Title	**Data Protection Policy**
Purpose	The aim of this policy is to ensure Maryhill Housing complies with the UK General Data Protection Regulations (GDPR) and fully understands its obligations under these regulations.
Scope	This policy is applicable to all Maryhill Housing staff as everyone is involved in processing personal data belonging either to our customers or staff. Compliance with this policy is a condition of employment and any deliberate breach of the policy may result in disciplinary action, which for serious or deliberate breaches may include dismissal. Knowingly breaching the provisions of the GDPR may also lead to legal action being taken against the organisation and individuals. Maryhill Housing's Data Protection Officer is the Performance & Governance Manager. Maryhill Housing is registered with the Information Commissioner as a Data Controller and our registration number is Z5989470. Any contractors completing work for Maryhill Housing will be briefed on the importance of data protection at the outset, for example as it relates to safeguarding sensitive personal information on a customer. Data Sharing Agreements have been developed for this purpose and will be issued to all key contractors along with the contract agreement.
Definitions	**Principles of Data Protection** There are six Principles of Data Protection contained in the GDPR that can be referred to by anyone who has a role to play in the management of personal information in Maryhill Housing. These are summarised below: • Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. • Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. • Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. • Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay. • Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the

	appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals. • Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. **Data Controller** – a person or organisation who decides how personal data is to be processed and for what purpose. Maryhill Housing is the data controller, not individual employees. **Data Processor** – an organisation or person who processes personal data for and on behalf of a controller. **Data Subject** – data subject means an individual (not an organisation), who is the subject of personal data such as a customer, staff member or Board member. **Personal Data** – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; **Special Categories of Personal Data** – include the following: • Racial or ethnic origin; • Political opinions; • Religious or philosophical beliefs; • Trade union membership; • Genetic data; • Biometric data for the purpose of uniquely identifying a natural person; Mental or physical health; • Data concerning health or data concerning an individual's sex life or sexual orientation. **Processing** – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Policy Statement	Processing of personal data will be carried out in line with our Privacy Policy where the data subject has given positive consent or there is a statutory requirement for that data to be given. A copy of the Privacy Policy will be provided to all customers/applicants when they become involved with Maryhill Housing, and will be available publicly on our website. Staff/applicants will be provided with the equivalent Employee Privacy Notice.

The request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

Details of the reasons why data is sought and the reasons for which it will be used will be stated on relevant Maryhill Housing forms as appropriate.

The processing of special categories of personal data will only be carried out with the individual's explicit consent.

Where personal information is held by Maryhill Housing on customers, applicants, staff members and other individuals, these people have the right to access the information, unless it is exempt under the General Data Protection Regulations. A Subject Access Request form and Right of Access Procedure is in place for this purpose.

Maryhill Housing will periodically test compliance with this policy to ensure that all managers and staff are following our Data Protection requirements. These checks will be carried out by our Internal Auditors as part of our three-year Internal Audit Plan, or internally by the Data Protection Officer.

Training

Training and guidance on what is expected in relation to Data Protection can be provided by the Data Protection Officer at any time should it be needed. This can include:

- New staff – Awareness e-learning will be provided at induction and copies of relevant policies shared for sign off.
- Existing staff – Ongoing refresher training will be provided via e-learning and in-person sessions as appropriate.
- Board members – copy of this policy made available along with the Privacy Policy, with training sessions provided as appropriate.

Security of Data

All staff members are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third party.

All personal data should be accessible only to those who need to use it. All personal data must be kept in a lockable room with controlled access, or in a locked drawer or filing cabinet.

If data is electronic then it should be stored on the F drive and not on local systems and have suitable security access levels applied, determined and monitored by the ICT team.

Particular care should be taken of portable IT equipment, memory sticks etc which should be password protected to prevent unauthorised access. Where highly sensitive data is by necessity stored on memory sticks, these must be encrypted. Special categories of personal data should not be kept on memory sticks or routinely taken from Maryhill Housing premises on any form of removable media.

Care should be taken to ensure that PC and mobile device screens are not visible except to authorised staff and that computer passwords are kept confidential. PCs, mobile phones, laptops and other mobile devices should not be left unattended without password protected screen savers and manual records should not be left where they can be accessed by unauthorised personnel. No personal information of customers or staff should be displayed on notice boards within offices.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be disposed of as "confidential waste". All disposal of IT equipment and electronic files will be managed by the ICT team as set out in the relevant ICT policies and procedures.

This policy also applies to staff who process personal data outside Maryhill Housing premises, such as when working from home. Off-site processing presents a potentially greater risk of loss, theft, damage to personal data. Staff should take particular care when processing personal data at home or in other locations. Any loss of data from either offices or off site must be reported to the Data Protection Officer immediately. A Data Breach Procedure is in place for this purpose.

Retention & Disposal

Maryhill Housing discourages the retention of personal data for any longer than necessary. Considerable amounts of data are collected, and some data will be kept for longer periods than others, however every effort should be made to review the need to keep it and safely dispose of data as soon as possible. A separate Retention Schedule is in place for this purpose.

Personal data will be disposed of in a way that protects the rights and privacy of data subjects (e.g. disposal as confidential waste, deletion from IT systems and backups).

CCTV

Under the GDPR images captured through CCTV are classed as personal data.

Where CCTV is in use, images will be treated as "data" in the same manner as paper or computer-based information. The main purpose of collecting data from CCTV cameras is the protection of Maryhill Housing customers, staff members and the public, the prevention of crime or anti-social behaviour and to safeguard property. Data from CCTV cameras may be used as evidence during criminal or other legal proceedings and may be passed to other agencies within the scope of our Registration with the Information Commissioner.

CCTV signage will be in place where CCTV is present. The sign should detail the purpose of using CCTV, who is responsible for operating the system, and who to contact (usually a telephone number) in the event of an enquiry.

	Access to CCTV systems will be restricted to ensure the maximum privacy for that personal data. The CCTV monitor should not be in a position where images can be seen by members of the public. If a meeting is being conducted in an office where CCTV is monitored, the CCTV monitor should be switched off if there is a risk that unauthorised people would be able to view images on screen. Images will be recorded on a time loop. This means that recorded images are not kept indefinitely. The length of time images are stored before being overwritten should be known to the staff members responsible for monitoring the system in order to respond to enquiries from customers. Recorded images will be kept securely and staff should not access these without the permission of their manager and only for specific purposes related to the use of CCTV, i.e. crime prevention/detection or dealing with anti-social behaviour. **Data Protection Impact Assessments** A Data Protection Impact Assessment (DPIA) must be carried out for any project or policy change that involves the processing of personal data which is likely to result in a high risk. This means that although you have not yet assessed the actual level of risk you need to screen for factors that point to the potential for a widespread or serious impact on individuals. A Data Protection Impact Assessment template form is in place for this purpose.
Approval	Board – 24th June 2021
Policy Owner	Data Protection Officer (Performance & Governance Manager)
Review	June 2024