

Data Protection Policy

Part 1: Introduction

The General Data Protection Regulation (GDPR) regulates the processing of information relating to individuals – both personal data and special categories of data. Personal Data is any information related to a natural person (normally called data subjects) that can be used to directly or indirectly identify the person

Special categories of data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or proceedings for, any offence committed or alleged to have been committed by that person, or the sentence given by any court in such proceedings

During the course of its activities the organisation will obtain, hold, use and disclose personal data about its stakeholders, patients, suppliers, staff and other third parties. North Kent Mind recognises that the correct and lawful processing of this data is important.

The types of personal data that North Kent Mind may process include information about staff (past and present which includes employees, agency staff and consultants), service users, stakeholders, suppliers, and others that it works with, advises or supports. The personal data, which may be held as computerised records as well as manual filing systems, card indexes or other media, is subject to certain legal safeguards specified in the GDPR and other regulations. This policy sets out how North Kent Mind will process all types of personal information to enable it perform its functions in line with legal requirements

Responsibilities

The **Executive Team** is the senior management team that will approve data protection documentation / processes and is accountable for data protection compliance and assurance.

The **Data Protection Officer (DPO)** has overall responsibility for data protection documentation, programme implementation across the organisation and will provide evidence of compliance to the ICO when required. The DPO is also responsible for ensuring that all staff are aware of their data protection responsibilities and is accountable to the Executive Team.

Information Asset Owners are responsible for protecting information in their service areas and will ensure that personal data is collected, used, stored, shared and disposed of in line with the requirements of the Regulation.

All staff are responsible for ensuring that:

- They comply with this policy and all related policies and procedures for handling personal data.
- Any personal data held in either electronic or paper format is processed securely and in line with the requirements of the Regulation.
- Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.
- They promptly forward any form of personal data related requests from data subjects to the data Protection Officer and when asked to do so, they provide responses promptly to requests and reviews.
- Personal data is retained in line with corporate records retention policy/schedule.
- They process personal data in line with intended purposes.
- That the information provided to North Kent Mind in connection with their employment is accurate and as up-to-date as possible.
- Personal data they collect and use to perform their functions is as up-to-date as possible.

Part 2: Data protection principles

The General Data Protection Regulation (GDPR) covers both computerised and manual records which contain personal data, and sets out a number of rights and principles which those who use personal information, such as North Kent Mind, must follow. Data users must comply with the data protection principles of good practice which underpin the Regulation. These state that personal data shall be:

*Processed lawfully, fairly, and in a transparent manner
in relation to the data subject*

1. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archival purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
2. Be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
3. Accurate and where necessary, kept up to date.
4. Kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed.
5. 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.

Fair and lawful processing

The Regulation does not intend to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Regulation. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. Other lawful ground for processing personal data are the protection of the vital interest of the data subject or of another natural person and for the performance of public interest task or the task of an official authority.

When special categories of data are being processed, additional conditions must be met. When processing this class of personal data as data controllers in the course of its business, North Kent Mind will ensure that those requirements are met.

In the course of North Kent Mind's work, it may collect and process personal data to enable it to:

- carry out its regulatory duties including but not limited to the consideration and investigation of complaints and policy issues, formal enforcement actions, providing advice and information
- maintain accounts and records
- support and manage staff,
- send promotional communications about the services provided
- undertake research
- administration of licenses
- maintenance of a public register
- internal and external support functions
- corporate administration
- the use of CCTV systems for crime prevention.

North Kent Mind may process data received directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data received from other sources (including, for example, in Court proceedings, business partners, sub-contractors and others).

North Kent Mind may also from time to time process special categories of data regarding staff or other individuals that it deals with, including:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs

- political opinions, sexual life
- trade union membership
- offences (including alleged offences)
- criminal and legal proceedings, outcomes and sentences.
- genetic and biometric data

This information may be processed for a number of reasons, including but not limited to:

- equal opportunity monitoring
- to meet the needs of individuals with disabilities
- for disciplinary or grievance proceedings
- to fulfil a legal obligation
- and/or to fulfil North Kent Mind's role and function including for purposes of litigation.

Any personal or special categories of data that North Kent Mind holds will only be held for the purposes for which it was gathered. In other circumstances where special categories of data is being processed or held, North Kent Mind will seek the explicit consent of the individual involved unless one of the limited exemptions applies. All staff must be aware and respect their obligations in relation to the confidentiality of special categories of data.

Collected for Specified and Legitimate Purpose(s)

The Regulation aims to ensure that organisations are open about their reasons for obtaining personal data and that personal data is collected in line with the reasonable expectations of the individuals concerned. North Kent Mind will be clear from the outset (at the point of collection) why personal data is collected and what it intends to do with it.

The organisation will comply with the fair processing requirement including the duty to give privacy notices to individuals when collecting their personal data. To this effect, North Kent Mind will provide such notices to data subjects and ensures that when such data is collected its use and disclosure are in line with the requirements of the Regulation.

North Kent Mind will specify the purpose(s) for which it collects, uses, stores, discloses and shares personal data and also ensure that the processing of personal data is not incompatible with the original purpose(s).

Adequate, relevant and Limited Data Processing

North Kent Mind upholds the principle of data minimisation and will only collect personal data to the extent that it is required for the specific purpose notified to the data subject. For the purpose of personal data minimisation, the Regulation specifically mentions pseudonymisation which is the processing of personal data in a way that the data can no longer be attributed to a specific data subject without the use of additional information. North Kent Mind will anonymise and

pseudonymise personal data whenever possible to ensure that data is protected when handled by data users.

Accurate data

North Kent Mind will ensure that personal data it holds is accurate and kept up to date and will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or outdated personal data will be deleted or amended and all reasonable steps will be taken to comply with this principle.

Timely Processing

North Kent Mind holds different types of information for different lengths of time, depending on the legal and operational requirements and will keep some personal information longer than others in line with financial, legal or archival requirements.

North Kent Mind will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. When personal data is no longer needed, it will be disposed of unless there are other legal grounds for retaining the data.

Security of Personal Data

North Kent Mind will ensure that personal data processed in the organisation is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

North Kent Mind will implement/maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality: only people who are authorised to use the data can access it.
- Integrity: personal data will be accurate and suitable for the purpose for which it is processed.
- Availability: authorised users will be able to access the data if they need it for authorised purposes. Personal data will be stored on North Kent Mind's central computer system instead of individual PCs.

North Kent Mind will take the following steps to ensure the security of personal data:

- The pseudonymisation and encryption of personal data;
- Ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Restoration of availability and access to personal data in a timely manner in the event of a physical or technical incident;
- Regular testing, assessment and evaluation of the effectiveness of technical and organisational measures for ensuring the security of the processing.

Approved by CEO 31.5.2019

Next Review May 2020

Page 5

The Accountability Principle

The Regulation has introduced an accountability obligation which requires a proactive and systematic approach to data protection compliance and assurance. North Kent Mind will implement a comprehensive data protection management programme across the organisation and will include an internal governance structure to foster a culture of data protection from top down. Elements of this organisation-wide will be used to demonstrate compliance with the Regulation and these will include:

- Records of data processing activities
- Data Protection impact assessment
- Data breach notification
- Using a Data Processor
- Appointment of a Data Protection Officer

Records of Data Processing Activities

Records of data processing activities will be documented as part of compliance with the accountability principle. The records will comprise of detailed information on all data processing activities that are carried out at the date of the records. The necessary processes will be in place to ensure that those records are updated on an ongoing basis..

Data Protection Impact Assessment (DPIA)

North Kent Mind will carry out Privacy Impact Assessments as and when required.

Privacy Impact Assessments will address the purpose(s) for which personal data is being processed and the processing operations to be carried out with the data. It will assess the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed. An assessment of the risks posed to individual data subjects and details of the measures in place to minimise the risks including safeguards, data security, and other measures to ensure the protection of personal data, will be used to demonstrate compliance with the Regulation.

Data Breach Notification

The Regulation specifically states that reporting data breaches forms part of the accountability principle. In the event of a personal data breach, North Kent Mind will notify the ICO in line with the requirements of the Regulation. Such notice will be provided without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. Where notification of breach is not made within 72 hours, North Kent Mind will provide a reasonable justification for the delay.

Using Data Processors

When North Kent Mind uses data processors to process personal data, such third parties will only process the data on documented instructions of the organisation unless required otherwise by law. Data processors used by North Kent Mind will implement appropriate measures to ensure a level of security appropriate to the risk associated with the type of data they process. North Kent Mind will ensure that its data processors provide information necessary to demonstrate compliance with their obligations under the Regulation.

Appointment of a Data Protection Officer (DPO)

As a public body, North Kent Mind is required to appoint a Data Protection Officer (DPO) to advise the organisation on its obligation under the Regulation and other data protection laws. The DPO will monitor data protection compliance, oversee the documentation of data processing activities provide data protection awareness to staff and conduct data processing internal audits. The DPO will have access to the organisation's data processing personnel and operations with significant independence in the performance of the role.

Rights of Data Subjects

North Kent Mind will process all personal data in line with data subjects' rights. Data subjects including Board and Committee members, staff (past and present), members of the public and individuals who have dealings with North Kent Mind have rights regarding the personal data that is being held about them.

The Regulation gives certain rights to individuals in respect of personal data that North Kent Mind holds about them and these are the:-

- a) Right to be informed
- b) Right of subject access
- c) Right to rectification
- d) Right to data erasure
- e) Right to restrict processing
- f) Right to data portability
- g) Right to objection
- h) Rights with respect to automated decision-making & profiling

Right to be Informed

Data subjects have a right to be informed on how their data is being processed and this is normally referred to as a privacy notice. The Regulation has increased the amount of information that is to be provided in a privacy notice and requires the following information to be included:

- The identity and the contact details of North Kent Mind;
- The contact details of the Data Protection Officer;
- The purposes and legal basis for the processing;
- Where the processing is based on legitimate interests, details of what these are
- The recipients or categories of recipients of the personal data;
- Details of any transfer to a third country and details of the safeguards and the means by which to obtain a copy of them or where they have been made available;
- The retention periods or the criteria used to determine that period;
- Details on rights of access to and rectification/deletion of personal data.
- Rights to object to processing and the right to data portability;
- If processing is based on consent, the right to withdraw consent
- The right to lodge a complaint with the supervisory authority;
- Details on whether the data subject is obliged to provide the personal data and the consequences of failure to provide it;
- Details of any automated decision making, including details of the logic used and potential consequences for the individual.

North Kent Mind will provide privacy notices to data subjects in line with the above requirements at all points of personal data collection.

Right of Subject Access

A data subject may make a subject access request (“SAR”) at any time to find out more about the personal data which North Kent Mind holds about them. The organisation will respond to SARs within one month of receipt but this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject will be informed of the need for the extension.

North Kent Mind will not charge a fee for the handling of normal SARs but reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Right to Rectification

If a data subject informs North Kent Mind that their personal data held by the organisation is inaccurate or incomplete, requesting that it be rectified, the personal data in question will be rectified, and the data subject informed of that

rectification, within one month of receipt the data subject's notice. This can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension.

In the event that any affected personal data has been disclosed to third parties, those parties will be informed of any rectification of that personal data.

Right to Data Erasure

Data subjects may request that North Kent Mind erases the personal data it holds about them.

When such requests are made, unless the organisation has reasonable grounds to refuse to erase personal data, all requests for erasure will be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. This can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension.

In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties will be informed of the erasure unless it is impossible or would require disproportionate effort to do so.

Right to Restrict Data Processing

Data subjects may request that North Kent Mind ceases to process personal data it holds about them. If a data subject makes such a request, the organisation will retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

In the event that any affected personal data has been disclosed to third parties, those parties will be informed of the applicable restrictions on processing it unless it is impossible or would require disproportionate effort to do so.

Right to Data Portability

North Kent Mind processes personal data using automated means. Where data subjects have given their consent to the organisation to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between North Kent Mind and the data subject, they have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes - such as transmitting it to other data controllers.

All requests for copies of personal data will be complied with within one month of the data subject's request but this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject will be informed of the need for the extension.

Right to Objection

Data subjects have the right to object to the processing of their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to the processing of their personal data based on legitimate interests, North Kent Mind will cease such processing forthwith, unless it can be demonstrated that there are legitimate grounds for such processing that override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

Rights in Respect of Automated Decision-Making & Profiling

In the event that North Kent Mind uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the organisation.

The right does not apply in the following circumstances:

- The decision is necessary for the entry into, or performance of, a contract between North Kent Mind and the data subject;
- The decision is authorised by law; or
- The data subject has given explicit consent

Data subjects are entitled to a number of rights with regards to profiling and when North Kent Mind carries out data profiling, it will give effect to those rights of data subjects.

Transferring personal data to a country outside of the EEA

North Kent Mind may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA will take place only if one or more of the following applies:

- a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
- b) The transfer is effected with the use of appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by the ICO; certification under an approved certification mechanism; or provisions

inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;


- c) The transfer is made with the informed consent of the relevant data subject(s);
- d) The transfer is necessary for the performance of a contract between the data subject and North Kent Mind or for pre-contractual steps taken at the request of the data subject;
- e) The transfer is necessary for important public interest reasons;
- f) The transfer is necessary for the conduct of legal claims;
- g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Subject to the requirements outlined above, personal data held may also be processed by staff operating outside the EEA who work for North Kent Mind or for one of its suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details or the provision of support services.

Document Review

The Data Protection Officer is responsible for ensuring this policy remains current and up to date. A current version of this document is available to all members of staff and is published.

This policy was approved by a member of Senior Management and is issued on a version-controlled basis under his signature.

Signature: 

Date: 31st May 2019

Change History Record

Issue	Description of Change	Approval	Date of Issue
1.0	Initial issue	J. Bateman	31 May 2019
1.1	Minor reformatting	J. Bateman	11 Nov 2019