



DATA PROTECTION POLICY (GDPR)

December 2022-24


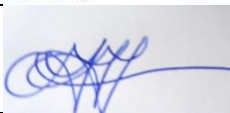


BETHEL HEALTH AND HEALING NETWORK



Document Title	DATA PROTECTION POLICY
Document Purpose:	To ensure that all Bethel staff, volunteers, trustees, contractors and service users understand their rights and responsibilities in relation to data protection.
Document Statement:	Bethel are committed to being fully compliant with all applicable UK data protection legislation in respect of the processing of personal data, as well as safeguarding the “rights and freedoms” of individuals whose information may be processed.
Document Application:	All staff, volunteers, trustees, contractors and service users
Responsible for Implementation:	Data Protection Leads: Senior Operations Manager; Deputy - CEO
Policy Owner:	Data Protection Leads
Status:	Active
Effective Date:	19.12.2022
Review Period:	Bi-annually (in line with legislative guidance)
Associated Documents:	Data Protection, Privacy and Electronic Communications Regulation 2020 (“UK GDPR”); Data Protection Act 2018 (“DPA”); Risk Register; Data Protection Impact Assessment Form (DPIA); Data Protection Activity Log
Associated Policies:	Safeguarding Vulnerable Adult Policy; Children’s Safeguarding Policy; Information and Communications Policy; Data Subject Access Request Policy and Procedure; Recruitment Policy; Complaints Policy

APPROVAL RECORD

Next review by Trustees	Name:	Authorised signature:	Date:
November 2021	Duncan Moore (Chair)		8/12/2021
December 2022	Jennifer Jones-Rigby		19/12/2022
December 2024			



BETHEL HEALTH AND HEALING NETWORK



Contents

1.	Scope.....	4
2.	Introduction.....	4
3.	Policy Aims	4
4.	The Data Protection Principles	5
5.	Good Practice	5
6.	Lawful, Fair, and Transparent Data Processing.....	6
7.	Processed for Specified, Explicit and Legitimate Purposes.....	6
8.	Adequate, Relevant and Limited Data Processing	7
9.	Accuracy of Data and Keeping Data Up to Date	7
10.	Timely Processing	8
11.	Secure Processing.....	8
12.	Accountability	8
13.	Privacy Impact Assessments.....	9
14.	The Rights of Data Subjects.....	10
15.	Keeping Data Subjects Informed	10
16.	Data Subject Access.....	11
17.	Rectification of Personal Data	12
18.	Erasure of Personal Data	12
19.	Restriction of Personal Data Processing	12
20.	Objections to Personal Data Processing	13
21.	Personal Data.....	13
22.	Explicit Consent and Other Conditions for Processing Data	14
23.	Consent – Receiving Information from Bethel.....	15
24.	Parental Consent	15
25.	Legitimate Interest as a Condition for Processing Data	15
26.	Data Security.....	16
27.	Data Protection Measures	16
28.	Organisational Measures	17
29.	Data Breach Notification	18
30.	Staff Training.....	19
31.	Monitoring the Data Protection Policy	19





1. Scope

Bethel Health and Healing Network, hereafter referred to as Bethel, its board of trustees and its senior management team, with a registered address at 196-198 Edward Road, Balsall Heath, Birmingham B12 9LX, and a registered charity number 1116225, are committed to being fully compliant with all applicable UK data protection legislation in respect of the processing of personal data, as well as to safeguarding the “rights and freedoms” of individuals whose information may be processed pursuant to the Data Protection, Privacy and Electronic Communications Regulation 2020 (“UK GDPR”) and the Data Protection Act 2018 (“DPA”) along with any other applicable legislation, hereafter referred to as ‘Regulation’. All policies, procedures and staff guidance developed by Bethel are strictly followed to ensure such processing is lawfully implemented, maintained and periodically reviewed, and where required, amended.

Bethel’s data protection policy framework shall take into consideration the organisation’s management responsibility, organisational structure, jurisdiction and geographical location and as such ensure its obligations to lawful data processing are maintained.

2. Introduction

Bethel Health and Healing Network (Bethel) is a registered charity and limited company offering a range of services to promote the health and wellbeing of the people of Birmingham and the surrounding areas.

At Bethel, we seek to grow as a respected provider of health and wellbeing services and to serve those communities in most need to be physically, emotionally and spiritually healthy. Bethel is a vision and value-led Christian organisation that seeks to reflect this in the way that it operates and communicates, both internally and externally.

3. Policy Aims

This Policy sets out the obligations of Bethel regarding data protection and the rights of employees, service users and suppliers (“data subjects”) in respect of their personal data under all UK data protection laws including The Data Protection, Privacy and Electronic Communications regulation 2020 (UK GDPR), The Data Protection Act 2018 (DPA) and The Privacy and Electronic Communications Regulation (PECR).

UK data protection laws defines “personal data” as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.





This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must always be followed by Bethel, its employees, agents, contractors, or other parties working on behalf of Bethel.

Bethel is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

4. The Data Protection Principles

This Policy aims to ensure compliance with the objectives set out below and are as follows:

- To enable Bethel to broadly meet its data protection obligations in relation to how personal information is managed.
- To demonstrate that Bethel is accountable for such processing in accordance with Article 5 (2) of the UK GDPR.
- To support Bethel's aims and objectives and its legitimate interests to process personal data.
- To safeguard the personal data of Bethel's donors, supporters, and/or members and beneficiaries with which it works along with any other individuals for which Bethel may process data.
- To set appropriate systems and controls according to Bethel's technical and organisational standards.
- To ensure data protection is built into the design of new products and services which include the processing of data, so that data privacy is evidenced by default.

5. Good Practice

Bethel shall always ensure compliance with data protection legislation and good practice by ensuring:

- Processing personal information only when to do so is necessary and there is a demonstrable purpose.
- Ensuring the principles of minimisation are followed and that the least possible amount of personal data is processed, and that personal data is never processed unduly.
- Ensuring the principle of transparency is followed and that individuals are informed of how their personal data is or will be used, by whom and who it may be shared with.
- Processing personal data is fair and proportionate.
- Keeping a record of all categories of personal data processed.
- All personal data that is kept is accurate, up-to-date and rectifiable.
- Retaining personal data no longer than required by statute or regulatory body, or for organisational purposes.
- Where possible, giving individuals the right of 'access' to their data that may directly or indirectly identify them, as well as all other individual rights pertaining to their personal data.





- Ensuring that all personal data is maintained securely in accordance with this policy, both technically and physically.
- Transferring personal data outside of the UK only in situations where it shall be appropriate and where safeguards are in place.
- Applying various statutory exemptions and exceptions, where appropriate, but only where suitable supporting policy allows.
- Implementing a data protection activity/breach incident record, pursuant to this policy.
- Identifying stakeholders, both internal and external, document their responsibilities and any purpose for processing and ensure suitable agreements are in place.
- Identifying personnel that are responsible and appoint a Data Protection Lead or Officer (DPO).

6. Lawful, Fair, and Transparent Data Processing

The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

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 a party or in order to take steps at the request of the data subject prior to 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 data controller. A data controller is a person, company, or other body that determines the purpose and means of personal data processing.
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 fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7. Processed for Specified, Explicit and Legitimate Purposes

Bethel collects and processes the personal data set out in this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us).

Bethel only processes personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected,





where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

8. Adequate, Relevant and Limited Data Processing

Bethel will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as outlined above. Personal data must be adequate, relevant and restricted to only what is required for processing. Bethel will therefore:

- Ensure that personal data which is superfluous and not necessarily required for the purpose(s) for which it is obtained, is not collected.
- Approve all data collection forms, whether in hard-copy or electronic format.
- Carry out an annual review of all methods of data collection, checking that they are still appropriate, relevant, and not excessive.
- Securely delete or destroy any personal data that it is no longer necessary to process in accordance with Bethel's technical and organisational standards.

9. Accuracy of Data and Keeping Data Up to Date

Bethel shall ensure that all personal data collected and processed is kept accurate and up to date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

- Data should not be kept unless it is reasonable to assume its accuracy, and data that is kept for long periods of time must be examined and amended, if necessary.
- All staff must receive training on privacy and data protection. It is the responsibility of the Data Protection Lead/ accountable person to ensure all those that process data for which Bethel is the controller understand the importance of collecting and maintaining accurate personal data.
- Individuals are personally responsible for ensuring that the personal data held by Bethel is accurate and up to date. Bethel will assume that information submitted by individuals via data collection forms is accurate at the date of submission.
- All employees of Bethel are required to update Bethel as soon as reasonably possible of any changes to personal information to ensure records are up to date at all times.
- Bethel (the data controller) must ensure that relevant and suitable additional steps are taken to ensure that personal data is accurate and up to date.
- The Data Protection Lead/ accountable person shall, on an annual basis, carry out a review of all personal data controlled by Bethel and decide whether any data is no longer required to be held for the purpose notified to the ICO, arranging for that data to be deleted or destroyed in accordance with the UK GDPR.
- The Data Protection Lead/ accountable person shall also ensure that where inaccurate or out-of-date personal data has been passed on to third parties, that the third parties are duly informed and instructed not to use the incorrect or out-of-date information as a means for making decisions about the data subject involved. Data Protection Lead/ accountable





person shall also provide an update to the third party, correcting any inaccuracies in the personal data.

10. Timely Processing

Bethel shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

11. Secure Processing

Bethel shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in this Policy.

12. Accountability

Bethel's Data Protection Lead is the Senior Operations Manager. The CEO shall deputise when required.

Bethel shall keep written internal records of all personal data it is collecting, holding, and processing, which shall incorporate the following information:

1. The name and details of Bethel, its Data Protection Lead, and any applicable third-party data controllers.
2. The purposes for which Bethel processes personal data.
3. Details of the categories of personal data collected, held, and processed by Bethel and the categories of data subject to which that personal data relates.
4. Details (and categories) of any third parties that will receive personal data from Bethel.
5. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards.
6. Details of how long personal data will be retained by Bethel.
7. Detailed descriptions of all technical and organisational measures taken by Bethel to ensure the security of personal data.

In accordance with UK data protection laws, Bethel is responsible for ensuring overall compliance and being able to demonstrate that each of its processes is compliant with the UK GDPR requirements. To this extent Bethel is required to:

- Maintain all relevant documentation regarding its processes and operations.
- Appoint an accountable person / data protection lead.
- Ensure Bethel is registered as a controller under the Information Commissioners Office (ICO), if applicable.
- Implement proportionate security measures.





- Train Bethel staff and volunteers in data protection awareness training.
- Ensure it has, and continues to have, up to date data processor and data sharing agreements in place.
- Carry out Data Protection Impact Assessments (DPIAs) and implement the outcome.
- Comply with prior notification requirements.
- Seek approval of relevant regulatory bodies.
- Appoint a Data Protection Officer (DPO), if deemed necessary.
- Seek the opinion of a data protection practitioner, if deemed necessary.
- Publish an accountability statement and a privacy notice in the public domain.

13. Privacy Impact Assessments

It is vital that Bethel is aware of all risks associated with personal data processing and it is via its risk assessment process that Bethel can measure the level of risk. Bethel is also required to carry out assessments of the personal data processing undertaken by other organisations on its 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 using new technologies, or when a high risk is identified in relation to the “Rights and Freedoms” of natural persons, Bethel is required to engage in a risk assessment of the potential impact. More than one risk may be addressed in a single assessment (also known as a ‘**Data Protection Impact Assessment**’ (DPIA)). Bethel will develop and agree upon a procedure for completing a DPIA. This procedure will always be followed where there is a need to measure risk. The procedure is completed by the Data Protection Lead/ accountable person and if necessary, the opinion of a professional GDPR practitioner is taken into account.

In addition to this, and if the outcome of a DPIA points to a higher risk than Bethel intended and personal data processing could result in distress and/or may cause ‘damage’ to data subjects, it is for the Data Protection Lead/ accountable person to decide whether Bethel ought to proceed with the processing, and the matter should be escalated to the individual. In turn, the Data Protection Lead/ accountable person may escalate the matter to the regulatory authority (prior agreement) if significant concerns have been identified.

It is the role of the Data Protection Lead/ accountable person 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 is required by the UK GDPR and this data protection policy.

Bethel takes a cautious approach to risk, it aims to reduce the risks associated with processing personal data as far as possible by following a clear set of policies and procedures, providing training to all staff, and carefully assessing the privacy impact of any new activity.

Bethel shall carry out **Privacy Impact Assessments** when and as required under the Regulation. Privacy Impact Assessments shall be overseen by Bethel’s Data Protection Lead and shall address the following areas of importance:





- The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data.
- Details of the legitimate interests being pursued by Bethel.
- An assessment of 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.
- Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

14. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure (also known as the 'right to be forgotten');
5. The right to restrict processing;
6. The right to data portability;
7. The right to object; and
8. Rights with respect to automated decision-making and profiling.

15. Keeping Data Subjects Informed

Bethel shall ensure that the following information is provided to every data subject when personal data is collected:

1. Details of Bethel including, but not limited to, the identity of its Data Protection Lead.
2. The purpose(s) for which the personal data is being collected and will be processed (as detailed in this Policy) and the legal basis justifying that collection and processing.
3. Where applicable, the legitimate interests upon which Bethel is justifying its collection and processing of the personal data.
4. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.
5. Where the personal data is to be transferred to one or more third parties, details of those parties.
6. Where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place.
7. Details of the length of time the personal data will be held by Bethel (or, where there is no predetermined period, details of how that length of time will be determined).
8. Details of the data subject's rights under the Regulation.
9. Details of the data subject's right to withdraw their consent to Bethel's processing of their personal data at any time.
10. Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation).





11. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it.
12. Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

The information set out above shall be provided to the data subject at the following applicable time:

1. Where the personal data is obtained from the data subject directly, at the time of collection.
2. Where the personal data is not obtained from the data subject directly (i.e. from another party):
 - If the personal data is used to communicate with the data subject, at the time of the first communication; or
 - If the personal data is to be disclosed to another party, before the personal data is disclosed; or
 - In any event, not more than one month after the time at which Bethel obtains the personal data.

16. Data Subject Access

Data subjects have the right to access all personal data in relation to them held by Bethel, whether as manual records or electronic format. Data subjects therefore may at any time request to have sight of confidential personal references held by Bethel as well as any personal data received by Bethel from third parties. To do so, a data subject must submit a Subject Access Request, guidelines for processing this request are circulated to all staff at Bethel, please see “**Data Subject Access Request Policy and Procedure**” for further details.

A data subject may make a subject access request (“DSAR”) at any time to find out more about the personal data which Bethel holds about them. Bethel is normally required to respond to DSARs within one month of receipt (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 shall be informed of the need for the extension).

The purpose of the Subject Access rights is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary.

All subject access requests received must be forwarded to Bethel’s Data Protection Lead(s).

Bethel does not charge a fee for the handling of normal DSARs. Bethel 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.





17. Rectification of Personal Data

If a data subject informs Bethel that personal data held by Bethel is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall 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 shall be informed of any rectification of that personal data.

18. Erasure of Personal Data

Data subjects may request that Bethel erases the personal data it holds about them in the following circumstances:

1. It is no longer necessary for Bethel to hold that personal data with respect to the purpose for which it was originally collected or processed.
2. The data subject wishes to withdraw their consent to Bethel holding and processing their personal data.
3. The data subject objects to Bethel holding and processing their personal data (and there is no overriding legitimate interest to allow Bethel to continue doing so).
4. The personal data has been processed unlawfully.
5. The personal data needs to be erased in order for Bethel to comply with a particular legal obligation.
6. The personal data is being held and processed for the purpose of providing information society services to a child.

Unless Bethel has reasonable grounds to refuse to erase personal data, all requests for erasure shall 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 shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

19. Restriction of Personal Data Processing

Data subjects may request that Bethel ceases processing the personal data it holds about them. If a data subject makes such a request, Bethel shall 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 shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

20. Objections to Personal Data Processing

Data subjects have the right to object to Bethel processing their personal data based on legitimate interests (including profiling) and direct marketing (including profiling).

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

Where a data subject objects to Bethel processing their personal data for direct marketing purposes, Bethel shall cease such processing forthwith.

Where a data subject objects to Bethel processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. Bethel is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

21. Personal Data

The following personal data may be collected, held, and processed by Bethel:

1. Name, telephone numbers, next of kin, emergency contact details and addresses of service users, volunteers, students and staff. This information is kept for contractual reasons, emergencies and quality control.

2. This data may be collected at various stages:

- Service users – referral information, initial assessments, monitoring and evaluation information during and post-support stages
- Staff/volunteers/students – application, interview and during and post-employment/volunteering stages

The UK GDPR covers all personal data processed by Bethel, irrespective of whether this data is held by individual members of staff or clients in their own separate files.

Bethel does collect and process 'special category data'. Bethel directly collects data such as health data, sexual orientation and ethnicity, however more categories of special category data may be indirectly collected when supporting a service user.





The UK GDPR separately defines ‘**special categories of personal data**’ which relates to the following:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious or philosophical beliefs
- Whether they are a member of a trade union
- Their genetic data
- Biometric data used to uniquely identify them
- Their physical or mental health or condition
- Their sex life or sexual orientation

‘Special Categories of personal data’ can only be processed under limited conditions specified in Article 9 of the UK GDPR 2018 in the context of Bethel this would most often be where:

- The individual has given their explicit consent.
- There is a legal requirement to process the information such as immigration, equality requirements or such as in the event of a court case.
- The processing is required for occupational health purposes, absence management or the provision of health or social care services.

22. Explicit Consent and Other Conditions for Processing Data

Explicit consent to the processing of personal data by the data subject must be:

- Freely given and should never be given under duress, when the data subject is in an unfit state of mind or provided on the basis of misleading or false information
- Explicit
- Specific
- A clear and unambiguous indication of the wishes of the data subject
- Informed
- Provided either in a statement or by unambiguous affirmative action
- Demonstrated by active communication between the data controller and the data subject and must not be inferred or implied by omission or a lack of response
- In relation to sensitive data, consent may be provided in writing; if given verbally must be acknowledged in writing, unless there is an alternative legitimate basis for the processing of personal data.

Bethel may collect consent when service users, attendees of events, donors, support participants and supports use its website to engage with Bethel. Bethel’s privacy notice on its website clearly explains the reason and purpose for collecting the data, the legitimate interest of Bethel, the name of the data protection lead, details of its data retention period, information about international transfers, ways to withdraw consent and details of how to complain about Bethel to the ICO. Consent is always collected specifically for the purpose the data will be processed.





23. Consent – Receiving Information from Bethel

In accordance with the UK GDPR 2018, and in particular with the PECR, consent is used when an individual completing a form or by giving Bethel their contact details including their email address. Consent is sometimes used to deliver the services that the charity may provide and to deal with contractual arrangements or to answer a request for information.

Bethel understands that consent is for the time being, and always ensure that individuals are informed of their right to opt-out of future communications whenever they wish. Equally, the right of erasure will be upheld.

24. Parental Consent

Parental or custodial consent is required if/when Bethel is a provider of services to children, defined as being under the age of 13.

25. Legitimate Interest as a Condition for Processing Data

Bethel's vision to enable and empower people to become physically, emotionally, and spiritually healthy. The organisation's mission is to offer a range of holistic services that promote health and wellbeing to people in need.

Bethel uses **Legitimate Interest** as a condition for processing data, and always consider the potential impact on any data subjects whom they may communicate with. The three-stage process that has been implemented is:

1. We measure whether the data subject might reasonably expect us to process their data. For example, if we have had a previous engagement or sent a previous communication with or to the data subject, we believe this might in many cases mean they would expect us to process their data unless they told us not to in the past. This assumes that they did not opt-out of future communications, or object to our marketing or fundraising efforts. However, we also believe that there are occasions other than this where data subjects might understand we would legitimately process their data using this condition.
2. We look carefully to understand whether our Legitimate Interest might impact adversely on the data subject. For example, if a data subject was a person at risk or in a vulnerable circumstance, we would not process their data for marketing purposes. However, we would process their data to provide important information they may require about our services. We have a procedure for ensuring data subjects such as these are suppressed on our data base or forgotten where necessary.
3. Thirdly, we carefully consider whether any safeguards should be in place to protect data subjects against harm when we process their data. We do this by completing a **Legitimate Interest balancing test**. The test measures whether the interests of Bethel outweigh the





rights of the data subjects concerned. The outcome of such a test is documented in the **Activity Log**.

26. Data Security

All employees and volunteers of Bethel are personally responsible for keeping secure any personal data held by Bethel for which they are responsible. Under no circumstances may any personal data be disclosed to any third party unless Bethel has provided express authorisation and has entered into a confidentiality agreement, a data processing agreement or a **data sharing agreement** with the third party. The Data Protection Lead is responsible for this activity.

27. Data Protection Measures

Bethel shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

1. Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely.
2. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.
3. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.
4. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient.
5. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of Bethel requires access to any personal data that they do not already have access to, such access should be formally requested from Bethel.
6. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar.
7. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of Bethel or not, without the authorisation of Bethel.
8. Personal data must always be handled with care and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time.
9. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.
10. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to Bethel or otherwise unless express permission has been given by Bethel and, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.





11. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Bethel where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to Bethel that all suitable technical and organisational measures have been taken).
12. All personal data stored electronically should be backed up regularly with backups stored onsite.
13. All electronic copies of personal data should be stored securely using passwords.
14. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised.
15. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Bethel, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.
16. Where personal data held by Bethel is used for marketing purposes, it shall be the responsibility of Bethel to ensure that data subjects have not added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service.

28. Organisational Measures

Bethel shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

1. All employees, agents, contractors, or other parties working on behalf of Bethel shall be made fully aware of both their individual responsibilities and Bethel's responsibilities under the Regulation and under this Policy and shall be provided with a copy of this Policy.
2. Only employees, agents, sub-contractors, or other parties working on behalf of Bethel that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by Bethel.
3. All employees, agents, contractors, or other parties working on behalf of Bethel handling personal data will be appropriately trained to do so.
4. All employees, agents, contractors, or other parties working on behalf of Bethel handling personal data will be appropriately supervised.
5. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
6. The performance of those employees, agents, contractors, or other parties working on behalf of Bethel handling personal data shall be regularly evaluated and reviewed.
7. All employees, agents, contractors, or other parties working on behalf of Bethel handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract.
8. All agents, contractors, or other parties working on behalf of Bethel handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Bethel arising out of this Policy and the Regulation.





9. Where any agent, contractor or other party working on behalf of Bethel handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Bethel against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

29. Data Breach Notification

All personal data breaches must be reported immediately to Bethel's Data Protection Lead/ or Deputy.

A breach of data protection law will have occurred if data is accessed by an unauthorised party or where the controller has lost control of the data. However, not all such breaches will be reported to the supervisory authority. The decision to report such a breach will be made solely by the data controller. Factors that may determine whether a breach is reportable include:

- Sensitivity of the categories of data. For example, data identifying a health condition.
- Quantity of data concerned.
- Whether there is a potential for a high risk of harm to the data subjects concerned.

Mitigating factors that may be taken into account when not reporting a breach:

- The data is retrievable.
- Evidence that data has been contained and that those who may have access will not process the data in such a way as to cause harm or distress to the data subjects concerned.
- When a data breach must be reported the following procedure will be adopted.
- The accountable person will make the report.
- The report will be made using the ICO's website and in writing.
- The case number supplied by the ICO will be recorded in the activity log.
- Where appropriate the data subjects will be informed however, this will not occur should this cause more distress or harm than the incident itself, the data controller will make this decision.
- Make available any documents or records that the ICO requires to pursue their enquiries.
- Cooperate and assist the ICO.
- Record any guidance the ICO gives in accordance with the breach.
- Undertake risk assessments where required.
- Keep records of the incident.
- Train staff where required in order to ensure the breach doesn't happen again.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the Data Protection Lead must ensure that all affected data subjects are informed of the breach directly and without undue delay. The Data Protection Lead must also notify the Board of Trustees.

Data breach notifications shall include the following information:

Bethel Health and Healing Network
Contact: 0121 661 4276 or email enquiries@bethelnetwork.org.uk
Address: 196-198 Edward Road, Balsall Heath, Birmingham B12 9LX
Company number: 05813084 | Charity: 1116225
Website: www.bethelnetwork.org.uk
Data Protection Policy (GDPR) V3.0 December 2022-24 18





- The categories and approximate number of data subjects concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of Bethel's Data Protection Lead (or other contact point where more information can be obtained).
- The likely consequences of the breach.
- Details of the measures taken, or proposed to be taken, by Bethel to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

It will be the responsibility of Bethel's Data Protection Lead, or their nominee in their absence to determine if the incident needs to be reported to the Information Commissioner's Office, and if so, to report it within 72 hours of being notified of the breach.

30. Staff Training

Staff awareness of the need to protect data is critical to compliance with the law. Therefore, all staff that process personal information are trained in relevant aspects of data processing and security. The training occurs at least annually and is delivered by a data protection practitioner. Should a data protection policy vulnerability be identified, further training may be required.

31. Monitoring the Data Protection Policy

- This Policy will be reviewed biannually by the senior management team and signed off by the Integrated Governance Sub-committee/CEO.
- The latest version of this Policy document dated December 2022 is available to all employees and volunteers of Bethel.

