DATA PROTECTION POLICY

Version:	REVIEW July 2023
Lead Directorate:	Corporate Services
Approved by:	EMT
Date:	25 August 2023

1 Introduction

1.1 We are committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulations (GDPR) and Data Protection Act 2018.

1.2 As a social landlord we process data to carry out landlord and related functions and ensure the welfare of our residents and communities.

1.3 PCH complies with data protection principles by ensuring Personal Data is:

- processed lawfully, fairly and transparently
- only collected for specified, explicit, and legitimate purposes and not subject to further processing which is incompatible with the original purpose
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- kept for no longer than is necessary
- processed with appropriate security using technical and organisational measures

1.4 This Policy applies to everyone who processes Plymouth Community Homes (PCH) data including staff, Board members, volunteers, involved residents and Data Processors, and applies to PCH and its subsidiary entities.

1.5 Further detailed information on the topics noted within this policy are available on the intranet.

1.6 The policy appendices include a summarised version for staff induction and the website, and a statement on processing special category and criminal data (as required by legislation).

2 Responsibilities

2.1 PCH is the Data Controller of the information that it collects and manages. It is responsible and accountable for compliance with legislation and remains responsible for data when it is processed by other organisations on our behalf (Data Processors).

2.2 PCH has appointed the Head of Governance as its Data Protection Officer; their responsibilities include:

- informing and advising PCH and its employees about data protection requirements
- monitoring compliance with data protection laws and PCH policies, including managing internal data protection activities and ensuring staff are trained
- providing advice on Data Protection Impact Assessments and ensuring the impact assessment performance is monitored
- co-operating with and acting as a point of contact for the ICO

The Head of Customer Experience and Assurance is the Deputy DPO.

2.3 The Governance Team, and in particular the DPO and Governance Officer (Information and Compliance), provide advice and guidance on data protection matters.

2.4 Information Asset Owners (IAO) have been identified for all Personal Data and are noted in the Information Asset Register; they are generally the Head of Service or a nominated senior manager. IAOs are responsible for ensuring data is:

- collected, processed and managed appropriately
- properly protected
- appropriately and fully utilised

2.5 The Strategy, Performance and Insight Team are responsible for overseeing and monitoring maintenance of data accuracy and retention.

2.6 The Digital & IT Team are responsible for the overall prevention and detection of security and/or malicious threats. Their approach ensures we are resistant to security risks/breaches, but due to the ever evolving/changing threat landscape there will always be risks and threats. They are also responsible for ensuring any new system or Digital & IT based project is risk assessed using the Data Protection Impact Assessment.

2.7 Compliance with data protection legislation is the responsibility of everyone who handles Personal Data; they must understand and comply with relevant policies and attend training. New starters undertake training when they join PCH and all staff have training tailored to their role at least every 2 years. When remote/home working, everyone is responsible for ensuring the PCH data protection policies and procedures are followed.

3 Data Categories

3.1 Personal Data

3.2 Personal Data includes any information relating to a living identified or identifiable individual (a Data Subject); this may include:

- name and contact details (including email, telephone numbers and addresses)
- identification information (including age and gender)
- family details (including next of kin and marital status)
- financial information (including income, welfare benefit entitlements and bank details)
- national identifiers (including National Insurance or social security number)
- education and employment details
- online identifiers (including IP address or cookies)
- device identifiers (identifiers for a smartphone)
- photographs, CCTV images, films and telephone recordings
- whistleblowing (confidential reporting) information

3.3 Personal Data includes information held manually (paper or written format) or electronically (emails, information on computer systems, social media, images, voice recordings, WhatsApp, Teams, etc.).

3.4 Personal Data can be related to employees, volunteers, tenants, clients, service users, Board and Committee members, members of the public, contractors, suppliers and more.

3.5 Personal Data can be provided by the Data Subject or a third party, such as health care professionals or the local authority.

3.6 Sensitive and Criminal Offence Data

3.7 Sensitive Data or 'Special Categories of Personal Data' includes:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union membership
- physical or mental health status (past, current or future)
- disability
- sex life or sexual orientation
- genetic data
- biometric data (i.e., DNA, fingerprints and retina scans)

3.8 Data relating to criminal convictions or offences can include (but is not limited to):

- criminal proceedings, allegations (whether proven or unproven) and investigations
- penalties (such as driving points on a Driving Licence), conditions and restrictions placed on individuals

3.9 Although it does not cover information about victims and witnesses of crime, PCH will take particular care when processing this information as it is likely to be sensitive.

4 Lawful Basis for Processing

4.1 In order to process data, we must have a lawful basis, as set out in legislation. The PCH Information Asset Register sets out the lawful basis for processing each type of data.

4.2 Data will only be used for the purpose for which it was originally collected. If a new use is proposed, we assess the potential impact (usually through a Data Protection Impact Assessment) to ensure the proposed purpose is compatible with the original; if appropriate the Data Subject will be advised.

4.3 PCH must have an appropriate policy for processing special category and criminal data (see below and appendices). Personal data processed for these purposes is treated confidentially and maintained by the relevant team on the individual's file, which is secured by role defined access and user specific passwords. It is only shared within PCH on a strict need-to-know basis where the law allows. It may be shared outside of PCH where a lawful reason applies.

4.4 <u>Processing Personal Data</u>

4.5 The lawful bases available for processing Personal Data are:

- **consent** (only to be used when a genuine choice can be offered – see below)
- for the performance of a **contract** or to take steps to enter into a contract
- for compliance with a **legal obligation** (including a court order)
- to protect the **vital interests** of a Data Subject or another person (life or death)
- for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the Data Controller
- in the **legitimate interests** pursued by the Data Controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the Data Subject

4.6 Most of our Personal Data processing relates to 'performance of a contract' (such as a tenancy agreement, support agreement or employment contract).

4.7 There are also instances where it is in PCH's legitimate interests to process data; where this is the case, a Legitimate Interest Assessment is carried out in advance.

4.8 Processing Sensitive (Special Category) Data

4.9 In addition to a lawful basis for processing Personal Data, Sensitive Data requires a further lawful basis; these are:

- **consent** (only to be used when a genuine choice can be offered – see below)
- carrying out obligations under **employment, social security or social protection law**, or a collective agreement
- protect the **vital interests** of a Data Subject or another person (life or death)
- processing by a not-for-profit body with a **political, philosophical, religious or trade union aim** (unlikely to be appropriate for PCH processing activities)
- data is **manifestly made public** by the Data Subject
- establishment, exercise or defence **of legal claims** or where courts are acting in their judicial capacity
- substantial **public interest** (this is a detailed area and includes matters such as **equalities monitoring, fraud, unlawful acts, insurance,** etc)
- **preventative or occupational medicine**, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services or a contract with a health professional
- public interest in the area of **public health**
- **archiving** purposes in the public interest, or scientific and historical research or statistical purposes

4.10 Most of PCH's Sensitive Data processing relates to our 'obligations under social protection law' and 'public interest', with some under 'consent' (see section below). The definition of "social protection" (taken from Art 2(b) of EC Regulation 458/2007) covers the services that housing associations provide: "interventions […] to relieve households and individuals of the burden of a defined set of risks or needs [such as] sickness and/ or healthcare, disability, old age […] housing and social exclusion".

4.11 Processing criminal data

4.12 There are 28 lawful bases available for the processing of criminal offence data; PCH generally uses:

- employment, social security and social protection (as above)
- statutory and government purposes (compliance with the law)
- preventing or detecting unlawful acts
- regulatory requirements relating to unlawful acts and dishonesty
- preventing fraud
- suspicion of terrorist financing or money laundering
- safeguarding of children and individuals at risk
- insurance

4.13 Processing under Consent

4.14 Where we rely on consent, we ensure there is a clear explanation of what the individual is being asked to agree and why. The Data Subject must be able to give consent freely and choose to 'opt-in'. Our Privacy Notice makes it clear consent can be withdrawn and how this can be done.

4.15 We generally use our housing system to record the date consent was given and the mechanism (i.e., written, verbal). Written consent documentation is also saved. We will

consider whether consent is the most appropriate lawful basis and, where appropriate, refresh consent every 4 years.

4.16 Consent guidelines and checklists are available on the intranet.

5 Rights of the Individual

5.1 PCH ensures the following rights of individual Data Subjects are met:

- right to be informed
- right of access (subject access request)
- right to rectification
- right to erasure (or right to be forgotten)
- right to restrict processing
- right to data portability
- right to object
- rights in relation to automated decision-making and profiling

5.2 We provide Data Subjects with information about their individual rights and how these can be exercised in our Privacy Notices (see below).

6 Provision of Privacy Information

6.1 When collecting Personal Data, we provide an appropriate Privacy Notice and aim to use the same medium that we use to collect personal information; this could be:

- orally – face to face or when we speak to someone on the telephone
- in writing – on forms where we are collecting personal information
- through signage – for example, an information poster at Plumer House
- electronically - text messages, websites, emails, apps and other electronic forms

6.2 We take a layered approach, by providing the key privacy information immediately in a statement with more detail available on our website or intranet. This approach is used where there is not enough space to provide full details, such as CCTV signage.

7 Data Security

7.1 PCH is required to ensure “data 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”.

7.2 Staff are responsible for ensuring any Personal Data they hold are kept securely and not disclosed to unauthorised third parties. All Personal Data is accessible only to those who have a legitimate need and passwords are used to access systems and software. There are a range of technical, physical, and organisational security measures at our offices designed to prevent unauthorised access, including access controls and CCTV at Plumer House.

7.3 The Information Security Policy outlines PCH’s approach to data security. The Digital and IT Acceptable Usage Policy outlines ‘acceptable usage’ for various aspects of IT equipment and services, with a focus on the security and protection of systems and data; it includes mobile devices, personal devices and remote working.

7.4 Whilst much of PCH’s Personal Data is held electronically, some data is also held in hard copy. In the interests of confidentiality and security, staff must ensure they clear their desk

of Personal Data at the end of every day. The Information Security Policy contains a section on clear screen and desk management.

7.5 The PCH Business Continuity Policy and Strategy are supported by a range of business continuity plans and a Disaster Recovery (IT Infrastructure) Procedure.

7.6 PCH has the Cyber Essentials Certification which demonstrates our commitment to cyber security and ensures there are technical controls in place to guard against the most common cyber threats.

7.7 Data Protection legislation restricts the processing and transfer of data outside the European Union to third countries or international organisations. Transfer is prohibited unless certain conditions are met; these include:

- the country in which the recipient is based has been the subject of an 'adequacy decision' by the European Commission; this ensures an adequate level of protection
- the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks due to the absence of an adequacy decision
- the transfer is **necessary** for the performance of a contract between the Data Subject and Data Controller

8 Data Accuracy

8.1 In order to comply with the data accuracy principle, PCH:

- encourages good recording keeping and data management
- takes reasonable steps to ensure the accuracy of any Personal Data it obtains
- ensures the source of Personal Data is clear
- carefully considers challenges to the accuracy of information
- considers whether it is necessary to update the information

9 Data Minimisation, Retention and Disposal

9.1 PCH does not collect and retain data 'just in case' it is useful. Personal Data is limited to what is necessary in relation to the purpose/s for which they are processed, and kept in a form which permits identification of Data Subjects for no longer than is necessary.

9.2 The Data Retention, Disposal and Minimisation Policy explains our approach to retention and disposal of data, and includes a Retention Schedule (managed by the Strategy, Policy and Performance team), which details the length of time different data should be retained.

10 Sharing Personal Data

10.1 In order to deliver services effectively, PCH often needs to share data with others, such as partner organisations or contractors. Disclosure of data to a third-party can take the form of:

- systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose (Data Controller to Data Controller, usually with a Data Sharing Agreement in place)
- exceptional, one-off decisions to share data for any of a range of purposes (Data Controller to Data Controller); where these become more regular requests, a Data Sharing Agreement should be set up
- sharing with a Data Processor (a formal Data Processor contract/agreement is required so that PCH, as Data Controller, remains accountable for the data)

10.2 It is good practice to have a Data Sharing Agreement where information is shared with another Data Controller. The agreement should set out a common set of rules to be

adopted by the various organisations involved in a data sharing operation including security measures that must be put in place. A register of Data Sharing Agreements is kept and regularly reviewed to ensure the basis for sharing remains lawful and the third-party is complying with the terms of the agreement

10.3 PCH will only share personal data with our contractors or suppliers if it is satisfied that they have appropriate technical and organisational measures in place. A contract compliant with data protection requirements and setting out their Data Processor responsibilities must be in place prior to Personal Data being provided. Contract management arrangements include a requirement to monitor compliance.

10.4 PCH ensure any data shared is necessary, proportionate and in accordance with a lawful basis, for example:

- as a requirement of law or regulation, i.e.:
  - payroll data shared with HMRC
  - for the prevention, investigation and/or detection of crime, for the apprehension and/or prosecution of offenders (note: there is a DSA with the Police which includes template data request forms)
  - for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)
  - for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights
  - PCH has a duty to co-operate with local authorities implementing their statutory duties around adult and children safeguarding
- with the permission/consent of the individual(s) concerned (i.e. permission from a customer for their MP to raise their issue with us or to provide Personal Data to a third party as part of a Subject Access Request)
- sharing essential information with utility companies, as we have a legitimate interest in making sure that utility charges are directed to those responsible; this is included in our Privacy Notice

10.5 All sharing requests are considered on a case-by-case basis using the guidance available on the intranet and these principles:

- verify the requester (call them back or verify their email)
- check for an existing Data Sharing Agreement and follow it
- understand and justify the purpose(s) of sharing (i.e. lawful basis, as noted above)
- only share what is necessary for the purpose
- provide the information securely (i.e. encrypted email or password protected document)
- the duty to share information can be as important as the duty to safeguard the individual and their confidentiality; consider the safety and well-being of the individual and others who may be affected by their actions
- consider whether it is appropriate/safe to inform the individual that you have shared their information
- if in doubt consult your manager and/or the DPO

10.6 PCH provides privacy information to individuals of how their personal data is shared in our Privacy Notices and at source.

10.7 We do not sell or dispose of for gain, any Personal Data.

11 Monitoring Data Subjects

11.1 PCH recognises that whilst there are a number of benefits to using monitoring equipment, there is a real potential to intrude into an individual's privacy. When considering the use of equipment such as call recording, CCTV, drones with cameras, vehicle tracking devices and noise monitoring equipment, we:

- undertake a Data Protection Impact Assessment
- record it on a register
- review it at least annually to ensure it remains appropriate

11.2 The CCTV Policy provides information about PCH's approach to CCTV in residential areas and is the responsibility of the Head of Neighbourhoods.

11.3 All calls into PCH's 08 numbers are recorded and there is a message at the beginning advising that the call is being recorded. Where a call is transferred from a 08 number to another extension, these calls are also recorded (even if they are transferred multiple times). Calls to direct lines and outgoing calls are not recorded. The retention period for call recordings is 6 months, after which they are permanently deleted unless they are to be specifically kept as part of an ongoing case.

11.4 PCH uses a vehicle tracking system which collects Personal Data that is processed in accordance with the data protection principles. For more information refer to the Vehicle Tracking Policy.

12 Direct Marketing

12.1 Direct Marketing is 'the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals', this definition includes material promoting the aims of not-for-profit organisations.

12.2 The Privacy and Electronic Communications Regulations (PECR) 2003 and subsequent amendments provide rules about sending marketing and advertising by electronic means, such as by telephone, email, text and picture or video message, or by using an automated calling system.

12.3 PCH undertakes some direct marketing for shared ownership and open market sales properties.

12.4 We comply with the PECR by obtaining consent before sending marketing texts, emails or making calls and check if a number is registered with the Telephone Preference Service (see consent section above).

12.5 For clarity, customer satisfaction surveys are not marketing, but we do offer an opt out.

13 Data Breaches

13.1 PCH aims to:

- ensure incidents posing a risk to the rights and freedoms of a Data Subject are notified to the Information Commissioners Office (ICO) within 72 hours of PCH becoming aware
- increase responsiveness - timely reporting enables employees to be open and transparent at an earlier stage, which helps when undertaking investigations
- pre-empt complaints and litigation – PCH can prepare proactively. More detailed information on an incident given to the Data Subject at an early stage may lead to fewer complaints and claims, saving time and resources, and help provide reassurance

- target resources more effectively - reported incidents provide evidence to better target resources; they identify areas for change and improvement
- reduce costs - financial benefits arise from reduced frequency and severity of incidents
- manage reputation – by managing incidents and learning from them

13.2 Everyone is responsible for reporting breaches, potential breaches and near miss data incidents to the DPO, who oversees the investigation process and keeps a Data Breach Register including lessons learnt.

13.3 If an employee is found to be the cause of multiple data breaches, further training and guidance will be provided.

13.4 PCH has a Security Incident/Data Breach Procedure, with a reporting form available on the intranet.

14 Compliance

14.1 PCH recognises the importance and benefits of complying with data protection legislation. We are required to consider the nature, scope, context and purposes of processing as well as the risks to rights of individuals; we implement appropriate technical and organisational measures that ensure that processing is compliant.

14.2 We demonstrate compliance by:

- appointing a DPO with appropriate skills, knowledge and experience
- implementing a range of policies, procedures and guidance
- training staff when they join PCH and then at least every 2 years
- providing opportunities and encouraging staff to report issues and make queries
- using Data Protection Impact Assessments to consider issues and tease out risks and concerns to be addressed
- using peer and professional support
- recording learning and identifying improvements (i.e. via data breaches and near misses)
- documenting our decisions, that are based on good research, discussions with service leaders and IAOs, and professional advice where needed
- PCH and its subsidiaries are registered with the Information Commissioners Office (ICO)
- creating and improving security features on an ongoing basis
- regularly updating the Information Asset Register (including Record Of Processing Activities or ROPA)
- data protection internal audits

15 Policy Monitoring and Review

15.1 This policy is the responsibility of the Head of Governance, who is the Data Protection Officer.

15.2 PCH will monitor this policy to ensure it meets good practice and current legislation and will review it every three years, or more frequently if good practice or regulation changes.

15.3 EMT and the Audit and Risk Committee receive an annual report on data protection, including data breaches, subject access requests and lessons learnt.

Issue	Description of change	Approval	Date of issue	Next review

1	Data Protection Policy 2018, Data Breach Policy and Privacy Policy 2018 updated and merged into a new Data Protection Policy 2023	EMT Aug 2023	Sept 2023	Aug 2026
2				

Appendix A
Summary of Data Protection Policy

(for the website, intranet and staff induction)

This is a summary of the PCH Data Protection Policy, a full version can be found on our website or internet pages.

Who does the Policy apply to?

The Policy applies to everyone who processes PCH data including staff, Board members, volunteers, involved residents and Data Processors, and applies to PCH and its subsidiary entities.

What are the principles of data protection?

PCH must ensure Personal Data is:

- processed lawfully, fairly and transparently
- only collected for specified, explicit, and legitimate purposes and not subject to further processing which is incompatible with the original purpose
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- kept for no longer than is necessary
- processed with appropriate security using technical and organisational measures

What is Personal Data?

As a social landlord, we process Personal Data to carry out landlord and related services, and ensure the welfare of our residents and communities.

Personal Data includes any information relating to a living identified or identifiable individual (a Data Subject):

- name and contact details (including email, telephone numbers and addresses)
- identification information (including age and gender)
- family details (including next of kin and marital status)
- financial information (including income, welfare benefit entitlements and bank details)
- national identifiers (including National Insurance or social security number)
- education and employment details
- online identifiers (including IP address or cookies)
- device identifiers (identifiers for a smartphone)
- photographs, CCTV images, films and telephone recordings
- whistleblowing (confidential reporting) information

We may also process Sensitive Data:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union membership
- physical or mental health status (past, current or future)
- disability
- sex life or sexual orientation
- genetic data
- biometric data (i.e., DNA, fingerprints and retina scans)

Occasionally we may also process data relating to criminal convictions or offences, such as criminal proceedings, allegations and investigations.

When can we process Personal Data?

We must have a lawful reason for processing each type of data.

Most of our processing relates to 'performance of a contract' (such as a tenancy agreement, support agreement or employment contract) and 'social protection law' (which covers the functions of a housing association).

We occasionally use 'consent' to process Personal Data, but we must give a clear explanation of what the individual is being asked to agree and why. The Data Subject must be able to give consent freely and choose to 'opt-in'.

What are the rights of Data Subjects?

Data Subjects have these rights:

- right to be informed
- right of access (subject access request)
- right to rectification
- right to erasure (or right to be forgotten)
- right to restrict processing
- right to data portability
- right to object
- rights in relation to automated decision-making and profiling

We have a set of Privacy Notices available on our website and Intranet that explain what data we collect, how we use it, who we share it with and how Data Subjects can exercise their rights in relation to their data.

Can a Data Subject request a copy of their data?

Anyone can ask an organisation for a copy of the Personal Data that is held about them; this is called a subject access request. These requests are dealt with by the Governance Team and must be responded to within one month.

How do we share data?

We need to share data to deliver services, this includes:

- regular sharing with contractors who are delivering works or services on our behalf – in this case we agree how they will process that data via a contract
- regular sharing with other agencies such as the Police or the local authority in relation to anti-social behaviour data – in this case we must have a legal basis for sharing
- one-off sharing - in this case we must have a legal basis for sharing

Sharing requests are considered on a case-by-case basis using these principles:

- verify the requester (call them back or verify their email)
- check for an existing Data Sharing Agreement and follow it
- understand and justify the purpose(s) of sharing (i.e. lawful basis, as noted above)
- only share what is necessary for the purpose
- provide the information securely (i.e. encrypted email or password protected document)

- the duty to share information can be as important as the duty to safeguard the individual and their confidentiality; consider the safety and well-being of the individual and others who may be affected by their actions
- consider whether it is appropriate/safe to inform the individual that you have shared their information
- if in doubt consult your manager and/or the Governance Team

How do we deal with data breaches?

Everyone is responsible for reporting breaches, potential breaches and near miss data incidents to the Governance Team. Where a breach has occurred, we will apologise and investigate so that we can learn from the incident.

What happens when a new software or system is being introduced?

We must ensure the software or system has appropriate safeguards and is fit for purpose before it is implemented. A Data Protection Impact Assessment (DPIA) is carried out to identify and mitigate any risks, such a data breach or security; this assessment is reviewed by our Digital & IT team and Governance team.

More information:
Data Protection Policy (full version)
Data Protection Officer: governance@plymouthcommunityhomes.co.uk

Appendix B
Special Category and Criminal Data Statement

Background

PCH must have an appropriate policy for processing special category and criminal data; this is covered by the policy above with further information in this appendix.

Personal data processed for these purposes is treated confidentially and maintained by the relevant team on the individual's file, which is secured by role defined access and user specific passwords. It is only shared within PCH on a strict need-to-know basis where the law allows. It may be shared outside of PCH where a lawful reason applies.

PCH processes special category and criminal data in reliance of the following conditions from Schedule 1 DPA 2018.

1. Employment, social security and social protection

PCH may process special category and criminal data, including criminal convictions, criminal offences or related security measures in reliance of this condition.

1.1. Employment

PCH processes data about prospective, current and previous employees and Board members for employment purposes, including data about health and criminal convictions and associated proceedings.

Personal Data processed for employment purposes is maintained by HR as part of applicant and employee personal files. In the event of employees being seconded under contract to another organisation, or a secondee carrying out work for PCH, PCH and the other organisation may share Personal Data in reliance on this condition, as set out in the applicable contract.

Any information about criminal convictions obtained as part of a Disclosure and Barring Service (DBS) check is stored and retained in line with DBS requirements.

1.2. Social Protection

PCH processes data about applicants, tenants, members of the public and residents necessary for performing or exercising obligations or rights imposed or conferred by Social Protection law.

Social Protection includes "all interventions from public or private bodies intended to relieve households and individuals of the burden of a defined set of risks or needs" arising from "sickness and/or health care; disability; old age; survivorship; family/children; unemployment; housing; and social exclusion" EUR-Lex - 32007R0458 - EN - EUR-Lex (europa.eu).

We may rely on this condition in circumstances such as:

- managing tenancies
- ensuring appropriate support packages are in place
- anti-social behaviour case management (in particular health, criminal convictions and data relating to hate crimes and harassment)
- work with individuals/families in relation to social exclusion and family support
- the provision of welfare and benefits advice

Examples of how we may share this data (where there is a legal basis to do so) include repairs/maintenance contractors, support agencies and the Police.

2. Research

PCH may process special category and criminal data to undertake or to procure another organisation to undertake, research on its behalf.

Such research will be undertaken with the consent of the individuals involved and subject to appropriate safeguards for the rights and freedoms of the data subject (article 89 GDPR). Those safeguards must ensure appropriate technical and organisational measures are in place to ensure respect for the principle of data minimisation.

Where practical the data will be anonymised[1]. Where this is not practical, PCH will consider pseudonymisation[2] and ensure appropriate security is in place, including for the transfer of data to another organisation. A Data Sharing Agreement will also be put in place.

3. Substantial Public Interest

DPA 2018 Schedule 1 part 2 specifies the conditions for processing personal data necessary for the performance of a task carried out in the public interest. Schedule 1 part 3 para 36 permits the processing of criminal data which meets one of these conditions:

3.1. Equality of opportunity or treatment (para 8)

PCH recognises the importance of equality, diversity and inclusion, and monitors and reviews the existence or absence of data across all areas so we can fulfil our duties under the Equality Act 2010.

Any processing of specified categories of personal data used for these purposes[3] is carried out confidentially and securely.

Data collected is not used to make decisions about the Data Subject; where such data is required for decision-making a different condition for processing will be identified.

Data collected as part of an application form[4] is stored separately from the application data and pseudonymised.

3.2. Racial and ethnic diversity at senior levels of organisations (para 9)

PCH collects and monitors racial and ethnic diversity data in relation to Board membership and senior management roles.

Data collected is not used to make decisions about the Data Subject; where such data is required for decision-making a different condition for processing will be identified.

[1] In order to be anonymised under GDPR, the personal data must be stripped of sufficient elements that the individual can no longer be identified.

[2] 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

[3] Racial or ethnic origin, religious or philosophical beliefs, health, sexual orientation

[4] For example, applications for jobs, board membership or properties

3.3. Preventing or detecting unlawful acts (para 10)

PCH may rely on this condition to process data about applicant, tenant, Board member and staff criminal convictions, in certain circumstances, to enable us to manage any potential risks to PCH, and its staff and residents.

We rely on this condition to disclose certain items of Personal Data to the Police, DWP or other similar bodies for the prevention and detection of unlawful acts, such as fraud. Data disclosed under these circumstances is shared securely and only the minimum amount of information necessary is shared.

We rely on this condition when carrying out initial investigations into concerns that one or more individuals are being drawn into terrorism, or making initial reports or requests for advice to the Police. Any personal data processed for these purposes is processed sensitively and confidentially on a strict need-to-know basis.

We may also rely on this condition to process information about employees' criminal convictions, if appropriate. Any information about criminal convictions obtained as part of a Disclosure and Barring Service (DBS) check is stored and retained in line with DBS requirements.

3.4. Regulatory requirements relating to unlawful acts and dishonesty etc. (para 12)

PCH may rely on this condition if/when it processes criminal conviction data about its Board members and some senior employees to ensure they are fit and proper persons to fulfil the role.

Such data is shared securely with regulators such as HMRC, Companies House, Financial Conduct Authority and Regulator for Social Housing.

3.5. Safeguarding of children and of individuals at risk (para 18)

Many PCH residents are under 18, either as family living with tenants or as young tenants. Some of our residents are vulnerable and potentially at risk.

We may rely on processing special category data without the consent of the individual under this ground in certain circumstances, where we are:

- protecting an individual from neglect or physical, mental or emotional harm; or
- protecting the physical, mental or emotional well-being of an individual

where it is necessary for reasons of substantial public interest to do so, and where consent either cannot be given, it is unreasonable for us to obtain consent, or if obtaining consent would prejudice the provision of the protection.

This condition is most likely to be relied upon where we are working with in partnership with relevant statutory agencies as part of a multi-agency approach and may be securely shared with named individuals in statutory agencies.

Nothing in this policy will prevent the sharing of data with a statutory organisation if concerns are identified about the safety or significant wellbeing of an individual.

3.6. Disclosure to elected representatives (para 24)

PCH may rely on this condition to respond to Councillor and MP casework enquiries, where the enquiry is in response to a request from an individual. We can only use this condition to process personal information that is relevant to the subject matter of that communication, and which is necessary in order to answer that enquiry.

Where the request to the Councillor/MP comes from an individual other than the Data Subject, we can only use this condition to disclose the Data Subject's data without their consent if:

- consent cannot be given by the Data Subject
- the Councillor/MP cannot reasonably be expected to obtain the consent of the Data Subject
- obtaining the consent of the Data Subject would prejudice the action taken by the Councillor/MP
- the processing is necessary in the interests of another individual and the Data Subject has withheld consent unreasonably

Responses to casework enquiries are held securely on the Pentana IT system and access is restricted by role. Where responses contain sensitive information, they are sent via a secure email link or through a similarly secure method.

4. Consent

PCH will use consent to process data where other conditions (such as Social Protection or substantial public interest) do not apply.

Where PCH is involved in a special project or partnership (such as the current Livewell health partnership) we will ask for consent to collect special category or criminal data and ask consent for sharing that data.

5. Processing criminal conviction and offences or related security measures data

In addition to the above conditions, and in common with other special category data, PCH may also rely on one of the following conditions to process criminal convictions and offences or related security measures (as set out in paras 29–33 DPA Act 2018):

- explicit consent
- protecting the individual's vital interests in relation to the processing of criminal data
- criminal data made manifestly public by the data subject
- legal claims

We may use any or all of the above to process data in connection with the management of a tenancy. This data is kept securely with access restricted to specific roles within PCH. It will only be shared with another organisation where there is a legal basis for doing so, and where there is an information sharing agreement in place which specifies how the data can be used.

Where the data is used in the context of the Risk Alert system, to protect PCH staff and contractors from potential harm, a flag system is used advising of the required action (e.g. visit in pairs) without providing data as to the reason for the flag.