Data Protection Policy

4net Technologies Ltd Trading as FourNet
3 Scholar Green Road, Cobra Court, Manchester M32 0TR
Tel: 0845 055 6366

Table of Contents

Document Control

Document Title:	002 09 Data Protection Policy
Owner	Stuart Williams
Category:	Restricted
Classification:	ISO Controlled
Version:	5.0
Date:	30.09.25
Review Frequency:	Annually
Next Review Date:	30.09.26

Document Information

The official controlled copy of this manual is the digitally signed PDF document on the FourNet SharePoint® and visible to all authorised users. All printed copies and all electronic copies and versions except the ones described above, are considered uncontrolled copies used for reference only.

This document is controlled as a single entity, as any change, however slight, even a single character, to any part of the document by definition changes the entire document. For this reason, as well as the fact that the concept of "page" varies with the publication format, page-level revision is not practiced with this or any other FourNet document.

Authorisation

Review and Approved for Release:

Document Prepared by: Sarah-Jane Heber-Hall
Head of Compliance

Verified and Authorised by:

Richard Pennington
Chief Executive Officer (CEO)

1. Introduction

This Policy sets out the obligations of FourNet Technologies Limited ("**the Company**"), registered in the United Kingdom under number 05448638, whose registered office is at 3 Scholar Green Road, Stretford, Manchester, M32 0TR, regarding data protection and the rights of customers, employees, and suppliers ("**data subjects**") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("**GDPR**") and Data Protection Act 2018 (the DPA).

The GDPR and the DPA 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 the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company 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.

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR and the DPA. The GDPR and the DPA sets out the following principles with which any party handling personal data must comply. All personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject.
- 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.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 and the DPA in order to safeguard the rights and freedoms of the data subject. and
- 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.

3. The Rights of Data Subjects

The GDPR and the DPA sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

- The right to be informed (Part 13).
- The right of access (Part 14);
- The right to rectification (Part 15);
- The right to erasure (also known as the 'right to be forgotten') (Part 16);
- The right to restrict processing (Part 17); and
- The right to object (Part 18).

4. Lawful, Fair and Transparent Data Processing

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

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The 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 with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The 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; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data 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.
- FourNet also acknowledge the need to comply with Article 40 GDPR Codes of Conduct, and our Data Protection Policy has been aligned to meet the fundamental requirements of this code of conduct. We also work hard to comply with other specific European and global data protection related legislation, as required during the course of our business activities.

5. Special Category Data

If the personal data in question is "special category data" (also known as "sensitive personal data"), for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation, at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
- The processing relates to personal data which is clearly made public by the data subject;
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR and the DPA;
- The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR and the DPA based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

6. Specified, Explicit and Legitimate Purposes

The Company collects and processes the personal data set out in Part 20 of this Policy. This includes:

- Personal data collected directly from data subjects;
- The Company only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR and the DPA); and
- Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 14 for more information on keeping data subjects informed.

7. Adequate, Relevant and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above and as set out in Part 20, below.

8. Accuracy of Data and Keeping Data Up-to-Date

The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 15, below.

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

9. Data Retention

The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For Formal Documentation used within the Business, that may contain staff names, this is archived once superseded and then deleted after 24 months.

For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Privacy Policy.

10. Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 20 to 27 of this Policy.

11. Accountability and Record-Keeping

- The Company has a Data Protection Lead, they can be contacted via a dedicated email address– dpo@fournet.co.uk.
- The Data Protection Lead shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies and with the GDPR, the DPA and other applicable data protection legislation.
- The Company shall keep written internal records of all personal data collection, holding and processing, which shall incorporate the following information:
- The name and details of the Company, its Data Protection Lead and any applicable third-party data processors;
- The purposes for which the Company collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the Company and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Company (please refer to the Company's Data Privacy Policy); and
- Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

12. Data Protection Impact Assessments

The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.

Data Protection Impact Assessments shall be overseen by the Data Protection Lead and shall address the following:

- The type(s) of personal data that will be collected, held, and processed;
- The purpose(s) for which personal data is to be used;
- The Company's objectives;
- How personal data is to be used;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to the Company; and
- Proposed measures to minimise and handle identified risks.

13. Keeping Data Subjects Informed

The Company shall provide the information set out in Part 14.1 to every data subject:

- Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
    - if the personal data is used to communicate with the data subject, when the first communication is made; or
    - if the personal data is to be transferred to another party, before that transfer is made; or
    - as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

13.1 Information Provided

The following information shall be provided:

- Details of the Company including, but not limited to, the identity of its Data Protection Lead;
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 20 of this Policy) and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;
- Details of data retention;
- Details of the data subject's rights under the GDPR and the DPA;
- Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;
- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR and the DPA);
- 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; and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions and any consequences.

14. Data Subject Access

Data subjects may make Subject Access Requests ("**SARs**") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data and why.

Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection related dedicated email address - dpo@fournet.co.uk.

Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

All SARs received shall be handled by the Company's Data Protection Lead.

The Company does not charge a fee for the handling of normal SARs. The Company 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.

15. Rectification of Personal Data

Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

The Company shall rectify the personal data in question and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

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

16. Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
- The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);
- The personal data has been processed unlawfully; and
- The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

Unless the Company 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. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject's 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).

17. Restriction of Personal Data Processing

Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

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).

18. Objections to Personal Data Processing

Data subjects have the right to object to the Company processing their personal data based on legitimate interests and direct marketing.

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

Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

19. Personal Data Collected, Held and Processed

The following personal data is collected, held, and processed by the Company (for further details please refer to the Company's Data Privacy Policy (002_08): The Data Retention information from this policy can be found under section 20

Data Ref.	Type of Data	Purpose of Data
Customer	Name	Contacting Customer for the purpose of executing the contract and/or order
Customer	Business Telephone Numbers	Contacting Customer for the purpose of executing the contract and/or order
Customer	Business Email Addresses	Contacting Customer for the purpose of executing the contract and/or order
Customer	Business Postal Addresses	Contacting Customer for the purpose of executing the contract and/or order
Customers Staff	Name	To build an internal telephone directory for the customers staff
Customers Staff	Business Telephone Numbers	To build an internal telephone directory for the customers staff
Supplier	Name	Contacting Supplier for the purpose of executing the contract and/or order
Supplier	Telephone Numbers	Contacting Supplier for the purpose of executing the contract and/or order
Supplier	Email Addresses	Contacting Supplier for the purpose of executing the contract and/or order
Supplier	Postal Addresses	Contacting Supplier for the purpose of executing the contract and/or order
Customer	Voice Recordings	In some cloud-based services FourNet will use a purpose-built voice recorder in order to record calls for training or legislative purposes. FourNet do not access this data unless specifically requested to do so. This data is stored and protected in line with our security policies.
FourNet Staff	Name	Used to execute the employment contract between FourNet and that staff member.
FourNet Staff	Telephone Numbers	Used to execute the employment contract between FourNet and that staff member.
FourNet Staff	Addresses	Used to execute the employment contract between FourNet and that staff member.

Data Ref.	Type of Data	Purpose of Data
FourNet Staff	National Insurance Number	Used to execute the employment contract between FourNet and that staff member.
FourNet Staff	PAYE Information	Used to execute the employment contract between FourNet and that staff member.
FourNet Staff	Medical Information	Used to execute the employment contract between FourNet and that staff member.
FourNet Staff	DBS and Security Clearance details	DBS Certificates considered only for the purpose of role-based requirements for which it was obtained, and then destroyed within 6 months. Security Clearance details obtained for the duration that they are valid for and held securely within an asset portal with restricted access that is regularly monitored and updated.
Prospective Customers	Name	Contacting Prospective Customers for the purpose of sales and marketing activities
Prospective Customers	Job Title	Contacting Prospective Customers for the purpose of sales and marketing activities
Prospective Customers	Business Telephone Numbers	Contacting Prospective Customers for the purpose of sales and marketing activities
Prospective Customers	Business Email Addresses	Contacting Prospective Customers for the purpose of sales and marketing activities
Prospective Customers	Business Postal Addresses	Contacting Prospective Customers for the purpose of sales and marketing activities

Note: FourNet DO NOT/WILL NOT store personal contact numbers, email, or postal addresses unless this has been explicitly requested to by the data subject for business related activities.

20. Data Retention

We will not keep your personal data for any longer than is necessary in light of the reason(s) for which it was first collected. Your personal data will therefore be kept for the periods laid out in table 1, shown below.

For Formal Documentation used within the Business, that may contain staff names, this is archived once superseded and then deleted after 24 months.

Please note that financial data is held for a period of up to seven years, where practicable to do so. personal data is removed from this type of data before it is archived.

Data Subject	Data Type	Retention Period
Customer	Contact Details	For the duration of the contract plus 24 months.
Supplier	Contact Details	For the duration that the supplier remains on the FourNet approved supplier list plus 24 months.
Staff	Personnel Records and Contact Details including H & S and First Aid training, as well as information required to authorise financial payments, like Business Travel and mileage claims and allowances. DBS Certificate Information	For the duration of employment plus 72 months, to cover the time limit for bringing any civil legal action. All emails and IM's will be deleted after 3 months from the date of leaving. Ongoing deletions of emails and IM's will be retained for 12 months only within backups. Only for the purpose for which it was obtained, and then destroyed within 6 months.
Accident Books , accident records / reports	Incident information	3 years from the date of last entry for all people over 18.
Subject Access requests	Data Protection Information	1 year following completion of the request.
Prospective Customer	Contact Details	24 months unless the Customer opts out, in which case the data will be deleted immediately.
Visitors	Contact Details	24 months

21 Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing personal data must be encrypted. Methods of encryption are detailed with in the FourNet Statement of Applicability to the ISO 27001 standard.
- All emails containing personal data must be marked "confidential;"
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable; and
- 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.

22 Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords and data encryption;
- 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;
- All personal data stored electronically is be backed up daily and encrypted;
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of Richard Pennington, Chief Executive Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given and for no longer than is absolutely necessary; and
- 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 the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR and the DPA (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

23 Data Security - Disposal

When 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. For further information on the deletion and disposal of personal data, please refer to the Company's Data Privacy Policy.

24 Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Lead;
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation from the Data Protection Lead;
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- 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; and
- Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Chief Marketing Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

25 Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security further information about FourNet's IT Strategy and Security can be found in the ISO27001 Statement of Applicability:

- 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, in line with FourNet's Password Policy
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, 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;
- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and

- No software may be installed on any Company-owned computer or device without the prior approval of the Chief Technical Officer.

26 Organisational Measures

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

- All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and the DPA and under this Policy and shall be provided with a copy of this Policy;
- Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to and use of, personal data in order to perform their assigned duties correctly shall have access to personal data held by the Company;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Privacy Policy;
- The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and the DPA and this Policy by contract;
- All agents, contractors, or other parties working on behalf of the Company 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 the Company arising out of this Policy and the GDPR and the DPA; and
- Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

27 Data Breach Notification

All personal data breaches must be reported immediately to the Company's Data Protection Lead.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g., financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Lead must ensure that the Information Commissioner's Office is informed of the breach without delay and in any event, within 72 hours after having become aware of it.

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 29.2) 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.

Data breach notifications shall include the following information:

- 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 the Company's data protection officer (or other contact point where more information can be obtained);
- The likely consequences of the breach; and
- Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

28 Information Commissioner's Office Notification

Additionally, Fournet must notify the Information Commissioner's Office in writing without undue delay and no later than 72 hours after first becoming aware about any incident which has an actual adverse effect on the security of network and information systems that results in a substantial impact on the provision of the services to its Customers. The notification must contain:

1. Fournet's name and the services it provides;
2. The time the incident occurred;
3. The duration of the incident
4. Information concerning the nature and impact of the incident;
5. Information concerning any, or any likely, cross-border impact of the incident; and
6. Any other information that may be helpful to the Information Commissioner's Office.

29 Information Security Incident Management

Staff must acquaint themselves with the Company's Information Security Incident Management Policy as detailed in document reference 002 39 Information Security Incident Management Policy. This is with regards to any information security risk, weakness or event that may compromise this Data Protection Policy.

30 Enforcement

Any member of staff found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. In certain circumstance, investigation by regulatory bodies and or the police may apply.

31 Communicating FourNet's Policies

Relevant training, bulletins, education materials, policies, procedures, and processes are provided on an ongoing basis to all employees to ensure they are fully aware of their responsibilities and are kept up-to-date of any new requirements. These are communicated in a number of ways, including, but not limited to:

- Induction sessions;
- PDR meetings;
- Company meetings;
- Atlas/Citation portal; and
- Regular company bulletins via Microsoft Teams.

32 Review and Ownership of This Policy

This policy will be reviewed and amended as required, and at least annually by the Data Protection Lead and Head of Compliance. This document is managed by the ISO review process and, as such any revisions will be authorised at Board Level prior to general release.

This policy document is ISO controlled and as such, the source document will be stored in the secure area of the FourNet ISO SharePoint® and a PDF version in FourNet Open Access ISO Documents PDFs folder, sub-folder 002 Policies.

Change History

Date	Version	Brief Description	Author
10.04.17	0.1	Initial Draft	Toni Hazlewood
23.06.17	0.2	For Board Review	Matt Dawe
21.09.17	0.3	Amendments Following Board Review	Toni Hazlewood
05.01.18	1.0	First Release	Matt Dawe
03.01.19	2.0	Annual Review	Matt Dawe
06.07.20	3.0	FourNet Rebranding/Updates	Toni Hazlewood
11.10.20	4.0	Renumbered in line with ISO Documentation Policy	David O'Brien
04.12.20	4.1	Information Security Incident Management	David O'Brien
17.11.21	4.2	Annual Review	David O'Brien
20.12.21	4.3	Inclusion of ICO Notification	David O'Brien
15.09.22	4.4	Annual Review	Sarah-Jane Heber-Hall
09.03.23	4.5	Inclusion of Data retention details from Data Privacy Policy under Section 20.	Sarah-Jane Heber-Hall
20.09.23	4.6	Inclusion of DBS certificate retention periods for staff	Sarah-Jane Heber-Hall
08.11.23	4.7	Review of staff email retention amendment to Data Retention Table	Sarah-Jane Heber-Hall
02.10.24	4.8	Annual Review	Sarah-Jane Heber-Hall
09.04.25	4.9	Review of definition for our Data Protection lead	Sarah-Jane Heber-Hall
20.09.25	5.0	Reference added to GDPR Code of Conduct and other European and global GDPR related legislation	Sarah-Jane Heber-Hall