedure needs to be followed in relation to this matter, therefore please refer to Housing 21's **Data Subject Access Request Procedure**, for more details.

Disclosure
Is a set of documents released to the data subject which have been collated from the personal information we hold, process, and store both electronically and manually, and has had a full data protection assessment. The disclosure is normally supplied with redactions (words blanked out) as they are exempt under the provisions of the act. Please refer to the **Data Subject Access Request Procedure** for full details.

Data Protection Officer (DPO)
This is the individual appointed, by Housing 21, under the DPA18 who is responsible for embedding data protection compliance across the organisation and providing employees with the training and tools to comply with the Regulation and Legislation in their day-to-day activities. The registered Data Protection Officer for Housing 21 is: Sonia Hawley, Information Governance Manager and Data Protection Officer (DPO) who can be reached at: DataProtection@Housing21.org.uk.

Personal Data
Personal data is any information which relates to a living individual (Data Subject) who can be identified from the information. It also extends to any information which *may* identify the individual.

Data Subjects can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access.

Personal Data includes special categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (e.g., Name, email address, location, or date of birth) or an opinion about that person's actions or behaviour. Examples of personal data include:

- Name and address
- Date of Birth
- Statement
- Any expression or opinion communicated about an individual
- Minutes of meetings, reports
- Emails, file notes, handwritten notes, sticky notes
- CCTV footage if an individual can be identified by the footage
- Employment and Tenancy applications
- Spread sheets, or any list of set up by code or employee/tenant reference number
- Initials
- Job Title

Personal data may only be processed provided:

- The individual has given their explicit consent to the processing
- It is necessary for the performance of a contract with the individual
- It is required under a legal obligation
- It is necessary to protect the vital interests of the individual
- It is to carry out public functions
- It is necessary to pursue the legitimate interests of the data controller or certain third parties (unless this is prejudicial to the interests of the individual)

Special Category (Sensitive) Data
This is any information revealing an individual's:

- Ethnicity or racial origin
- Sexual orientation
- Sex life
- Religious or philosophical beliefs
- Political opinions
- Membership of a trade union
- Health, physical or mental health conditions
- Biometric date
- Genetic data

This information may only be processed provided:

- The individual has given their explicit consent (i.e., signature or has opted-in)
- The individual has already made this information public
- It is to protect the vital interests of the individuals or other individuals
- It is necessary for the purposes of, or in connection with legal proceedings or for obtaining legal advice and for the administration of justice or any enactment, function of the Crown
- It is necessary for the administration of justice
- It is for medical purposes and is undertaken by a health professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to a health professional
- It is necessary for the purposes of exercising or performing any right or obligation as data controller in connection with employment

Pseudonymisation Or Pseudonymised Data
This is replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Consent
This is agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

This means Housing 21 must only process personal data on the basis of one or more of the lawful basis set out in the DPA18, which include consent.

A Data Subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.
Unless we can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data, for automated decision-making and for cross border data transfers. Usually, we will be relying on another legal basis (and not require explicit consent) to process most types of sensitive data. Where explicit consent is required, you must issue a Fair Processing Notice to the Data Subject to capture explicit consent.

You will need to evidence consent captured and keep records of all consents so that we can demonstrate compliance with consent requirements.

Explicit Consent
This is consent which requires a very clear and specific statement (that is, not just action). Explicit consent therefore means that the data subject must give an express statement of consent, for instance, in a written (signed) statement. This is only required when using it as a basis for processing special category data.

Artificial Intelligence
Artificial Intelligence (AI) can be defined in many ways. However, within ICO guidance, this is defined as umbrella term for a range of algorithm-based technologies that solve complex tasks by carrying out functions that previously required human thinking. Decisions made using AI are either fully automated, or with a 'human in the loop'. As with any other form of decision-making, those impacted by an AI supported decision should be able to hold someone accountable for it.

Automated Processing
This refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements. Profiling is an example of Automated Processing.

Automated Decision-Making
This is when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. It is important to note that the DPA18 prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

1. Housing 21 is **[not]** currently using personal data in automated decision-making processes. In the event that that this situation changes, Housing 21 shall notify data subjects of its' intentions to commence such processing.
2. Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the UK GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Housing 21.
3. The right described in 2. does not apply in the following circumstances:
1. The decision is necessary for the entry into, or performance of, a contract between H21 and the data subject;
2. The decision is authorised by law; or
3. The data subject has given their explicit consent.

Purposes (Data Classes)
The Data Controller must provide a general description of the personal information which it intends to process with the ICO. This is referred to as the 'purpose.' Some examples of the 'purpose' or 'data classes' can be found on the following documents at Housing 21:

- Tenancy Applications
- Employment Applications
- Advertising, Marketing and Public Relations
- Accounts and Records

The following are examples of data classes which Housing 21 currently use:

Employee, Agent, and Contractor Administration.

- Personal Details; Family, Lifestyle and Social Circumstances; Education and Training Details; Employment Details; Financial Details; Goods or Services Provided; Racial or Ethnic Origin; Religious or Other Beliefs of a Similar Nature; Trade Union Membership; Physical or Mental Health or Condition; Offences (Including Alleged Offences)

Advertising, Marketing, Public Relations, General Advice Services.

- Personal Details, Family, Lifestyle and Social Circumstances; Employment Details; Financial Details; Physical or Mental Health or Condition; Offences.

Data Protection by Design and Default

This involves implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the DPA18. This means Housing 21 needs to consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data.

The organisation shall consider privacy by design and by default when processing personal and special category data. Privacy by design and by default is a legal obligation. Privacy by design and by default requires organisations to consider data protection issues at the design stage of the processing and throughout its cycle.

Data Privacy Impact Assessment (DPIA)

These are the tools and assessments used to identify and reduce risks of a data processing activity. The DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the processing of personal data. Employees should conduct DPIAs (and discuss your findings with the DPO) when:

- implementing major system or business change programs involving the Processing of Personal Data including:
- using new technologies (programs, systems, or processes), or changing technologies (programs, systems, or processes).
- considering Automated Processing, including profiling.
- conducting large scale processing of sensitive data; and large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate.
- an assessment of the necessity and proportionality of the Processing in relation to its purpose.
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

The templates for both DPIA Internal and DPIA External can be found on the Information Governance pages on the intranet or can be provided upon request to the DPO.

Privacy Guidelines
These are Housing 21's privacy related guidelines provided to assist in interpreting and implementing the Data Protection Policy and related policies.

Privacy Notices
(Also referred to as Fair Processing Notices (FPNs), Data Protection Notices or Privacy Policies)
These are separate notices setting out information that may be provided to data subjects when the Housing 21 collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.

To fully meet the requirements of data protection regulation and legislation Data Controllers are required to issue Fair Processing Notices (FPNs) to anyone who they collect, receive, process and store information from.
The purpose of this notice is to inform individuals of their rights regarding information held about them, why it is held and who it may be shared with, passed onto. It is always best practice to have a fair processing notice on resident and/or employment application forms.

Data Breach
This is any act or omission that compromises the security, confidentiality, integrity, or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure, or acquisition (including through theft), of personal data is a data breach.

The Information Commissioners Office (ICO) will take relevant action against a data controller, which is known and referred to as enforcement action. This can include being issued with substantial monetary fines and/or employees themselves being the subject of direct prosecution, if it is determined that the data breach was intended and malicious in nature.

You are required to report this within 24 hours internally, to ensure that there is enough time to report to the ICO and inform data subjects (if required). In relation to reporting the incident, please notify the DPO at dataprotection@housing21.org.uk within 24 hours (working) of the breach.

For full details on how to report a data incident or breach, please refer to Housing 21's **Security Incident Event Management (SIEM) Plan**. It is important to note that all data incidents (even suspected) and breaches, should be notified to either the IT Helpdesk or the Data Protection Officer (DPO) with immediate effect, as the DPO is required to carry out an investigation surrounding the circumstances of the breach and where applicable, inform the ICO within 72 hours of being made aware of any serious breaches of personal data.

Recording Information

There are strict controls for recording information which data controllers are required to comply with:

- Only relevant an updated personal data should be held
- Personal data should not be kept for longer than necessary and only for the period during which it is being processed
- Medical judgements and subjective comments should be avoided
- Reports should be clear, concise, and accurate
- Confidential information from third parties should be recorded on file in such a way as to ensure it can be easily removed or made secure if it is sensitive personal data
- Inaccurate and subjective information should be removed from files and destroyed

Relevant Filing System

This is manual information relating to an individual which has been:

- Processed by electronic means
- Intended to be processed by electronic means
- Has and is still processed by electronic means

Or is in a structured manual file which has been set up in a manner where the individual's information can be readily accessed and located by:

- Reference to the individual
- Reference to the criteria relating to the individual
- Dividers setting out the topic, name and identifying information of the individual

Storing And Securing

It is a requirement for Data Controllers to ensure all manual and electronic information is kept secure and that personal data cannot be accessed by third parties. Therefore, ensuring they comply with the security statement in their notification. The following applies to all employees, including home based workers:

- All files are secure
- Clear desk and screen protocols are in place

- Restrictions are in place to ensure third parties are unable to view data during visits and/or video conferencing.
- All paper-based files are stored at the end of the day in lockable secure cabinets and the keys are also safely stored
- Electronic devices such as mobile phones, tablets, memory sticks, laptops and computers should all be encrypted, and password protected
- Adequate security controls are on place to prevent unauthorised access such as hacking and in the event of a loss items should be deactivated as soon as the organisation has been notified of the loss
- Adequate measures and procedures are in place for retention and destruction of both manual and electronic data when no longer needed

Transfers
This is any information which you intend to transfer outside of the European Economic Area (EEA). Advice should always be sought from the DPO, prior to any consideration of internal transfers of our employee or resident personal data.

Security Statement
This is part of the general description of information which data controllers are required to declare as part of their notification with the ICO. This statement should cover our security measures on: Information security; controlling physical security; control on access to information; business continuity plans; training employees; handling breaches of security

Information Notice
An Information Notice is a legal document which the ICO can issue to a data controller requiring them to supply information to the Commissioner within a prescribed time so that he can assess whether the data controller is complying with data protection legislation.

Enforcement Notice
An Enforcement Notice is a legal document which the ICO can issue to a data controller requiring them to take certain steps to comply with data protection legislation.

Information Tribunal
An Information Tribunal is a body set up where a data controller can appeal against an information or enforcement notice served by the ICO.

Further Advice and Assistance
This can be a complex area so for more detailed information, advice, or guidance, please contact the Information Governance Manager and Data Protection Officer) at: dataprotection@housing21.co.uk or refer to the information governance pages on the intranet.