GDPR, Data Protection and storage of information

Nottinghamshire Mind recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 which regulates the use of personal data. This does not have to be sensitive data; it can be as little as a name and address.

The GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information about people, electronically or on paper. Nottinghamshire Mind has also notified the Information Commissioner that it holds personal data about individuals.

When dealing with personal data, Nottinghamshire Mind must ensure that:

Data is processed fairly, lawfully and in a transparent manner – this means that personal information should only be collected from individuals if staff have been open and honest about why they want the information.

Data is processed for specific purposes only – this means data is collected for specific, explicit and legitimate purposes only.

Data is accurate and kept up to date and is not kept longer that it is needed – personal data should be accurate, if it is not it should be corrected. Data no longer needed will be shredded or securely disposed of.

Data is processed in accordance with the rights of the individuals – individuals must be informed, upon request, of all the personal information held about them.

Data is kept securely – there should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Data Breach

GDPR defines a personal data breach as a 'breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed', examples include-

- Access by a third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration or personal data without permission

- Loss of availability or personal data

Nottinghamshire Mind takes the security of personal data seriously, computers are password protected and have up to date security software.

Consequences of a personal data breach

A breach of personal data may result in a loss of control of personal data, discrimination, identify theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore, a breech, depending on the circumstances of the breech, can have a range of effects on individuals.

Nottinghamshire Mind's duty to report a breach

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and ICO without undue delay and where feasible not later than 72 hours after having become aware of the breach. The Data Protection officer must be informed immediately so they are able to report the breach to the ICO in the 72-hour timeframe.

If the ICO is not informed within 72 hours Nottinghamshire Mind via the DPO must give reasons for the delay when they report the breach.

When notifying the ICO of a breach Nottinghamshire Mind must-

- Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categorised and approximately number of personal data records concerned
- Communicate the name and contact details for the DPO
- Describe the likely consequences of the breach
- Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effects.

When notifying the individual affected by the breach, Nottinghamshire Mind must provide the individual with the points above.

Nottinghamshire Mind would not need to communicate with an individual if the following applies-

- It has implemented appropriate technical and organisational measures (i.e. encryption) so those measures have rendered the personal data unintended to any person not authorised to access it
- It has taken subsequent measures to ensure that the high-risk rights and freedoms of individuals is no longer likely to materialise or it would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

Records and Files retention and archive
There is a legal requirement that certain information stored by Nottinghamshire Mind is kept for a minimum of 6 years.

The following will therefore be retained for this period of time from when they cease to be active-

- All financial information including correspondence with the bank and bank statements
- Any legal documents including Trustee minutes
- All personnel information for former members of staff including evidence that
- Income Tax and National Insurance has been properly deducted and appropriate payments made
- All personal information including referral forms and application forms for former Service Users and Volunteers.

Archive files are stored at 6 Hardy Street, Worksop, Notts, S80 1EH and 14St John Street, Mansfield, Notts, NG18 1QT

DBS Disclosure handling and storage
As an organisation the DBS help assess the suitability of applicants for positions of trust, Nottinghamshire Mind fully complies with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of information.

Disclosure information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties. DBS disclosures are retained by the Admin Team at Head Office.

Once employment or volunteering ceases Nottinghamshire Mind will ensure that any Disclosure information is destroyed by secure means, e.g. by shredding, pulping or burning. While awaiting destruction, Disclosure information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack). Nottinghamshire Mind will not keep any photocopy or other image of the Disclosure or any copy or representation of the contents Disclosure. However, with standing the above, we may keep a record of the date of issue of a Disclosure, the name of the subject, the type of disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

Subject Access Request guidance (SAR)'s

This procedure is to followed when an individual contacts Nottinghamshire Mind to request access to their personal information held. Requests must be completed within 1 month, so it should be actioned as soon as it is received. SAR's should be provided free to change, however, you we will charge a 'reasonable' fee when a request is manifestly unfounded or excessive, particularly if it is repetitive.

Steps to action a request

Is it a valued SAR?

- the request must be in writing
- has the person requesting the information provided sufficient detail to allow the information to be located?

Verify the identity of the requestor

- be confident that the person requesting the info is indeed the person it relates too

Determine where the personal information will be found

- consider the type of information requested and the data processing map to determine where the records are stored
- If you do not hold any personal data, inform the requestor, if you do continue to the next step

Screen the information

- some of the information may not be disclosure able due to certain exemptions, however legal advice will be sought before applying any exemptions, for example-
    - references you have given
    - publicly available information
    - management information
    - negotiations with the requestor
    - legal advice and proceedings
    - personal data and third parties

Are you able to disclose all the information?

- In some cases, emails and documents may contain the personal information or other individuals who have not given their consent to share their personal information with others. If this is the case the other individual's personal data must be redacted before the SAR is sent out.

Prepare the SAR response (using the sample letters at the end of this document) and make sure to include as a minimum the following information

- The purpose of the processing
- The categories of personal data concerned
- The recipients or categories of recipients to whom personal data has been or will be disclosed
- Where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object such processing
- The right to lodge a complaint with the information Commissioners office (ICO)
- If the data has not been collected from the data subject, then the source of such data
- The existence of any automated decision making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Be sure to also provide a copy of the personal data undergoing processing.

All SAR's should be logged to include the date of receipt, identity of the data subject, summary of the request, indication of if Nottinghamshire Mind can comply, date the information is sent to the data subject.