DATA PROTECTION POLICY

Adopted:	Adopted October 2019	Last Reviewed:	October 2019
Next Review Due:	October 2022		

The lawful and appropriate management of personal data is extremely important to OTHA.

This policy sets our commitment to protecting personal data and how we will implement this with regards to the collection and handling of personal data as defined in the following legislation:

- General Data Protection Regulations (EU) 2016/679 (GDPR)
- UK Data Protection Act 2018 (DPA2018)
- Privacy and Electronic Communications Regulations (PECR)
- Any legislation that will replace the GDPR in UK law after leaving the European Union.

Failure to comply with data protection legislation could lead to financial penalties, regulatory action, as well as reputational damage.

Scope

The Policy applies to all personal data that OTHA holds relating to living identifiable individuals regardless of the category of data or the format of the data. Personal data is any data which could be used to identify a living individual e.g. name, address, email, postcode, CCTV image, and photograph. Special categories of personal data is any information about racial or ethnic origin, political opinions, religious beliefs, health (mental and physical), sexual health, trade union membership and criminal convictions.

The policy applies to personal data held or accessed on OTHA premises or accessed remotely via home or mobile working. Personal data stored on personal and removable devices are also covered by this policy.

This policy applies to:

- All Staff, including temporary staff
- All Governing Body Members

The Data Protection Principles

Data protection laws describe how organisations must collect, handle and store all personal data. Ensuring compliance is underpinned by the following principles.

Personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;

- 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;

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition to these principles the law requires organisations to be responsible for, and must be able to demonstrate, compliance with the above principles.

Responsibilities for Compliance

OTHA's voluntary Governing Body Members are ultimately responsible for ensuring that OTHA meets its legal obligations, however the day to day management is delegated to the Senior Management Team.

All staff have a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in line with this policy and the data protection principles.

Data Protection Lead Officer (Depute CEO) is responsible for monitoring compliance with this policy and the data protection legislation; managing personal data breaches and data subject rights; recording and maintaining appropriate records of processing activities and the documented evidence required for compliance.

Compliance

OTHA will comply with our legal obligations and the data protection principles by:

Processing Lawfully and Fairly
OTHA will ensure processing of personal data, and special categories, meets the legal basis as outlined in legislation. Individuals will be advised on reasons for processing via a freely available Privacy Notice.

Where data subjects' consent is required to process personal data, consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the process for Data Subjects to withdraw consent will be simple.

Purposes
Personal data will only be used for the original purpose it was collected for. These purposes will be clear to the data subject.

If OTHA wish to use personal data for a different purpose, we will notify the data subject prior to processing.

Adequate and Relevant data
OTHA will only collect the minimum personal data required for the purpose. Any personal data discovered as excessive or no longer required for the purposes collected for will be securely deleted.

Any personal information that is optional for individuals to provide will be clearly marked as optional on any forms.

Accurate
OTHA will take reasonable steps to keep personal data up to date, where relevant, to ensure accuracy.

Any personal data found to be inaccurate will be updated promptly. Any inaccurate personal data that has been shared with third parties will also be updated.

Retention
OTHA will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data are outlined in the Records Retention Schedule.

Data will be disposed of in a responsible way to ensure confidentiality and security.

Security
OTHA will implement appropriate security measures to protect personal data.
Personal data will only be accessible to those authorised to access personal data on a 'need to know' basis.

Employees will keep all data secure, by taking sensible precautions and following the relevant OTHA policies and procedures relating to data protection.

Data Sharing

In certain circumstances OTHA may share personal data with third parties. This may be part of a regular exchange of data, one-off disclosures, or in unexpected or emergency situations.

Appropriate security measures will be used when sharing any personal data.

Where data is shared regularly a contract or data sharing agreement will be in place to establish what data will be shared and the agreed purpose.

OTHA will consider all the legal implications of sharing personal data prior to doing so.

Data Subjects will be advised of any data sharing in the Privacy Notice.

Data Processors

Where OTHA engage Data Processors to process personal data on our behalf, we will ensure:

- Data processors have appropriate technical security measures in place
- No sub-processors are used without prior written consent from OTHA
- An appropriate contract or agreement is in place explaining the full requirements of the data processor.

Security Incident & Breach Management

Occasionally OTHA may experience a personal data breach; this could be if personal data is:

- Lost, for example via misplacing documents or equipment that contain personal data, through human error, or via fire, flood or other damage to premises where data is stored
- Stolen; theft or a result of a targeted attack on our network (cyber-attack)
- Accidently disclosed to an unauthorised individual
- Inappropriately accessed or used

All security incidents or personal data breaches will be reported and managed by the Data Protection Lead Officer in consultation with the Data Protection Officer (DPO), Lesley Selbie of RGDP.

The Information Commissioner's Office and the individuals affected will be notified promptly, if required.

All breaches will be managed under OTHA's Breach Management Procedures.

Individual Rights

OTHA will uphold the rights of data subjects to access and retain control over their personal data held by us.

OTHA will comply with individuals':

- **Right to be Informed** – by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.
- **Right to Access** – by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.
- **Right to Rectification** – by correcting personal data that is found to be inaccurate. We will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies with be rectified without undue delay.
- **Right to Erasure** (also known as 'the right to be forgotten') - we will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.
- **Rights to Restrict Processing** - we will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right.
- **Right to Data Portability** – by allowing, where possible, data to be transferred to similar organisation in a machine-readable format.
- **Right to Object** – by stopping processing personal data, unless we can demonstrate legitimate grounds for the processing, which override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defence of legal claims.

Privacy by Design

We have an obligation to implement technical and organisational measures to demonstrate that we have considered and integrated data protection into our processing activities throughout the organisation.

When introducing any new type of processing, particularly using new technologies, we will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and carry out Data Protection Impact Assessment.

All new policies including the processing of personal data will be reviewed by the Data Protection Lead Officer, in consultation with the DPO, to ensure compliance with the law and establish if a Data Protection Impact Assessment is required.

Advice will be provided by the Data Protection Lead Officer on conducting Data Protection Impact Assessments in line with OTHA's Data Protection Impact Assessment Procedure.

Training

All staff will be aware of good practice in data protection and where to find guidance and support for data protection issues.

Adequate and role specific training will be provided regularly to everyone who has access to personal data, to ensure they understand their responsibilities when handling data.

Breach of Policy

Any breaches of this policy, may be considered under the OTHA disciplinary procedures, and may result in disciplinary action being taken, including dismissal.

Monitoring and Reporting

Annual audits will be undertaken to check compliance with the law, this policy and any relevant procedures.

An annual report will be presented to the Governing Body at the start of each financial year.

Related Policies & Procedures

The following policies and procedures should be read with this policy:

- Information Security Policy
- Subject Access Request Procedures
- Breach Management Procedures
- CCTV Policy & Procedures
- Data Privacy Impact Assessment Procedures

Policy Review

This policy will be reviewed at least every three years, although changes will be made to the policy during the three-year period if required to meet changes in legislation and to address any weakness identified in the policy.

Appendices

Privacy Notice – Customers
Retention Schedule