Data Protection Policy

Version	4.0	**Issue Date**	August 2020	**Review**	July 2021
Author	Sonia Hawley	**Job Title**	Senior Information Governance Officer & Data Protection Officer (DPO)		

Summary

The Data Protection Act 2018 (DPA18) is the UK's implementation of the General Data Protection Regulation (GDPR). The DPA18 & GDPR provide individuals with the right to know what personal and sensitive (special category) 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.

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
- Data Controller obligations in the protection of personal data
- Individuals rights in relation to their personal data

The term 'employee' refers to all Housing 21 employees, including: permanent, fixed term, temporary, Board Members, secondees, third party representatives, agency workers, volunteers, interns and agents.

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.

Data Protection

Data Protection applies to all personal and sensitive (special category) 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').

'**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)

- A person'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

[1] This list is not exhaustive: Desktop PC's, Laptops, Tablets, and Mobile Phones.

[2] Manual records are paper based and structured, accessible and form part of a relevant filing system (filed by subject, reference dividers or content), where individuals can be identified and personal data easily accessed without the need to trawl through a file.

- 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.

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 Housing 21 or certain third parties (unless this is prejudicial to the interests of the individual)

'**Special Category Data**' is any information relating to an individual's:
- Ethnicity
- Gender
- Religious or Other Beliefs
- Membership of a Trade Union
- Sexual Orientation
- Physical or mental health conditions
- Offences committed or alleged to have been committed by that individual
- Biometric or genetic data

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

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.

Requests for personal data on deceased individuals may be covered by the Access to Health Records Act 1990. Employees should process such requests on a case by case basis and always consult with their manager before making a data disclosure. If unsure please consult with the Data Protection Officer (DPO).

Data Protection Principles
There are 7 (6 +1) 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)

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)

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)

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

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)

Principle 6 Personal Data (manual and electronic) must be processed in an 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)

Accountability Principle

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

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.

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 Privacy by Design 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.

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 are able to access the personal data when they need it for authorised purposes.

Employee Obligations
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 be kept secure at all times.

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

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

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.

Where employees do not comply with this policy, Housing 21 may also consider taking action in accordance with our disciplinary processes. Where it is found that an employee has knowingly (with intent) and maliciously 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 where a data breach has been found to have caused any actual or potential distress to our residents or employees.

Data Controller (Housing 21) Obligations
Housing 21 will follow the Code of Practice issued by the ICO when developing policies and procedures in relation to data protection compliance.

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.

Housing 21 will adhere to and follow the 7 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.

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 recommendations outlined in the legislation.

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 a large number of individuals. Housing 21 will conduct Legitimate Interest Assessments (LIAs) where it considers that it relies on Legitimate Interests as defined in the GDPR and DPA18, to process data.

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

[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.

Individuals ('Data Subjects') Rights

Housing 21 acknowledges individuals (data subjects) rights when it comes to how we handle their data. These include 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 on the basis of 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.

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).

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 'data 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 detailed guidance. Where an individual requests access to personal data held by Housing 21, always contact the organisation's Data Protection Officer (DPO), Sonia Hawley.

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.

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.

Each Corporate Department, Extra Care and Retirement Housing 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.

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

Record Keeping
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. Each Corporate and Operational business area has an Information Asset Register (IAR) which accurately details this information.

Training and Auditing
Housing 21 are required to ensure all employees have undergone mandatory data privacy related training to enable them to comply with data privacy laws. We also regularly test our systems and processes to assess compliance.

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.

Privacy by Design and Data Protection Impact Assessments (DPIAs)
Housing 21 are required to implement Privacy by Design 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.

You must assess what Privacy by Design 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.

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.

Direct Marketing
All organisations are subject to certain rules and privacy laws when marketing customers. A large proportion of fines issued by the ICO are as a result 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.

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.

Sharing, Processing and Retaining Information
Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put into place.

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. 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.

If agencies such as Supporting People or Social Services 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

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.

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, Sonia Hawley.

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.

Processing and Sharing Personal Data (Manual Records)
When confidential and sensitive personal data is being sent by post, wherever possible, the information should be checked by another member of staff before sending it, to ensure it is being sent to the correct recipient.

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.

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

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.

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.

Processing and Sharing Personal Data (Electronic Records)
Staff 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.

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 Outlook accounts. Please contact IS Service Desk (24999) for details on how to use this facility. Where a document is attached, always password protect this and provide the password to the recipient in a separate email or telephone them.

Data Protection Compliance when Working From Home
It is important to maintain the integrity and security of the personal data that we process on a daily basis for our customers and employees.

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

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

- Continue to save files on shared drives 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.

- 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! Follow this helpful guide: http://wilma.universe.local/HowDoI/Pages/Deal-with-spoof,-phishing-or-fraudulent-emails.aspx

- 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. Follow this guidance: http://wilma.universe.local/HowDoI/Pages/Send-Encrypted-Email.aspx.

- 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 separated at the time of disposal.

Video Conferencing

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

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 and Workplace 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**

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.

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).

Continue to stay alert to phishing emails or texts

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.

Personal Data Breach

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 a staff member
- Mistakenly sending personal data to an unintended recipient
- Accidentally sharing your screen (when third party personal data is visible) during a video call

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. 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 IS Helpdesk and follow the Security Incident Event Management (SIEM) Procedure. You should preserve all evidence relating to the potential Personal Data Breach.

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 staff; and/or
- Criminally prosecute organisations and in some circumstances individuals or employees of the organisation.

In the event that personal information has been lost, stolen or otherwise dealt with in contravention of this Policy, it must **immediately** be reported to Housing 21's Data Protection Officer or in the case of an electronic data breach the IS Service Desk 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.

Data Protection Officer (DPO)

The DPO is responsible for overseeing this Policy and, as applicable, developing related policies and privacy guidelines. The post is held by Sonia Hawley, Senior Information Governance Officer & Data Protection Officer (DPO), Sonia.Hawley@Housing21.org.uk.

Please contact the DPO with any questions or concerns about this Policy, data protection and security, or if you are concerned this Policy is not being or has not been followed. Always contact the DPO in the following circumstances:

- you are unsure of the lawful basis which you are relying on to process personal data;
- you need to rely on consent and/or need to capture explicit consent;
- you need to draft Privacy Notices or Fair Processing Notices;
- you are unsure about the retention period for the Personal Data being Processed;
- you are unsure about security or other measures you need to implement to protect personal data;
- there has been a Personal Data Breach;
- you need any assistance dealing with any rights invoked by a data subject;
- whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use personal data for purposes others than what it was collected for;
- you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;
- you need help complying with applicable law when carrying out direct marketing activities; or
- you need help with any contracts in relation to sharing Personal Data with third parties

Related Policies, Procedures and Legislation

- Data Subject Access Request Guidance
- Document Retention Policy and Procedure
- Information Governance and Security Policy and Procedure
- Equality, Diversity and Inclusion Policy
- Safeguarding Policy and Procedure
- IS Acceptable Use Policy and Procedure
- General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (DPA18)
- Crime and Disorder Act 1998
- Common Law Duty of Confidentiality
- 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)