mind Mid Kent

Data Protection Policy

Contents

1. Who this policy applies to

This policy applies to all employees, trustees and volunteers or sub-contractors (collectively referred to as personnel in this document) whose role involves processing personal data for which we are either the data controller or the data processor (see section 4 for definitions).

2. Aims of this policy

The policy aims to ensure our compliance with the Data Protection Act 2018 and the UK GDPR (General Data Protection Regulations), and to protect the rights and freedoms of people whose information we collect and process. The policy provides support, guidance and procedure for personnel engaged in processing our data and administering the rights of our data subjects.

3. Policy background

GDPR is European Union (EU) legislation that came into effect in May 2018. The Data Protection Act 2018 brought GDPR into UK law. It sits alongside and supplements the GDPR by providing exemptions, setting out separate data protection rules for law enforcement authorities, and extending data protection to some other areas. It also sets out the Information Commissioner's Office (ICO) functions and powers.

The UK GDPR together with amendments to Data Protection Act 2018 came into effect from 1 January 2021, reflecting the UK's status outside the EU. UK GDPR is based on the GDPR with some changes to make it work more effectively in a UK context. The purpose of the UK GDPR is to ensure the rights and freedoms of living individuals, and to protect their personal data by ensuring that it is never processed without their knowledge and without a lawful basis for processing.

4. Definitions

Child means anyone under the age of 18. It is only lawful to process the personal data of a child under the age of 13 upon receipt of consent from the child's parent or legal custodian.

Data controller may be a natural or legal person, whether a public authority, agency or other body which, individually or jointly with others, is in charge of ascertaining the purposes and means by which personal data shall be processed. Where UK predetermines the purposes and means of processing personal data, the data controller or, if appropriate, the specific criteria for selecting the data controller, may be provided for by UK law.

Data subject refers to any living person who is the subject of personal data (see above for the definition of 'personal data') held by an organisation. A data subject must be identifiable by name, ID, address, online identifier or other factors such as physical, physiological, genetic, mental, economic or social.

Data subject consent refers to any specific indication by the data subject that signifies consent to the processing of personal data. Consent may take place by way of a written or oral statement or by clear, unambiguous action and must be given freely at all times, without duress, with the data subject being properly informed.

Data protection lead is the person whose role is to oversee all the activity of a data controller or processor, ensuring compliance with legislation and policy. This role is also known as the information governance contact or senior information risk owner (SIRO).

Data protection officer (DPO) is a statutory independent role, governed by the UK GDPR. Their task is overseeing, facilitating and promoting data protection within their organisation. Public authorities and some other bodies must appoint a DPO, organisations who don't require a DPO will have a similar role such as a data protection lead.

Filing system refers to any personal data set which is accessible on the basis of certain benchmarks, or norms and can be centralised, decentralised or dispersed across various locations.

Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights, whose functions are defined in the Data Protection Act 2018.

Personal data means any data relating to a data subject.

Personal data breach refers to a security breach which results in the disclosure, alteration, destruction or loss of personal data, as well as unauthorised access to personal data that is stored, transmitted or processed by any other means, whether accidentally or unlawfully. All personal data breaches must be reported to relevant regulatory authority by the data protection lead at all times, whereas the data subject need only be informed of a data breach when it is likely that the breach will have an adverse effect on his or her privacy or personal data.

Processing refers to any action taken in relation to personal data, including but not limited to collection, adaptation or alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise.

Profiling refers to any form of personal data processing that is automated, with the intention of assessing personal aspects of a data subject or analysing a data

subject's employment performance, economic status, whereabouts, health, personal preferences and behaviour. The data subject has a right to object to profiling and a right to be informed of the fact that profiling is taking place, as well as the intended outcome(s) of the profiling.

Record of processing activities (ROPA) is a legal requirement and describes the purposes of the processing, retention schedules and other important information about processing activities.

Special categories of personal data refers to personal data covering such matters as racial or ethnic origin, beliefs - whether religious, political or philosophical - membership of a trade-union and data relating to genetics, biometric identification, health and mental health, sexual orientation and sex life.

Subject access request (SAR) is a request by a data subject for a copy of the personal data held and processed by a data controller.

Third party is a natural or legal person other than the data subject who is authorised to process personal data, whether a public authority, agency or other body controller, processor or any other person(s) under the direct authority of the controller or processor.

5. Policy

5.1. Principles of data protection

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime. They are set out right at the start of the legislation, and inform everything that follows.

Article 5(1) requires that personal data will be:

1) processed lawfully, fairly and in a transparent manner in relation to individuals ('**lawfulness, fairness and transparency**');
2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('**purpose limitation'**);
3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');
4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');

5) 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 ('**storage limitation**');

6) 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 ('**integrity and confidentiality**').

Article 5(2) adds that:

7) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**').

5.2. Application of the principles of data protection

Lawfulness, fairness and transparency

We only process personal data when we have identified a lawful basis (see section 5.4). Policies must be transparent, meaning that we must ensure that our personal data processing policies, as well as any specific information provided to a data subject, are readily available, easily accessible, and drafted using clear plain language.

Data subjects must have access to the following information:

1) Controller - the identity and contact details of the data controller and any of its representatives.
2) Purpose - the purpose or purposes and legal basis of processing.
3) Storage period - the length of time for which the data shall be stored.
4) Rights - confirmation of the existence of the following rights:
    a) Right to request access
    b) Right of rectification
    c) Right of erasure
5) Right to raise an objection to the processing of the personal data.
6) Categories - the categories of personal data.
7) Recipients - the recipients and/or categories of recipients of personal data, if applicable.

8) Location - if the controller intends to make a transfer of personal data to a third country and the levels of data protection provided for by the laws of that country, if applicable.

9) Further information - any further information required by the data subject in order to ensure that the processing is fair and lawful.

Purpose limitation

We collect and process personal data for specified, explicit and legitimate reasons. When personal data is obtained for specific purposes, it is only to be used in relation to that purpose.

Data minimisation

We collect and process personal data that is adequate, relevant and no more than is required. The data protection lead will:

1) ensure that personal data which is superfluous and not required for the purpose(s) for which it is obtained, is not collected;

2) approve all data collection forms, whether in hard-copy or electronic format;

3) carry out an annual review of all methods of data collection, checking that they are still appropriate, relevant and not excessive;

4) securely delete or destroy any personal data that is collected in a manner that is excessive or unnecessary according to our UK GDPR policies.

Accuracy

Personal data must be accurate and up-to-date.

1) Data should not be kept unless it is reasonable to assume its accuracy. Data that is kept for long periods of time must be examined and amended, if necessary.

2) All staff must receive training from our data protection lead or a suitable training provider to ensure they fully understand the importance of collecting and maintaining accurate personal data.

3) Individuals are personally responsible for ensuring that the personal data held by us is accurate and up-to-date. We will assume that information submitted by individuals via data collection forms is accurate at the date of submission.

4) All personnel are required to update the administration team as soon as reasonably possible of any changes to personal information, to ensure records are kept up to date.

5) The data protection lead must ensure that relevant and suitable additional steps are taken to ensure that personal data is accurate and up-to-date.

6) The data protection lead will carry out an annual review of all personal data controlled by us, referring to the ROPA, and determine whether any data is no longer required to be held in accordance with the guidelines of the ICO, arranging for that data to be deleted or destroyed in a safe manner.

7) The data protection lead will also ensure that where inaccurate or out-of-date personal data has been passed on to third parties, that the third parties are informed and instructed not to use the incorrect or out-of-date information as a means for making decisions about the data subject involved. The data protection lead will also provide an update to the third party, correcting any inaccuracies in the personal data.

Storage limitation

The form in which the personal data is stored must be such that the data subject can only be identified when it is necessary to do so for processing purposes. The following principles apply:

1) Personal data that is kept beyond the processing date must be either deleted, encrypted, pseudonymised or put beyond use and kept to an absolute minimum, to ensure the protection of the data subject's identity should a data breach incident occur.

2) Personal data must be retained according to the retention schedule in the ROPA and must be destroyed or deleted in a secure manner as soon as the retention date has passed.

3) Should any personal data be required to be retained beyond the retention period, this may only be done with the express written approval of the data protection lead, which must be in line with data protection requirements.

Integrity and confidentiality

Processing of personal data must always be carried out in a secure manner. Personal data must not be processed in an unauthorised or unlawful manner, nor should it be accidentally lost or destroyed. We will implement robust technical and organisational measures to ensure the safeguarding of personal data.

Accountability

As a data controller we must adhere to the principles of data protection and be able to demonstrate our compliance. The data protection lead has a key role, however data protection is the responsibility of all personnel.

5.3. Responsibilities under the UK GDPR

We are a data controller under UK GDPR. Employees with managerial or supervisory responsibilities are responsible for ensuring that good personal data

handling practices are developed, reviewed and encouraged within Mid Kent Mind, as per their individual job descriptions.

Breaches of this policy will be dealt with according to our disciplinary policy. If there is a possibility that the breach could amount to a criminal offence, the matter will be referred to the relevant authorities.

Data protection lead

The position of data protection lead, which involves the management of personal data as well as compliance with the requirements of the UK GDPR and demonstration of good practice protocol, is to be taken up by an appropriately qualified and experienced member of our management team, this will normally be the head of digital.

The data protection lead reports to the chief executive and, amongst other things, is accountable for the development, implementation and day-to-day compliance with this policy, both in terms of security and risk management. In addition, the data protection lead is directly responsible for ensuring that we are UK GDPR compliant and that our personnel are compliant in respect of data processing that occurs within their field of responsibility and/or oversight.

The data protection lead will always be the first point of contact for personnel needing guidance in relation to data processing and data protection compliance.

The data protection lead is also responsible for other procedures, such as subject access requests and carrying out data processing impact assessments.

It is not just the data protection lead who is responsible for data protection. All personnel who process personal data are responsible for ensuring compliance with data protection laws. All staff undergo mandatory annual training in GDPR and data security.

Personnel are personally responsible for ensuring that all personal data they have provided and has been provided about them is accurate and up-to-date.

Risk assessment

It is vital that we are aware of all risks associated with personal data processing and it is via our risk assessment process that we can assess the level of risk. We are also required to carry out assessments of the personal data processing undertaken by other organisations on our behalf and to manage any identified risks, to mitigate the likelihood of potential non-compliance with this policy.

Where personal data processing is carried out by using new technologies, or when a high risk is identified in relation to the rights and freedoms of natural persons, we are required to engage in a risk assessment of the potential impact. More than one risk may be addressed in a single data protection impact assessment (DPIA).

If the outcome of a DPIA points to a high risk that our intended personal data processing could result in distress and/or may cause damage to data subjects, it is up to the data protection lead to decide whether we ought to proceed and the matter should be escalated to them. In turn, the data protection lead may escalate the matter to the regulatory authority if significant concerns have been identified.

It is the role of the data protection lead to ensure that appropriate controls are in place to ensure that the risk level associated with personal data processing is kept to an acceptable level, as per the requirements of the UK GDPR and our risk acceptance criteria.

Record of processing activities (ROPA)

We keep and maintain an accurate record of processing activities (ROPA). The ROPA lists all of the various assets in which data is held, the lawful basis of processing (see section 5.4), the person responsible for the upkeep of the asset, the types and sources of the data, the retention period, and security measures protecting the data.

The ROPA is stored on our secure One Drive, Management File.

Registration and notification

We are registered with the Information Commissioner's Office (ICO) as a data controller engaged in processing personal information of data subjects. We have identified all the personal data that we process and recorded it in our record of processing activities (ROPA).

The data protection lead will retain a copy of all notifications made by us to the ICO and record all notifications made.

The ICO notification will be reviewed on an annual basis and the data protection lead is responsible for each annual review of the details of the notification, keeping in mind any changes to our activities.

5.4. Lawful basis for data processing

Our ROPA includes a record of the lawful basis of processing data, and where applicable the lawful basis of processing special category data and criminal data. Personnel and clients are notified of the lawful basis of processing together with their rights under UK GDPR through one or more of our privacy notices.

Parental or custodial consent is a legal requirement if/when we are a provider of online services to children under the age of 13.

Essential lawful bases

Under UK GDPR personal data can only be processed under one of the six lawful bases for processing. We will only process personal data when at least one lawful basis has been identified.

The lawful bases are:

1) The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
2) Processing is necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject before entering into a contract.
3) Processing is necessary for compliance with a legal obligation to which the controller is subject.
4) Processing is necessary to protect the vital interests of the data subject or of another natural person.
5) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Special category lawful bases

In addition a lawful basis for processing special category data must be identified prior to processing this kind of sensitive data. There are 10 lawful bases for processing special category data, however only three are likely to apply to our data processing:

1) The data subject has given explicit consent.
2) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.
3) Processing is necessary for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

For example we use the basis of employment, social security and social protection law to check if individuals are entitled to work in the UK.

We use health or social care to process information about the mental health of our clients in order to provide a safe and effective service.

Criminal lawful bases

Also in addition, a lawful basis for processing criminal data must be identified prior to processing this kind of data. UK GDPR gives extra protection to 'personal data relating to criminal convictions and offences or related security measures'. This covers a wide range of information about criminal activity, suspicion or allegations, investigations and proceedings. It includes not just data which is obviously about a specific criminal conviction or trial, but also any other personal data 'relating to' criminal convictions and offences. Information about a specific crime committed against an identifiable victim is the personal data of the victim and 'relates to' criminal offences. Even recording the fact that a person has no criminal convictions is personal data 'relating to' criminal convictions.

There are 28 lawful bases for processing criminal data, those that are likely to apply to our processing are:

1) Health or social care purposes
2) Counselling
3) Safeguarding of children and individuals at risk
4) Consent
5) Vital interests
6) Manifestly made public by the data subject

The area in which we formally process criminal data is in recruiting and managing personnel. Because our personnel have contact with individuals at risk, we are able to require an Enhanced DBS check. This means that we are processing personal data relating to criminal offences. The lawful basis that we apply in this case is safeguarding of children and of individuals at risk.

Processing of criminal data may occur incidentally in case management work with clients if they disclose material that relates to criminal offences (including the impact of being a victim). We will only record this kind of data when:

- we have identified a lawful basis for processing; and
- we believe that, in relation to the service we are providing, it is in the best interests of the client to record the data; or
- we believe that the information should be recorded in connection with safeguarding; or
- the information has manifestly been made public by the client.

5.5. The rights of data subjects

Data subjects enjoy the following rights in relation to personal data that is processed and recorded:

1) The right to make access requests in respect of personal data that is held and disclosed (see section 5.7).
2) The right to refuse personal data processing, when to do so is likely to result in damage or distress.
3) The right to refuse personal data processing when it is for direct marketing purposes.
4) The right to be informed about the functioning of any decision-making processes that are automated which are likely to have a significant effect on the data subject.
5) The right not to solely be subject to any automated decision-making process.
6) The right to claim damages should they suffer any loss as a result of a breach of the provisions of the UK GDPR.
7) The right to take appropriate action in respect of the following: the rectification, blocking and erasure of personal data, as well as the destruction of any inaccurate personal data.
8) The right to request that the ICO carry out an assessment as to whether any of the provisions of the UK GDPR have been breached.
9) The right to be provided with personal data in a format that is structured, commonly used and machine-readable.
10) The right to request that their personal data is sent to another data controller.
11) The right to refuse automated profiling without prior approval.

5.6. Profiling

Profiling is defined as any form of automated processing of personal data to analyse or predict aspects of the person's economic situation, interests, personal preferences, health, reliability, performance at work, behaviour location or movements.

We use profiling techniques to analyse our database and publicly available information about adults who have or may be interested in supporting us. Specialist third party prospect research companies may be engaged to assist in this process using their own database.

Profiling is used for marketing and fundraising purposes and not for any automated decision making. The lawful basis for profiling is 'justified interest'. These techniques deliver a better and more tailored experience to adult

supporters that takes into account their motivations, philanthropic interests and capacity to give. It also helps to avoids inappropriate contacts or requests.

Publicly accessible and available information sources may include:

Public Registers: Companies House, Charities Commission, The Electoral Commission, The Electoral Roll, The Financial Services Register, The Land Registry, The Law Society and professional directories.

UK Reference Volumes and Publications and Online Resources: Who's Who and Who Was Who, Debrett's (e.g. People Today, Peerage and Baronetage), fundsonline.org.uk, City of London Livery Company information, Rich Lists including The Sunday Times Rich List.

Reliable Print, Broadcast Media and Online Resources: newspapers (e.g. The Times and Sunday Times, The Guardian, The Telegraph, Financial Times, City A.M. (business newspaper) lifestyle magazines, e.g. Kent Life both online and printed versions. Information that individuals put into the public domain such as on company websites or biographies on professional networking sites, Linkedin for example.

The information from these publicly available sources includes things such as whether a person is a trustee of a charity or a company director, their business profession, and estimated property values.

People who are the subject of profiling activity are entitled to access details of the information used and are also entitled to object to profiling. When an objection is received, all profiling activity on the individual will cease and information generated through profiling will be securely destroyed.

5.7. Subject access request (SAR) and procedure

People have the right to ask us if we are processing their personal data, and if so to obtain a copy of their personal data. This is a subject access request (SAR) and it is important we recognise when a request has been made as UK GDPR does not set out a formal requirement for a valid request. It can be made verbally or in writing, including via social media. When it is clear that an individual is asking for their personal data, this must be treated formally as a SAR.

It is vitally important that personnel receiving a SAR (or a suspected SAR) report this immediately to their line manager and/or the data protection lead. Failure to do so can lead to serious consequences and may result in disciplinary action.

If we are not completely confident about the identity of the requester, we will confirm their identity before proceeding, for example by requesting verifiable ID. If the SAR is made by someone other than the person the data is about (such as a friend, relative or solicitor), we will need to confirm that they have written

authority to act on behalf of the person concerned, or see a document showing general power of attorney.

From the date of the request, or the date of confirmation of the requester's ID, we will complete the SAR within one calendar month. In the case of a complex request (for example technical difficulties in retrieving the information, large volumes of particularly sensitive information, specialist work in redaction) we may need up to another two calendar months and we will inform the requester before the end of the first calendar month.

In addition to a copy of personal data, people are entitled to the following information:

1) Our purposes for processing the data;
2) Categories of personal data that we're processing;
3) Recipients to whom we may disclose the data;
4) Our retention period for storing personal data;
5) Their right to request rectification, erasure or restriction or to object to processing;
6) Their right to lodge a complaint with the Information Commissioner's Office (ICO);
7) Information about the source of the data, if we did not obtain it directly from them;
8) Whether or not we use automated decision-making (including profiling);
9) The safeguards we have provided where personal data has or will be transferred to a third country or international organisation.

However we will not assume that the requester wants all of the information that we have, as sometimes it is only data relating to a particular issue or circumstance that they are looking for. If it has not been made clear in a written request, we will ask the requester about what they are seeking.

The data protection lead will then initiate a search for information relating to the person, in any media where the information might be found.

The information will then be examined to check that it is the personal data of the data subject. Any personal information that does not related to the data subject will be redacted.

There may be occasions when personal data includes information that is closely linked to someone else. In these situations we aim to release the personal data requested, however we will take into account and consider the impact of disclosing data about someone else. In the case of a negative impact on someone

else, we may withhold the information and we will record our reasons for doing so.

There may also be occasions when a search for personal data produces data that belongs to us, rather than the individuals identified. For example if a situation arises between clients within a service we run and that we need to manage, data recorded by us concerns our management of the situation and is considered to be our data, not that of individuals who may be identified. In this case the data will not be released and we will record our reasons.

After a final check, we will provide the data securely in any reasonable format that the data subject has requested and keep a dated record of the information sent.

Further detailed guidance about SARs is available from the ICO's website: https://ico.org.uk/right-of-access/

5.8. Partnerships, sharing and disclosure

Partnerships

When we work in partnership with a third party on any project or service that requires sharing personal data, an agreement must be in place that covers data protection. The agreement will clearly identify who are data controllers, data processors, and where accountability for data protection lies. The agreement will also identify the policies, procedures and privacy notices that apply to the project.

Sharing

All third parties working for us who have or may have access to personal data are required to read, understand and comply with this policy at all times. All third parties are required to enter into a data confidentiality agreement before accessing personal data. The data protection obligations imposed by the confidentiality agreement will be equally onerous as those to which we have agreed to comply with. We will have the right to audit any personal data accessed by third parties under the confidentiality agreement.

Disclosure

We must take appropriate steps to ensure that no personal data is disclosed to unauthorised third parties. This includes friends and family members of the data subject, governmental bodies and, in special circumstances, even the police.

Disclosure is permitted by the UK GDPR without the consent of the data subject under certain circumstances, namely:

- In the interests of safeguarding national security;

- In the interests of crime prevention and detection which includes the apprehension and prosecution of offenders;
- In the interests of assessing or collecting a tax duty;
- In the interests of discharging various regulatory functions, including health and safety;
- In the interests of preventing serious harm occurring to a third party;
- In the interests of protecting the vital interests of the data subject i.e. only in a life and death situation.

The data protection lead is responsible for handling all requests for the provision of data for these reasons and authorisation by the data protection lead shall only be granted with support of appropriate documentation.

5.9. Data retention and disposal

In line with the principle of 'storage limitation' (see section 3.3) we must not retain personal data for longer than is necessary. The ROPA describes all of our data assets and the retention period for the data held in the asset. In general, we retain client and personnel data for 5 years following the last engagement, and financial data for 7 years.

Personal data must be disposed of according to our secure disposal procedure (described in section 6.2 of our IT security policy) to ensure the rights and freedoms of data subjects are protected.

5.10. Adequacy of transfer

The following safeguards and exceptions are in place to ensure that data is not transferred to a country outside of the UK, with the transfer being off limits unless one or more of the safeguards or exemptions listed below apply:

Safeguards

1) Assessing the adequacy of the transfer, by reference of the following:
    a) The nature of the personal data intended to be transferred;
    b) The country of origin and country of intended destination;
    c) The nature and duration of the personal data use;
    d) The legislative framework, codes of practice and international obligations of the data subject's country of residence;
    e) The security measures to be implemented in the country of intended destination in relation to the personal data.

2) Binding corporate rules - we are free to implement approved binding corporate rules in relation to personal data transfer outside of the UK, however only with prior permission from the relevant regulatory body.

Model contract clauses – we are free to implement model contract clauses in relation to personal data transfer outside of the UK and there will be an automatic recognition of adequacy of transfer, should the model contract clauses receive approval from the relevant regulatory body.

Exceptions

In the absence of an adequacy decision, including binding corporate rules and model contract clauses, no transfer of personal data to a third country may take place unless one of the following preconditions is satisfied:

1) Explicit consent has been provided by a fully informed data subject, who has been made aware of all possible risks involved in the light of appropriate safeguards and an adequacy decision;
2) The personal data transfer is a prerequisite to the performance of a pre-existing contract between the data controller and the data subject or when the data subject requests that pre-contractual measures are implemented;
3) The personal data transfer is a prerequisite to the conclusion or performance of a pre-existing contract between the data controller and another person, whether natural or legal, if it is in the interest of the data subject;
4) The personal data transfer is in the public interest;
5) The personal data transfer is required for the creation, exercise or defence of legal claims;
6) The data subject is not capable of giving consent, whether due to physical or legal limitations or restrictions and the personal data transfer is necessary for the protection of the key interests of the data subject or of other persons;
7) The personal data transfer is made from an approved register, confirmed by UK law as having the intention of providing public information and which is open to consultation by the public or by an individual demonstrating a legitimate interest, but only so far as the legal requirements for consultation are fulfilled.

5.11. Data security

All personnel are personally responsible for keeping secure any personal data held by us for which they are responsible. Under no circumstances may any personal

data be disclosed to any third party unless we have provided express authorisation and have entered into a confidentiality agreement with the third party.

Accessing and storing personal data

Access to personal data will only be granted to those who need it and only according to the principles of our IT security policy.

All personal data must be stored:

- In a locked room, the access to which is controlled; and/or
- In a locked cabinet, drawer or locker; and/or
- If in electronic format and stored on a computer, encrypted according to the requirements set out in the IT security policy; and/or
- If in electronic format and stored on removable media, encrypted as per the IT security policy.

Before being granted access to any organisational data, all staff and volunteers must understand and have access to our IT security policy.

Computer screens and terminals must not be visible to anyone other than authorised personnel.

No manual records may be accessed by unauthorised personnel and may not be removed from the business premises in the absence of explicit written authorisation. Manual records must be removed from secured archiving when access is no longer needed on a day-to-day basis.

All deletion of personal data must be carried out in accordance with our retention requirements. Manual records which have passed their retention date must be shredded and disposed of as 'confidential waste' and any removable or portable computer media such as hard drives as USB sticks must be destroyed as per the IT security policy prior to disposal.

Personal data that is processed 'off-site' must be processed by authorised personnel, due to the increased risk of its loss, damage or theft.

5.12. Data Collection Methods

Data Collection Methods (sometimes referred to as 'Data Processing for ease) refers to the methods which MKM undertake as an organisation to collect data from clients, or prospective clients who may seek to engage with services provided by our organisation. MKM will generally collect data through three distinct means:

- Audibly via telephone discussions with clients, potential clients or other parties who may contribute data which the organisation needs to retain.

- Digitally via the completion of online website forms, e-mails, referral portals (such as MPS for work with Live Well Kent) and through other digital mediums.

- Paper-based forms – such as completed registration forms in face-to-face settings, wellbeing checks for face-to-face services and other paper-based notes.

The security guidance used to ensure that data is held in a secure method in accordance with GDPR guidance can be found in MKM's 'Information Security Policy'. Responsibility for oversight of MKM's data collection methods sits with the Digital Lead, who is tasked with overseeing the record keeping of a 'ROPA' – or record of processing activities in accordance with data protection legislation.

This record will clearly outline all of MKM's data collection methods, their disposal timeframe, and the associated levels of data security precautions which should be applied to these collection methodologies.

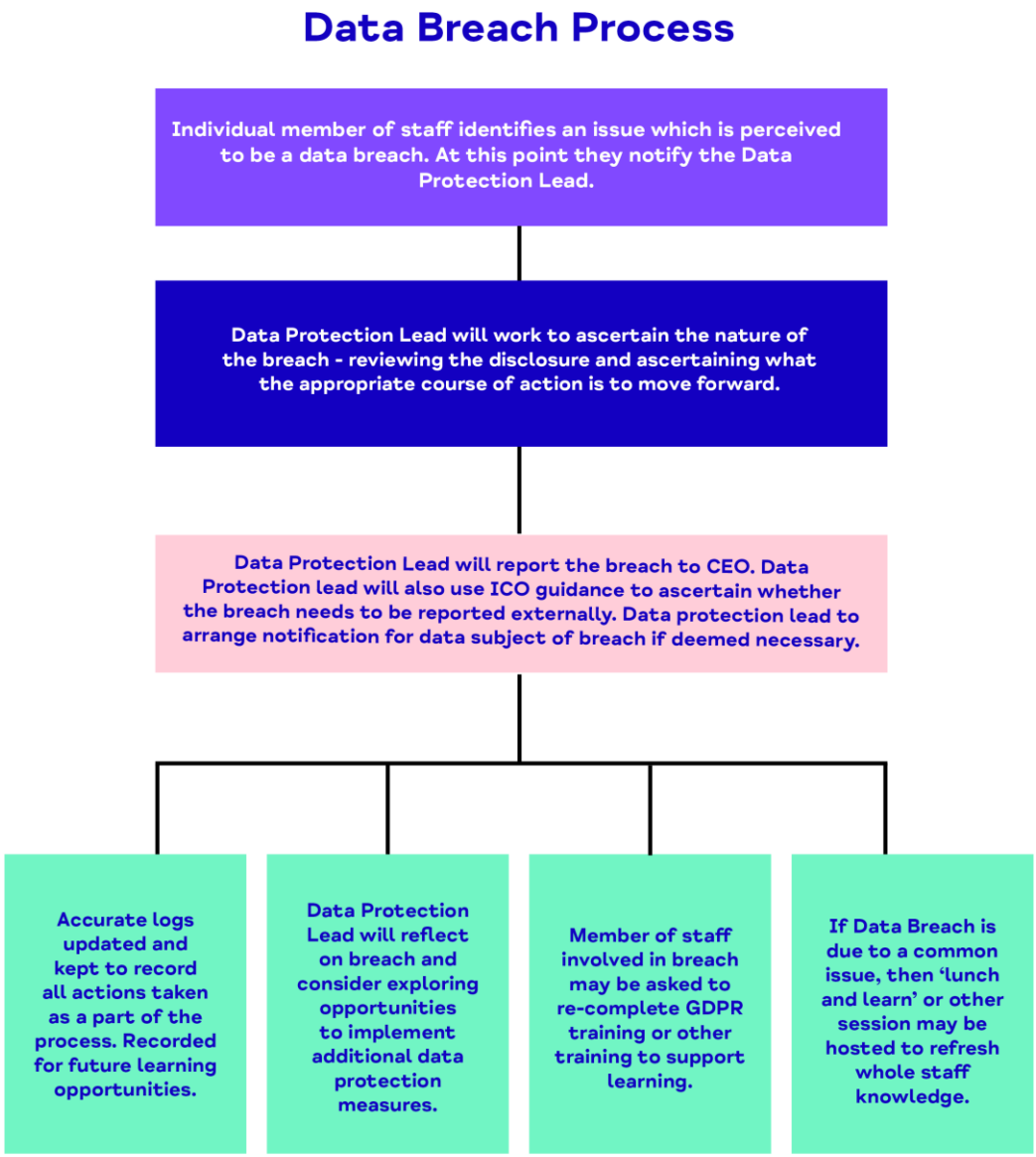
5.13. Personal data breaches

Personnel who become aware of any actual, suspected or possible security breach which could lead to the disclosure, alteration, destruction, loss, or unauthorised access to personal data must immediately report their concern to the line manager and/or the data protection lead. Failure to do so can lead to serious consequences and may result in disciplinary action.

The data protection lead will determine if the breach meets the criteria for a formal ICO notification, considering the number of people affected together with the likelihood and severity of the risk to their rights and freedoms. If there is any doubt, the data protection lead will consult the ICO for guidance.

If the breach is considered notifiable, the data protection lead will make a formal notification to the ICO. A record of the report, the outcome, and any necessary remedial action will be recorded.

A chart of this reporting process can be found below:



5.14. Complaints

All complaints about our processing of personal data may be lodged by a data subject directly with the data protection lead, providing details of the complaint. The data subject must be provided with the organisation's privacy notice at this stage.

Complaints may also be made by a data subject directly to the relevant regulatory body:

Information Commissioner's Office
Wycliffe House

Water Lane
Wilmslow SK9 5AF
0303 123 1113

www.ico.org.uk

All complaints in relation to how a complaint has been handled and any appeals following the submission of a complaint shall be dealt with by the data protection lead and the data subject is required to submit a further complaint.

6. Related policies

Data protection principles and practice must be embedded within any of our activities that require processing of personal data. Examples include work with clients and beneficiaries; fundraising, marketing and training for supporters and the general public; staff/volunteer recruitment and management. Consequently, many of our policies and procedures will relate to data protection. The following examples in particular include issues of data protection and where applicable should be read in conjunction with this policy:

- Information Security
- Computer Equipment Security & Clear Desk
- Confidentiality
- Home working
- Safeguarding adults at risk
- Safeguarding children and young people
- Recruitment
- DBS checking procedure
- Whistleblowing
- Equality and diversity
- Compliments, comments and complaints

This list is a guide and not exhaustive, as issues of data protection will arise frequently and personnel need to be alert to new situations where a need to collect, process and/or share personal data arises.

7. Policy review

This policy should be reviewed every year by the Board of Trustees. Upon review, this policy should be submitted to the relevant approving committee for approval.

8. Ownership and control

8.1. Ownership

Responsible (for reviewing & updating the policy)	
Accountable (for making decisions on the policy and for the overall meaning, objectives and compliance with the policy)	
Consulted (for input into changes and updates to the policy)	
Informed (about changes and updates to the policy)	
Approving committee (where approval is necessary as defined by the Policies Terms of Reference document)	

8.2. Control

Date of last review	June 2023
Date of next review	June 2024
Reviewer	
Review outcome	
Submitted for approval to	
Date submitted	

Outcome of approval	
Amends completed	