Data Protection Policy (Privacy Standard)

Version	3.0	**Issue Date**	April 2018	**Review**	May 2019
Author	Deirdre LaBassiere	**Job Title**	Senior Information Governance Officer & Data Protection Officer (DPO)		

Summary

The General Data Protection Regulations (EU 2016/679) (GDPR) gives individuals the right to know what information is held about them, how it is processed, how it is safeguarded and sets out requirements for organisations processing personal data (referred to under the GDPR as 'Data Controllers'). The GDPR is overseen and enforced by the Information Commissioners' Office (ICO) who is an independent public body directly responsible to Parliament.

Housing and Care 21, as a Data Controller has a legal obligation to protect and manage the personal information of our customers, suppliers, colleagues, volunteers, employees, website users and other third parties (past or present), regardless of the media on which that data is stored.

This Privacy Standard sets out clear guidance on:

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

This Privacy Standard applies to all Housing and Care 21 staff. The term 'staff' refers to all Housing and Care 21 staff, including; permanent, fixed term, temporary, Board Members, secondees, third party representatives, agency workers, volunteers, interns and agents.

You must read, understand and comply with this Privacy Standard when processing Personal Data on behalf of Housing and Care 21 and attend training on its requirements. This Privacy Standard sets out what we expect from you in order for us to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Related Policies and Privacy Guidelines are available to help you. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Privacy Standard may result in disciplinary action.

This Privacy Standard (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, customers or regulators without prior authorisation from the Data Protection Officer (DPO).

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

'**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)

1. A person's name, address (postal and email) or Date of Birth
2. A statement of fact and/or any expression/ opinion communicated about an individual's actions or behaviour
3. Minutes of meetings and reports which refer to an individual
4. Emails, file notes, handwritten notes, sticky notes in relation to an individual
5. Individual identifiable CCTV Footage
6. Lettings, Sales and Employment application forms
7. Care Support Plans and Housing Files
8. 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 and Care 21 or certain third parties (unless this is prejudicial to the interests of the individual)

'**Sensitive Personal Data**' is any information relating to an individual's:

1. Ethnicity
2. Gender
3. Religious or Other Beliefs
4. Membership of a Trade Union
5. Sexual Orientation
6. Physical or mental health conditions
7. Offences committed or alleged to have been committed by that individual
8. Biometric or genetic data

Sensitive personal 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

[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.

- 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 a living, identified or identifiable individual who is the subject of personal data whether in a personal or business capacity.

What are the key principles we use when processing personal data?

There are 8 Principles under the GDPR which Housing and Care 21 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 (for which consent is recorded). (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 shall be made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests)

Principle 7 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)

Principle 8 Personal Data shall not be transferred outside the European Union unless that Country provides adequate levels of protection for the rights of the Data Subject. (Transfer Limitation)

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

Lawfulness, Fairness and Transparency
Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR 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 fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

- the Data Subject has given his or her 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

You must identify and document the legal ground being relied on for each Processing activity.

Consent

Housing and Care 21 must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, 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.

Transparency (Notifying Data Subjects)

The GDPR requires Housing and Care 21 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 all the information required by the GDPR including the identity of the Data Controller and DPO, how and why we will use, Process,

disclose, protect and retain that Personal Data through a Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data..

When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the GDPR 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 GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

You must comply with the Company's guidelines on drafting Privacy Notices/Fair Processing Notices.

Purpose Limitation

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.

Data Minimisation

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. You cannot Process Personal Data for any reason unrelated to your job 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.

Accuracy

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 we collected it. 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 or amend inaccurate or out-of-date Personal Data.

Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

Housing and Care 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. You must comply with the Company's guidelines on Data Retention.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. 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.

Security, Integrity and Confidentiality

We 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. You 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 Sensitive 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 are able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of our Information 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 GDPR and relevant standards to protect Personal Data.

Transfer Limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to

a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

- appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

- the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

How do we ensure compliance with the GDPR?

Staff Obligations
Staff 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.

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

Staff who manage and process personal or sensitive personal information will ensure that it is kept secure and where necessary, confidential. Sensitive personal information will only be processed in line with the provisions set out in the Data Protection Procedure.

Staff are responsible for notifying their line manager or the Senior Information Governance Manager/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.

Data Controller (Housing and Care 21) Obligations
Housing and Care 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 and Care 21 will ensure that Data Processing and/or Data Sharing Agreements, where Housing and Care 21 is the Data Controller, clearly outlines the roles and responsibilities of both the Data Controller and the Data Processor.

[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.

Housing and Care 21 will adhere to and follow the 8 Principles of the Act 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 and Care 21 will not transfer or share personal information with countries outside of the European Economic Area (EEA) unless that country has a recognised adequate level of protection in place in line with the recommendations outlined in the Act.

Housing and Care 21 will conduct Data Protection Impact Assessments which processing personal data that may result in high risk to data subjects or where we are processing information that relates to a large number of individuals. Housing and Care 21 will conduct Legitimate Interest Assessments where it considers that it relies on Legitimate Interests as defined in the GDPR to process data.

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

Individuals ('Data Subjects') Rights
Housing and Care 21 acknowledges individuals (data subjects) rights under the GDPR 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;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on Automated Processing, including profiling (ADM);
- 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 their rights and freedoms;
- make a complaint to the supervisory authority (the ICO); and
- in limited circumstances, receive or ask for their 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 and Care 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 'subject access'. A formal procedure needs to be followed in relation to this matter, therefore please refer to Housing and Care 21's **Subject Access Request Guidance** for more detailed guidance.

Where an individual requests access to personal data held by Housing and Care 21, always contact the Senior Information Governance Officer, Deirdre LaBassiere.

Housing and Care 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 GDPR.

Housing and Care 21 will only share information in accordance with the provisions set out in the GDPR and where applicable, Housing and Care 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 GDPR.

Each Corporate Department, Extra Care Court and Retirement Housing Scheme is responsible for the personal data which is holds. This responsibility extends to personal data that is processed by any third parties on behalf of Housing and Care 21.

Housing and Care 21 recognise and understand the consequences of failure to comply with the requirements of the GDPR may result in:

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

Where staff do not comply with this policy, Housing and Care 21 may also consider taking action in accordance with our disciplinary processes.

Access to the Records of the Deceased

Requests for data on deceased individuals from closed records are not requests under the GDPR (as they are not in connection with a living individual). The purpose of the request needs to be identified and staff should consult with their line manager and the Senior Information Governance Officer before proceeding with giving information. These records are covered by the Access to Health Records Act 1990.

How do we maintain Accountability to GDPR, Data Subjects and to Housing and Care 21?

Housing and Care 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 and Care 21 has put adequate resources and controls in place to ensure and to document GDPR 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 Privacy Standard, Related Policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices;
- regularly training Company Personnel on the GDPR, this Privacy Standard, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and
- 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.

Record Keeping
The GDPR requires us to keep full and accurate records of all our data Processing activities.

You 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 a minimum, the name and contact details of the Data Controller and the DPO, 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. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

Training and Auditing
We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data

Privacy by Design and Data Protection Impact Assessment (DPIA)
We 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 data privacy principles.

You must assess what Privacy by Design measures can be implemented on all

programs/systems/processes that Process Personal Data by taking into account the following:

- the state of the art;
- the cost of implementation;
- 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.

- Data controllers must also conduct DPIAs in respect to high risk Processing.
- You should conduct a DPIA (and discuss your findings with 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);
- Automated Processing including profiling and ADM;
- 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.

Automated Processing (Including Profiling) and Automated Decision-Making (ADM)
Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

- a Data Subject has Explicitly Consented;
- the Processing is authorised by law; or
- the Processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

Direct Marketing
We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner 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.

How do we share, process and retain information?
Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee or agent if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold 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 teams 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 & Care 21's policy on confidentiality.
- if the agency has their own robust policy on data protection and confidentiality which aligns with ours and is GDPR compliant

Before sharing and disclosing personal information, it is important to ensure you seek the consent of individual concerned (if this has not already 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, Head of Department and advice should *always* be sought from the Senior Information Governance Officer.

These circumstances include:

- Where Housing & Care 21 has a statutory duty to disclose information, e.g. tax office, council tax office.
- Where the police are investigating a criminal matter (under the Crime and Disorder Act 1988). 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 & Care 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.

When printing personal data, staff 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. This does not affect staff 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, 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, Soniya, Sonea, Sonje, Sonnjea etc.

All emails that are 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 staff 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.

What if there has been a breach of personal data?
A data breach is when the requirements of the GDPR are not followed. A breach of the GDPR can occur in many ways. For example:
(This list is not exhaustive)

- Theft or accidental loss of personal data
- A deliberate attack on the organisations systems
- The unauthorised use of personal data by a staff member
- Mistakenly sending personal data to an unintended recipient

The GDPR requires Housing and Care 21 to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or the ICO where we are legally required to do so.

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 being the DPO and/or the Information Security Department and follow the Security Incident Event Management Plan. You should preserve all evidence relating to the potential Personal Data Breach.

The penalties for breach the Act can be severe as the ICO (Information Commissioners Office) has regulatory powers to take the following action against organisations:

- The ICO has the power to impose monetary penalties of up to EUR20 Million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is the higher and dependent upon the severity of the data breach

- The ICO may issue an Undertaking or Enforcement Notice requiring an organisation to take remedial action and update procedures and train staff
- The ICO has the power to criminally prosecute organisations and in some circumstances individuals or staff of the organisation.

In the event that personal information has been lost, stolen or otherwise dealt with in contravention of this Privacy Standard this must **immediately** be reported to the Housing & Care 21's Data Protection Officer/Senior Information Governance Officer or in the case of an electronic data breach the IS Service Desk who will inform the Data Protection Officer/ Senior Information Governance Officer. This will allow for the appropriate reporting to the Information Commissioner's Office and appropriate mitigating actions to be carried out.

Data Protection Officer

The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Deirdre LaBassiere, Internal Audit and Risk, 21326, deirdre.labassiere@housingandcare21.co.uk

Please contact the DPO with any questions about the operation of this Privacy Standard or the GDPR or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

- if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by Housing and Care 21);
- if you need to rely on Consent and/or need to capture Explicit Consent;
- if you need to draft Privacy Notices or Fair Processing Notices;
- if you are unsure about the retention period for the Personal Data being Processed;
- if you are unsure about what security or other measures you need to implement to protect Personal Data;
- if there has been a Personal Data Breach;
- if you are unsure on what basis to transfer Personal Data outside the EEA;
- if 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;
- If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;
- If you need help complying with applicable law when carrying out direct marketing activities; or
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

Other related policies, procedures and legislative sources

- Subject Access Request Guidance
- Document Retention Policy and Procedure
- Information Governance and Security Policy and Procedure
- Diversity Policy and Procedure
- Safeguarding Policy and Procedure
- EU General Data Protection Regulations (2016/679)
- 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