



Data Protection Policy

Governance



Document Title	Data Protection Policy
Version number	
Version date	September 2026
Author Title & Issuing Department	Data Protection Officer Governance, Risk and Assurance
Target Audience	All Colleagues across emh Group, all subsidiaries of emh and all associated operating businesses

Approved By	Group Board
Date Approved	September 2026
Review Date	September 2029

Links to Regulatory Standards – Economic/ Consumer Standards	Governance & Financial Viability 1.1 Governance ▶ Adhere to all relevant law ▶ Comply with their governing documents and all regulatory requirements
Outcomes for Customers	▶ Assurance that data is processed within the UK GDPR requirements
How were tenants, residents and service users involved in the review/development of this document	This is a legal requirement; therefore, residents and service users have not been involved in the review/development of this document
Training Provision	Awareness to be raised across the business through InBrief, mandatory training and Leaders Forum
Links to the Business Plan	▶ Resilience
Links to Key Values	This Policy recognises all the Values of emh group. ▶ Integrity: The Policy seeks to ensure that everyone understands their rights and responsibilities under the Data Protection Act 2018. ▶ Diversity: The Policy sets out the data that will be held under the Equality Act 2010 ▶ Openness: The Policy sets out how personal information will be used and kept. It also sets out how individuals can access that information. ▶ Accountability: The Policy sets out who is responsible overall for the personal data referred to in the Policy



- Clarity: The Policy makes it clear, how data is used, shared and updated.
- Excellence: In applying this Policy, the group seeks to provide an excellent data protection service for all individuals.

Version Control

Version	Revision Date	Author: Job Title	Change Description
1	October 2012	Data Protection	Approved by EMT 24 January 2013
2	April 2017	Data Protection	Terminology and Housekeeping update
3	July 2017	Data Protection	Support contacts added
4	September 2018	Data Protection	New legislation updates to comply with GDPR and DPA 2018
5	December 2019	Data Protection	Major overhaul to reflect learning 18 months after the implementation of GDPR and DPA 2018
6	May 2020	Data Protection	Updated following internal data protection audit
7	June 2021	Data Protection	Updated to include reference to Data Protection Impact Assessment (following DSPT Submission)
8	March 2024	Data Protection	Three-Year Review, Major overhaul with several additions
9	September 2026	Data Protection Officer	Review and updates to reflect the amendments to data protection legislation under the Data (Use and Access) Act 2025



1. Introduction

Emh process personal and special categories of personal information about many individuals. This includes, tenants, customers, clients, service users, applicants, and prospective customers, employees, board members. Emh process this data to carry out its business and provide the services to the public and organisations it supports.

All individuals have a legal right to have their privacy respected, and these are inscribed in:

- ▶ the UK General Data Protection Regulation (UK GDPR)
- ▶ the Data Protection Act 2018 (DPA 2018);
- ▶ the Privacy and Electronic Communications Regulations 2003 (PECR)

These laws give a framework to ensure that personal data is processed in a legal, fair and transparent manner and that it is handled securely.

The aim of this policy is to inform emh group its subsidiaries and its employees, of their responsibilities under UK data protection legislation and how to comply with them.

The policy is concerned with the collection, storage, processing, sharing, destruction and/or security of personal information held and managed by emh, whether in electronic or physical format.

This policy applies to all colleagues (including temporary, casual or agency), contractors, consultants, suppliers and data processors working for, or on behalf of the group and it should be applied by the above in relation to our tenants, residents and service users.

This policy in particular relates to customer information, but the principles and requirements apply equally to employees, contractors and suppliers. There is a separate People Team Data Protection Policy which applies to employees and the processing of their data.

2. Definitions and Scope

The scope of this policy covers emh group; emh homes; emh care and support & midlands rural housing who are known throughout this policy as 'the group'. It also applies to any data relating to the functions of the emh treasury plc and emh development company limited.

This policy applies to all data held in relation to living, personally identifiable individuals and information processing, including collection, storage and destruction, for data held in both physical formats (i.e. paper, USB drives, etc) and digital (electronic) formats (i.e. on computers/servers, mobile devices etc.)

This policy does not relate to information about deceased individuals. However, an air of confidentiality would be appropriate when disclosure of a deceased person's personal data is requested. When disclosing information pertaining to a deceased individual, proof of death should be sought, e.g. a death certificate, and secure identification of the requesting individual (and proof of a legal right to have access to the deceased's personal data, for

example, proof that the individual is the administrator or executor of the estate of the deceased or the deceased's next of kin) should be put in place to avoid any claims that the group has breached a duty of confidence owed to the next of kin or administrator/executor of the estate. This is also relevant to minimise a risk of theft from the estate of the deceased person.

3. Specifics of the Policy

Key Definitions

Personal Data - This is any piece of information that can be used to identify a living human being, this includes any information that can identify a person directly or indirectly. They are often referred to as 'Personal Identifiers' because this is information that can lead to a person being identified.

Examples include, but are not limited to: name, address, email address, phone number, identification number, location data or online identifiers such as IP addresses

Privacy Notices – These are notices setting out information that may be provided to individuals when the group collects information about them.

Processing or process – means any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Sensitive Personal Data – Sometimes referred to as “special category personal data”, This is personal data includes information relating to an individual's race, ethnic origin, political affiliations, religious beliefs, trade union membership, genetics, biometrics (where used for ID purposes), health data, information about a person's sex life and or their sexual orientation.

General Data Protection Regulation (UK) mentioned throughout the document as the UK GDPR is the transposed and amended UK version of the EU's General Data Protection Regulation which sets out the overarching Data Protection Framework applicable in the UK or on organisations that process personal data relating to a UK resident in most situations outside the UK. It also regulates the transfer of personal data outside the UK and EEA areas.



Data Protection Act 2018 mentioned throughout this policy as the DPA 2018 is a United Kingdom Act of Parliament which amends and builds on the UK GDPR. It is a national law which includes and builds on the UK GDPR and replaces the Data Protection Act 1998. Relevant amendments to the DPA 2018 were introduced by the Data (Use and Access) Act 2025 (DUAA 2025).

Privacy and Electronic Communications Regulations 2003 mentioned throughout this document as PECR sit alongside the DPA 2018 and the UK GDPR. They give specific privacy rights in relation to electronic communications, marketing and electronic cookies.

Personal Data Breach or Data Breach means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

Legal Framework

The UK GDPR places a duty on all organisations to maintain a central register of personal data breaches; and report personal data breaches that are likely to pose a high risk to data subjects to the relevant supervisory authority.

Our supervisory body is the Information Commissioner's Office (ICO). We must report personal data breaches that are likely to pose a high risk to an individual's rights and freedoms, within 72 hours of becoming reasonable aware of the breach. Not all data breaches are notifiable, and advice must be sought from the Data Protection Team in any event.

If you know or suspect that a data breach occurred has occurred, you must report this to the Data Protection Team in accordance with our Personal Data Breach Policy.

If the breach is likely to adversely affect an individual's rights and freedoms after any mitigations implemented by us have been taken into account, we may also be required to inform those individuals without undue delay, unless there are justifiable reasons not to do so. We have introduced a robust breach detection, investigation and internal reporting procedure; this is known throughout the group as the Breach Toolkit. This will facilitate our decision-making about whether or not we need to notify the ICO and the affected individuals.

The DPA 2018 is the UK's domestic law which implements further data protection provisions alongside those already in the UK GDPR. PECR sit alongside the DPA 2018 and the GDPR. It sets out legal regulatory frameworks to ensure that organisations respect individual's privacy when they pertaining to

- ✓ marketing calls, emails, texts and faxes;
- ✓ cookies (and similar technologies);
- ✓ keeping communications services secure; and
- ✓ customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.



Data protection laws apply to both information processed within an automated system and manual filing systems where personal information is accessible. This could include a chronologically ordered set of manual records containing personal information.

Information that has been pseudonymised is still classed as personal data. However, provided that the key to reverse the pseudonymisation process is still secure, the likelihood is that any unauthorised access to pseudonymised data without the key would not pose a high risk to the rights and freedoms of individuals and thus would not need to be reported to the ICO. However, it would still need to be reported to the Data Protection Team.

Data Protection Impact Assessment

emh adopts a risk-based approach to processing personal data ensuring that it assesses any risks to privacy or to the rights and freedoms of people before commencing or commissioning or changing data processing activities. We shall as a minimum, ensure that a Data Protection Impact Assessment screening is undertaken where required by Data Protection Legislation and/or when one is deemed to be desirable by the Data Protection Team.

emh will maintain a procedure setting out how Data Protection Impact Assessments (DPIAs) are to be carried out and documented and ensure that appropriate resources are available to advise on DPIAs.

The Data Protection Team is responsible for maintaining a register of Data Protection Impact Assessments that have been undertaken by the organisation, and for its periodic review.

Emh uses a screening check list in the first instance to determine where a DPIA is required and relevant colleagues have been trained on how to carry out a DPIA. We provide guidance so that our colleagues understand the need to consider a DPIA to facilitate this. Please see the DPIA policy for more information.

The Data Protection Principles

The UK GDPR outlines six data protection principles that organisations need to follow when collecting, processing and storing individual's personal information. The group is responsible for complying with the principles and must be able to demonstrate the organisation's compliance practices.

The first principle is **lawfulness, fairness and transparency**. The group needs to ensure their data collection practice is lawful. To remain lawful, we need to have a thorough understanding of the GDPR and its rules for data collection. We need to have a lawful basis for processing personal data under Article 6 (personal data) and Sensitive Personal Data under both Articles 6 and 9 (Special Category Personal Data).



To ensure that we do not unlawfully or unfairly process personal data you should familiarise yourself with the group's privacy notices which describes the type of information we collect and why we collect it. If you are unsure whether any processing activity is inconsistent with the applicable privacy notice, please contact the Data Protection Team for assistance. Colleagues should also encourage data subjects to read their applicable privacy notice.

The second principle is **purpose limitation**. The group should be clear as to why we are collecting the personal data and what we intend to do with it. The group should only collect personal information for a specific business purpose and these purposes should be clearly documented within the Record of Processing Activities. Information collected cannot be used for a new purpose unless it is compatible with the original purpose(s) we have obtained consent or we have a clear obligation or function that is set out in law, and the group should only collect information for as long as necessary to complete that purpose.

The third principle is **data minimisation**. The group must only process the personal information that is needed to achieve its processing objectives. The information must be adequate, relevant and limited to what is necessary in relation to the purposes. Data Minimisation can ensure that in the event of a breach the unauthorised individual will only have access to a limited amount of information. Additionally, data minimisation makes it easier to keep information accurate and up to date, as well as reducing the costs to the Group incurs in collecting personal data the group does not actually need.

The fourth principle is **Accuracy**. The accuracy of personal information is integral to data protection, as incomplete or inaccurate information may lead to erroneous decisions being made. The group must take every reasonable step to rectify or complete information that is inaccurate or incomplete. Individuals have the right to request that inaccurate or incomplete information be erased or rectified without undue delay and at most, within one calendar month. The group's Data Subject Rights Procedure should be reviewed if any individual wishes to exercise their right of rectification or their right of eraser.

The fifth principle is **Storage Limitation**. The group needs to delete personal information when it's no longer needed, either for our own purposes or to comply with, or evidence our compliance with a legal obligation we are subject to. or no longer retainable by law. The group's Retention Policy sets out how long we should keep information. All information stored by the group should be retained in accordance with our Retention Policy. Any colleagues that are uncertain how long information should be kept should consult one of the responsible officers listed in section 1.7 of this document. It is the responsibility of the Data Owning team's manager to ensure this is upheld and carried out on a regular basis.

The sixth principle is **integrity and confidentiality**. This principle is also known as the 'Security Principle'. Personal information must be processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The group should encrypt personal information held in an electronic format wherever possible, using suitable measures, as well as ensuring the security of devices used to process that personal data. Additionally,



staff are responsible for ensuring that, when working away from the office, all personal data is kept secure, and that any calls or discussions where personal data may be discussed cannot be overheard, either by people or by smart devices with microphones.

Additional to the six principles we must evidence **Accountability**. The group is required to take responsibility for what we do with personal data and be able to show how we are complying with the 6 data protection principles, including maintaining records.

Data Subject Rights

In addition to the compliance with the Data Protection Principles the group will also comply with the eight individual Data Protection Rights of any person whose information is collected, processed and stored within any of the group's systems. In summary these include the right to:

- ▶ be informed about how their information is being used
- ▶ access to their personal information
- ▶ to have their information correct and up to date
- ▶ to their information erased when it is necessary
- ▶ to stop or restrict the processing of their information when it is necessary
- ▶ to get and reuse their information for different services
- ▶ to object to how their information is processed in certain circumstances
- ▶ to have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects them.

These Data Subject Rights are not absolute, please send all requests with regards to exercise a right to the Data Protection Team for action. Requests can be made verbally. If this is the case, please take details of not just the name of the requestor and the information they have requested, but also their contact details

Should you require any support or guidance in relation to data protection, including guidance on responding to a subject access request please speak to your manager in the first instance. There is a separate Subject Access Request policy.

The Data Subject Rights Policy ensures that the group complies with its legal obligations in respect of data subject rights under the relevant data protection legislation. The procedure is governed by our Data Subject Rights Policy. In the event of a conflict between the procedure and this policy this policy will take precedence.



Processing of Personal Data

The group is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

- ▶ Processing with the prior consent of the data subject
- ▶ Processing is necessary for the performance of a contract between the group and the data subject or is necessary to take steps (at the request of the data subject); prior to entering into a contract with them;
- ▶ Processing is necessary for the group's compliance with a legal obligation;
- ▶ Processing is necessary to protect the vital interests of the data subject or another person;
- ▶ Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the group official authority; or
- ▶ Processing is necessary for the purposes of the group's legitimate interests or the legitimate interests of a third party, provided that such processing does not override the individual rights and freedoms of the data subject.

Processing of Special Category Personal Data or Sensitive Personal Data

In the event that the group processes Special Category Personal Data or Sensitive Personal Data, the group must do so in accordance with one of the following grounds of processing, in addition to one or more grounds set out in 4.1 above:

- (a) Explicit consent
- (b) Is necessary for carrying out our Employment, social security and/or social protection obligations (if authorised by law)
- (c) is necessary to protect the Vital interests of a person where the data subject is physically or legally unable to give their consent;
- (d) of personal data that was manifestly made public by the data subject
- (e) is necessary to exercise, establish or defend Legal claims
- (f) is necessary for reasons of substantial public interest (with a basis in law)
- (g) Health or social care (with a basis in law)
- (h) Public health (with a basis in law)
- (i) Archiving, research and statistics (with a basis in law)

If the group is relying on conditions (b), (g), (h), or (i), we will also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.



If the group is relying on the substantial public interest condition, we also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018, as well as undertaking a Legitimate Interests Assessment (LIA) to ensure that our processing undertaken under this basis has implemented suitable measures to safeguard the data subject's interests.

If the group is relying on legitimate interests or substantial legitimate interests, consideration should be made as to whether this falls under a recognised legitimate interest, as set out in Article 6(1)(ea) UK GDPR (as amended by DUAA 2025). If this is the case, there is no requirement to undertake an LIA.

Privacy notices

The group has produced a number of tailored Privacy Notices, which we are required to provide to all customers and data subjects, whose Personal Data is processed by, or on behalf of, the group. The Privacy Notice for service users and customers must be provided to the customer from the outset of processing their Personal Data and they should be advised of the terms of the Privacy Notice when it is provided to them.

The Privacy Notices set out the Personal Data processed by the Association and the basis for that Processing. The general or public Privacy Notice is provided to all of the group's customers at the outset of processing their data, and the Employee Privacy Notices is provided to all employees at the outset of their employment.

Privacy Notices are available from the Data Protection Team, on the intranet or on the company website.

Employees

Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the group. Details of the personal data processing, and the basis for our processing of that Personal data is contained within the Employee Privacy Notice which is provided to Employees at the same time as their Contract of Employment, and the current version of this document is available on our intranet.

Consent

Consent as a ground for processing will need to be used from time to time by the group when processing Personal Data. It should be only used by the group where no other alternative ground for processing is available. In the event that the group requires to obtain consent to process a data subject's Personal Data, it shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form, or take some other form of



affirmative action, if willing to consent. Any consent to be obtained by the group must be for a specific and defined purpose (i.e. general consent cannot be sought).

4. Data Sharing

The group shares its data with various third parties for numerous reasons in order that its day-to-day activities are carried out in accordance with the groups relevant policies and procedures. In order that the group can monitor compliance by these third parties with Data Protection laws, the group will require the third-party organisations to enter into an agreement with the group governing the processing of data, security measures to be implemented and responsibility for breaches.

Data Sharing

Personal data is from time to time shared amongst the group and third parties who require to process personal data for their own separate purposes. Both the group and the third party will be processing that data in their individual capacities as data controllers.

Where the group shares in the processing of Personal Data with a third-party organisation (e.g. sharing with other housing associations or sharing with other public bodies), it shall require the third-party organisation to enter into a Data Sharing Agreement with the group.

Data Processors

A data processor is a third-party entity that processes personal data on behalf of the Association in the delivery of its services to the Group (e.g. payroll, maintenance and repair works).

A data processor must comply with data protection laws and the group's written instructions, including a written contract setting out the processor's contractual obligations, including clauses that are legally required to be inserted by the UK GDPR, or clauses that are required to be inserted to ensure that the Group complies with its legal obligations under the UK GDPR or DPA.

Data Collection

When initially collecting personal data relating to a data subject, directly from the data subject (no later than 30 days afterward), we must provide the Data Subject with a copy of our relevant a Privacy Notice during the course of collecting that information or provide them with a link to the Privacy Notice online.

If we are supplied Personal Data relating to a Data Subject by a third party, we must supply an appropriate Privacy Notice to the Data Subject without undue delay or when first



communicating with the data subject and no later than one month after receipt of that information. If this would be unfeasible or would involve disproportionate effort, the group may be entitled to rely on the privacy notice being made publicly available on-line as meeting this obligation.

If this notice has already been supplied to the individual, it does not need to be supplied again.

If we change the way Personal Data is processed, we may need to issue an updated privacy notice defining the new processing and legal basis.

5. Data Storage and Security

All personal data held by the group must be stored securely, whether electronically or in paper format.

Paper Storage

If Personal Data is stored on paper, it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no Personal Data is left where unauthorised personnel can access it.

When the Personal Data is no longer required it must be disposed of by the employee to ensure its destruction. If the Personal Data is required to be retained on a physical file, then the employee should ensure that it is affixed to the file which is then stored in accordance with the groups storage provisions.

Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to the groups data processors or those with whom the group has entered into a Data Processing or Sharing Agreement. If Personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must always be encrypted and stored securely when not being used. The Password must not be stored with or transmitted with the media holding the electronic Personal Data.

Personal Data must not be saved directly to mobile devices and instead must be stored on designated storage drives and servers with appropriate access controls in place.

6. Transfers of Data Outside the UK

The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK 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 UK if one of the following conditions applies:

- ▶ the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the data subject's rights and freedoms;
- ▶ appropriate safeguards are in place such as standard contractual clauses governing the transfer of personal data as approved for use by the UK Government;
- ▶ the data subject has provided their explicit (documented) consent to the proposed transfer after being informed of any potential risks; or
- ▶ the transfer is necessary for one of the other permitted reasons set out in the UK GDPR such as the performance of a contract with a data subject or reasons of public interest.

Apart from where the transfer is to a country deemed by the UK to have adequate data protection laws, we may be required to undertake a transfer impact assessment prior to the transfer taking place. Please contact the Data Protection Team prior to commencing such transfers.

7. Implementation

Data Protection laws place responsibilities on all employees and individuals, not just the organisation. All employees have a responsibility to ensure that information is processed in accordance with all current data protection laws. If you are directly involved in the processing of information you need to ensure that you understand the meaning of the data protection principles.

8. Responsibilities

This policy is written and overseen by the Data Protection Officer.

This policy will be monitored by the Data Protection Team and reviewed every three years, or when there are changes to legislation or renewed guidance issued by the ICO.

All colleagues (including temporary colleagues, casual colleagues, volunteers, apprentices and work experience) must comply with this policy. Managers have a duty to ensure colleagues have read this policy before starting to process any personal data on behalf of



the group and ensure that they have completed the mandatory data protection and cyber security training.

All colleagues have a duty to report any breach of this policy to the Data Protection Team without undue delay. Wilful or repeated breaches of this policy (or other applicable group data protection policies may result in disciplinary, or other remedial action, and in certain situations, may also amount to a criminal offence

Data Processors (contractors, suppliers and sub-contractors) and joint controllers or partners, must be subject to contractual terms designed to ensure that they process personal data in a transparent, appropriate, secure and legal manner. Each colleague member, when handling personal data, has a responsibility to carry out, or raise the following with their line manager for compliance:

- ▶ Ensure that it is covered by the individual company's Registration.
- ▶ Review and/or introduce new procedures to ensure that the group complies with the Data Protection Laws by completing a Data Protection Impact Screening Checklist in the first instance
- ▶ Ensure there is a condition for processing the personal information or sensitive personal information. (under Article 6 and Article 9 of the UK GDPR)
- ▶ Always consider wide a definition of processing in determining if an activity involved constitutes an activity governed by data protection laws.
- ▶ Always check before passing information to a third party that the group is registered to disclose the information to that third party and the third party is lawfully entitled to the information. Also ensure there are appropriate Data Sharing or Processing agreements in place or/ and the correct form is submitted and approved before the information is shared and that a record of the request and the disclosure is retained. Unless there are exceptional circumstances, do not disclose personal information to a third party solely based on a verbal request, and instead, ask for the request to be made in writing If in doubt, do not disclose without consulting with the Data Protection Team.
- ▶ Remember the need for strict security when handling personal information. We are all responsible for keeping personal information secure and to prevent unauthorised access.
- ▶ You must ensure that Personal information recorded on printouts, paper files, and any other form of media must never be left lying around. They must always be kept physically secure, and securely destroyed when no longer required. In accordance with our Data Deletion Policy.
- ▶ Filing cabinets containing manual information files should be locked when not being used.
- ▶ Computer workstations (including PC's laptops, terminal etc.) must always be locked, when unattended. Password(s) should never be divulged and should be non-

guessable, for example using three separate unrelated words. Passwords should be changed regularly in line with our internal ICT policy.

- ▶ Information stored on storage media for example CD's, USB Drives must be encrypted and password protected.
- ▶ Portable devices, for example cameras, PDAs, mobile phones that contain information must be 'locked'/ password protected.
- ▶ Password protection or similar means of controlling access must be incorporated within computer systems holding information governed by Data Protection laws.
- ▶ Your responsibility for security does not end with keeping it safe whilst it is in your possession / department; it extends to making known to other people to whom it is supplied that the information is to be protected in line with all current Data Protection Laws.
- ▶ Should you receive a request from a customer in relation to access to their information, you should contact the Data Protection Team as soon as possible and without delay. See the Subject Access Policy for further guidance.
- ▶ When working at home or away from the office do not leave confidential information unattended or out overnight. It may seem unlikely that a friend, stranger or family member would even be interested in personal data held by emh. Regardless, make sure that data is kept away from non-employees. Also ensure that any smart devices with microphones are disabled when receiving work voice/video calls in their vicinity.
- ▶ Be mindful of where you are on voice/video calls so that conversations are not overheard by persons unauthorised persons.
- ▶ If you are in any doubt or have any questions relating to Data Protection you must refer to the Data Protection Team, your line manager, or any of the responsible officers listed in section 1.5 of this document.

9. Data Breaches

A data breach can occur at any point when handling Personal Data and the emh has reporting duties in the event of a data breach or potential breach occurring. Breaches which are likely to pose a serious risk to the rights and freedoms of individuals need to be reported externally.

There are three types of personal data breach:

- ▶ Confidentiality breach - an unauthorised or accidental disclosure of, or access to, personal data
- ▶ Availability breach - an accidental or unauthorised loss of access to, or destruction of personal data
- ▶ Integrity breach - an unauthorised or accidental alteration of personal data



The group takes the security of data very seriously and in the event of a breach will take the following steps:

- ▶ As soon as emh or an individual becomes aware of, or have a reasonable suspicion that a personal data breach has, or may have occurred, the Data Protection Team must be notified of the breach or potential breach and be provided with all information available about the breach or potential breach without undue delay
- ▶ emh must seek to contain, or mitigate the impact of, the breach by whatever means available
- ▶ The Data Protection Team must record the personal data breach on the Groups' breach register and consider whether the breach is one which requires to be reported to the ICO and data subjects affected and do so in accordance the Personal Data Breach Policy
- ▶ Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

Please see our Personal Data Breach Policy for more information.

10. Breaches of this Policy

Any alleged breach of the Data Protection Policy will be investigated by emh.

A breach of the Data Protection Policy by an employee will be treated as a disciplinary matter under his or her contract of employment and an appropriate sanction may be applied. An investigation into any allegation of such a breach made against an employee will be conducted in accordance with emh's relevant policies for such investigations.

A breach of the Data Protection Policy by a Board or Committee Member will be treated as a breach of his or her duties and obligations to emh and his or her services agreement with emh. An investigation into any allegation of such a breach made against a Board or Committee Member will be conducted in accordance with emh's relevant policies for such investigations and an appropriate sanction may be applied.

11. Associated Documents

Legislation, guidance and policies that are relevant and should be read in conjunction with this Policy include:

Legislation

- ▶ UK General Data Protection Regulation



- ▶ Data Protection Act 2018
- ▶ Crime and Disorder Act 1998
- ▶ Human Rights Act 1998
- ▶ Privacy and Electronic Communications (EU Directive) Regulations 2003

Guidance

- ▶ Best Practice Guides – ICO

Internal Documents

- ▶ People Data Protection Policy
- ▶ Data Protection Section on the emh Central (Intranet)
- ▶ Personal Data Breach Policy
- ▶ Encryption Policy
- ▶ Data Breach Toolkit
- ▶ Subject Access Request Policy
- ▶ Document Retention Policy
- ▶ Data Subject Rights Policy
- ▶ Data Deletion Policy
- ▶ ICT Acceptable Usage Policy
- ▶ CCTV Policy
- ▶ Data Protection Impact Assessment Policy
- ▶ Special Category Data Policy