OnPath Policy

Data Protection Policy

Background

The UK GDPR (as defined below) requires all organisations which handle personal information to comply with a number of principles regarding privacy and disclosure.

The UK GDPR states that anyone who processes personal information must comply with six principles.

These state that information must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not used in a manner which is incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate and, where necessary, up to date;
- kept for no longer than is necessary; and
- used in a way which ensures it is kept secure and protected from unauthorised and unlawful processing and accidental loss or damage.

This internal data protection policy (Policy) describes how Personal Data must be collected, handled, stored, disclosed or otherwise processed by OnPath Energy employees and other personnel to meet OnPath Energy's data protection standards and to comply with application data protection legislation. The meaning of the terms Personal Data and processing is provided in the Key Terms section below.

Published by OnPath Energy : April 2024

Scope

In this Policy, **OnPath Energy, we** or **us** means OnPath Energy Limited or the relevant OnPath entity that is collecting, handling, storing, disclosing or otherwise processing Personal Data. OnPath Energy is required to maintain certain Personal Data about living individuals for the purposes of fulfilling operational and legal obligations.

OnPath Energy is committed to fulfilling its obligations under the applicable data protection legislation in respect of all processing of Personal Data in connection with its business and in so doing, meeting the expectations of our employees, customers, suppliers and local communities.

This Policy outlines the way in which we process Personal Data to promote a proactive approach to data protection compliance. It deals with our roles and responsibilities when handling the Personal Data that we process regardless of the media on which that Personal Data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, complainants, local community representatives, or any other Data Subject (as defined below).

All OnPath Energy staff (including directors, officers, contractors or consultants) who have access to or otherwise process any Personal Data held by or on behalf of OnPath Energy must adhere to this Policy. Such compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action. It may also result in us breaching the UK GDPR or other legal requirements. Enforcement action under UK GDPR may include fines and criminal prosecution and we could also have compensation claims made against us by individuals if we breach these laws. Claims and enforcement action can also generate significant negative publicity. This Policy is an internal document and should not be shared with third parties, including clients, without prior authorization.

OnPath Energy is required to ensure that all staff have undergone adequate training to enable them to comply with Data Protection Legislation. All staff must undergo all mandatory data protection training and related training as directed by HR.

OnPath Energy will ensure that there is someone within the organisation with specific responsibility for data protection the Data Protection Manager, and that they are appropriately trained to meet their duties.

Please note, in October 2023, OnPath Energy (previously trading as Banks Renewables) was acquired by Brookfield Renewable Partners L.P. together with institutional partners (Brookfield). OnPath Energy is currently utilising the services of The Banks Group Limited (company number 02267400) during a transitional period following the acquisition by Brookfield. This Policy and the contact details below will be updated following the end of this transitional period which is expected in June 2024. For more information, please contact us using the details below.

Any questions about the operation of this Policy, or any concerns that this Policy has not been followed, should be referred in the first instance to our current Data Protection Manager, whose contact details are:

Telephone: +44 330 335 8010

Email: privacyofficer@onpathenergy.com
Post: FAO: Data Protection Manager
OnPath Energy Limited,
Chase House,
4 Mandarin Road,
Houghton-Le-Spring,
DH4 5RA

We keep this Policy under regular review and it may be amended from time to time.

Key Terms

Some of the key terms used in this Policy are:

Controller	the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. For example, we are the Controller of all Personal Data relating to our personnel and our customers and suppliers.
Criminal Records Data	Personal Data relating to criminal convictions and offences, including Personal Data relating to criminal allegations, investigations and proceedings.
Data Subject	means the person to whom the Personal Data relates. For simplicity, in this Policy, we sometimes refer to these people as **individual** or **individuals.**
Personal Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. process or processing any use of, or activity carried out in relation to Personal Data, including collecting, recording, organising, storing, retrieving, altering, using, disclosing and destroying Personal Data. **Processed** shall be construed accordingly.
UK GDPR	the European General Data Protection Regulation (EU 2016/679) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 European Union (Withdrawal) Act 2018.

What is Personal Data?

Certain Personal Data is considered to be particularly sensitive and is subject to stricter rules regarding its processing. Under the UK GDPR, these categories of Personal Data are referred to as Special Category Personal Data and include:

- the racial or ethnic origin of the Data Subject;
- their political opinions;
- their religious beliefs or other beliefs of a similar nature;
- whether they are a member of a trade union or similar association;
- their physical or mental health or condition;
- their sexual life/orientation;
- their genetic or biometric data;
- details of any offence or alleged offence committed by them; or
- details of any court proceedings for any offence committed or alleged to have been committed by them.

Lawfulness, Fairness and Transparency

Personal Data must be processed fairly, lawfully and in a transparent manner.

We may only collect, process and share Personal Data fairly and lawfully for a specified lawful basis as set out in the UK GDPR. The list below identifies the lawful bases which are most likely to apply to us:

- the processing is necessary for the performance of a contract with the individual or to take steps at the request of the individual before entering into a contract;

- to meet our legal obligations;

- to pursue our legitimate interests, except where the processing prejudices the interests or fundamental rights and freedoms of individuals; or

- the individual has given consent to the processing; the requirements for obtaining a valid consent are explained below; where possible, you should seek to rely on an alternative ground to consent.

The other lawful bases are that the processing is necessary in order to protect the vital interests of an individual, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in a Controller. These are less likely to be relevant to our day-to-day processing and in some cases may never apply.

For each purpose that you use Personal Data you must identify a lawful basis. If you are in any doubt about which legal basis applies to the processing, please contact our Data Protection Manager for further advice and guidance.

Special Category Personal Data and Criminal Records Data

We must treat Special Category Personal Data very carefully and additional rules apply. We still need to have a lawful basis for processing Special Category Personal Data based on those noted in this Policy above, but we also need an additional justification for processing it drawn from a separate list in the UK GDPR and the Data Protection Act 2018. The justifications that are most likely to be relevant are:

- where the processing is necessary for employment or social security purposes (if authorised by law);

- where the processing is necessary for the establishment, exercise or defence of legal claims;
- where the processing is necessary for reasons of substantial public interest set out in national law; or

- the individual has given their valid and explicit consent to the processing.

Similar to the processing of Special Category Personal Data, an extra layer of rules applies when we process Criminal Records Data. This may happen when we are checking the suitability of taking on an individual to work for us. If you have any questions or concerns in relation to the processing of Criminal Records Data, you should contact our Data Protection Manager as soon as possible.

Consent

We are only able to rely on consent as a lawful basis where an individual clearly indicates that they agree, either by a statement or other positive action. For consent to be valid, it must:

- be granted via an affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be sufficient;

- be limited to specific processing activities and the individual must have been informed in sufficient detail about the processing activities so as to be able to fully understand what they are consenting to;

- if consent is given in a document which deals with other matters, be separate from those;

- not be a condition for the performance of a contract , unless the data processing is required in order to perform the contract.

Individuals must have the ability to easily withdraw consent to processing at any time and any withdrawals of consent should be dealt with promptly. Where there is any processing of Personal Data for a reason which was not covered by the consent, either a fresh consent will need to be obtained from the individual or you will need to satisfy an alternative lawful basis.

Consent must be recorded and you must be able to provide evidence that all consents have been obtained. As obtaining and providing evidence of consent is not straightforward, you should consider if it is appropriate to rely on consent as your lawful basis for processing and instead rely on a different lawful basis. It is also particularly difficult to use consent when carrying out employment related processing, given the imbalance of power in the relationship between employers and employees. If you wish to use consent as your lawful basis, you should contact our Data Protection Manager before any processing takes place and before asking for consent.

Transparency Information

We must give individuals very specific information about how we process their Personal Data. This information includes identifying the Personal Data we use, the purposes for which we use it and who we share it with. We provide this information to individuals through our privacy notices.

You should check that the way you are using Personal Data is covered by the purpose detailed in the privacy notices and that all relevant information concerning that processing has been provided within the notices. If it is not, you should refer to our Data Protection Manager who will then consider the processing and will take the appropriate action.

If we obtain Personal Data about an individual from a third party and not directly from the individual, we must also in most circumstances provide the individuals with a privacy notice which explains the same information to them as if we had collected their Personal Data directly. This notice should be provided within a reasonable period after collection and within one month at the latest.

Specified Purpose

Personal Data must be collected only for specified, explicit and legitimate purposes that are communicated to the individual. It must not be further processed in any manner incompatible with those purposes.

We can generally only use the Personal Data for a new purpose if either:

- this is compatible with the original purposes disclosed to the individual when it was first obtained;

- we get consent specific to that new purpose; or

- we have a clear obligation or function set out in law allowing the new use.

If you plan on using any Personal Data for a new purpose, you should contact our Data Protection Manager for further advice and guidance.

Adequate, Relevant and Not Excessive

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Do not collect

or retain Personal Data that is just "nice to have". It should be the minimum necessary for the purpose.

You should ensure that when Personal Data is no longer needed for the specified purposes, it is destroyed in accordance with our Record Retention Policy. You may only process Personal Data if and when the performance of the duties of your role requires it. You should not process Personal Data for any reason unrelated to the duties of your role.

Accuracy

We must keep Personal Data accurate, complete and up to date and reasonable steps should be taken to delete or rectify inaccurate Personal Data. The most appropriate way to do this is to check with the individual that their Personal Data is correct at the time it is collected and at regular intervals afterwards.

Where appropriate, you should assess the accuracy of Personal Data at the time of collection from sources other than the individual. It is more likely to be appropriate to do this the more important it is that the Personal Data is accurate (e.g. if you are using it to make decisions that affect an individual).

You must update Personal Data as soon as practicable after becoming aware that it is inaccurate, incomplete or out of date, and ensure that the updates are made across all relevant records and systems. If this is not possible, you must take reasonable steps to destroy the Personal Data.

Kept For No Longer Than Is Necessary

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the Personal Data is processed, including for the purpose of satisfying any legal, accounting or reporting requirements.

You should ensure that when Personal Data is no longer needed for the specified purposes, it is deleted or anonymised in accordance with our Record Retention Policy. Our privacy notices include details for individuals as to how long their Personal Data is held.

Greater care needs to be taken to ensure that Special Category Personal Data and Criminal Records Data is not retained for longer than is necessary given the risks associated with storing and using this Personal Data.

Handling of Personal Data and Special Category Personal Data

In order to meet the requirements of the UK GDPR, OnPath Energy will:

- observe and comply with the conditions regarding the fair collection and use of personal information;
- meet its legal obligations to specify the purpose for which information is used;
- collect and process Personal Data only to the extent that is needed to meet operational and legal requirements;
- ensure the quality of information used;
- apply checks to determine the length of time Personal Data is held, and dispose of it confidentially once its retention period has elapsed;
- take the appropriate security measures to safeguard the Personal Data it maintains to minimise the risk of unauthorised disclosure or loss;

- ensure that requests to access Personal Data are dealt with efficiently and within the statutory timescale; and

- ensure that Personal Data is not transferred out of the UK without suitable safeguards.

Sharing Personal Data with Third Parties

Generally, under the UK GDPR, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. Third parties may need access to the Personal Data that we process, for example as part of providing services to us. Before sharing any Personal Data with a third party or considering engaging a supplier to process Personal Data on our behalf, please contact our Data Protection Manager for further advice and guidance on how to ensure this complies with the UK GDPR.

An individual must not be credit-checked (or any personal information passed to credit reference agencies) except with the consent of that individual.

Individual Rights and Access to Personal Data
Under the UK GDPR, individuals have rights in relation to information processed about them. This could be on computer or in paper records.

These include the right to:

- receive certain information about our processing activities – included in our privacy notices;

- access – individuals are entitled to receive confirmation from us as to whether or not we are processing their Personal Data and, if we are, to access it and be provided with certain information in relation to it (referred to as a subject access request). For more information on how individuals can exercise this right, please see OnPath Energy's Subject Access Requests Procedure document;

- rectification – individuals can, subject to certain requirements and limitations, require us to correct any inaccuracies in the Personal Data we hold on them without undue delay;

- erasure – subject to certain requirements and limitations, individuals can require us to erase their Personal Data;

- restriction of processing – in certain circumstances individuals can require us to restrict processing;

- data portability – in certain circumstances individuals can receive the Personal Data in a structured, commonly used machine-readable format so that it can be transferred to another company;

- object or challenge processing – if we are processing Personal Data on the grounds of it being necessary for the performance of a task carried out in the public interest or being necessary for our legitimate interest, individuals have the right to object to our processing their Personal Data, subject to certain limitations;

- withdraw consent – individuals have the right to withdraw their consent to our processing of their Personal Data at any time;

- object to direct marketing – individuals may object to the use of their Personal Data for direct marketing purposes;

- request a copy of an agreement – individuals may request a copy of the agreement under which Personal Data is being transferred outside of the UK;

- object – individuals can object to decisions based on any automated processing;

- prevent processing that is likely to cause damage or distress to an individual or anyone else;
- be notified of a Personal Data Breach – individuals should be notified where a Personal Data Breach is likely to result in a high risk to the individual's rights and freedoms; and

- complain – individuals have the right to complain to the appropriate regulatory authority.

If you receive any communication (either verbally or in writing) from an individual in relation to our use of their Personal Data, or from another person or body (including the Information Commissioner's Office (ICO)), you must immediately forward any request from an individual you receive to our Data Protection Manager who will consider the request, consulting with the appropriate team if necessary and prepare an appropriate response.

You must not allow a third party to persuade you to disclose Personal Data without proper authorisation.

Exempt Information

Access to personal information is subject to a number of exemptions which are:

- confidential references provided by the organisation. References received by the organisation are not automatically excluded but may be similarly protected as disclosing information relating to identifiable third parties as set out below;

- Personal Data processed for the purposes of management forecasting or management planning to the extent that disclosure would be likely to prejudice the conduct of that business only;

- Personal Data which consists of records of the intentions of the organisation relating to any negotiations with the employee to the extent that disclosure would be likely to prejudice those negotiations only; and
- information relating to an identifiable third party (person, not business). Disclosure is not required unless the third party has consented to the disclosure, or it is reasonable to comply with the request without third party consent. Failing this, the data must be edited prior to disclosure so that the identity of third parties is not apparent. If the information being sought is a health record and the third party is a health professional that has compiled or contributed to that health record then disclosure should be made.

Data Protection and OnPath Energy Employees

Initial Personal Data relating to employees is ordinarily obtained from job application forms submitted to the organisation and thereafter principally from employees themselves by way of annual appraisal. A statement on the organisation's standard application form and terms and conditions of employment clearly outlines that the data collected will be strictly confidential and used only for the purposes of personnel and salary administration or otherwise in connection with the company's business.

Requests made by external sources, for data concerning OnPath Energy employees which have been authorised by the organisation are:

- requests from agents authorised by the employee who is the subject of the data, e.g. mortgage requests or references. However, confirmation should be sought from the employee that the information is to be released and if possible the employee's written consent should be obtained;

- requests made for the purposes of law enforcement (i.e. for the prevention and detection of crime, the assessment or collection of any tax or duty or the assessment or collection of any liability via the Child Support Agency). Disclosure is only allowed where failure to make disclosure would be likely to prejudice one of those purposes. In all cases written evidence should be obtained from, as applicable, the Police, Inland Revenue, Customs and Excise and/or the Child Support Agency as to the purpose of the request;

- requests for any other compulsory legal processes;

- requests, if urgently required, for the prevention of injury and damage to health;

- requests required by authorised officials or representatives of recognised trade unions. However, confirmation should be sought from the employee that the information is to be released and if possible the employee's written consent should be obtained; and

- requests required by specifically identified external sources, e.g. pension administrators, in order to administer internal company benefit schemes.

Security

We are required by law to have appropriate technical and organisational security measures in place to prevent unauthorised or unlawful processing, and against accidental loss, destruction, damage, access, use or disclosure. We will have and continue to develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable).

You are responsible for protecting the Personal Data we hold. You must follow the procedures we set out to protect the Personal Data we hold from unlawful or unauthorised processing and against the accidental loss of, destruction or damage to that Personal Data. You must exercise particular care in protecting Special Category Personal Data and Criminal Records Data from unauthorised or unlawful processing against accidental loss, destruction, damage, access, use or disclosure. You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;

- integrity means that Personal Data is accurate and suitable for the purpose for which it is processed; and

- availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of our Information Security Policy and Data Security Breach Procedure. You should not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect Personal Data.

Notification of a Personal Data Breach to the ICO

If a Controller becomes aware of a Personal Data Breach in relation to Personal Data for which the Controller is responsible, the Controller must notify the breach to the ICO without undue delay and where feasible not later than 72 hours after becoming aware of it. In certain instances, the Controller may also have to notify any affected individuals.

This does not apply if the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of individuals.

If you discover or suspect that a Personal Data Breach has occurred you must follow our Data Security Breach Procedure and immediately report such Breach to the Data Protection Manager.

Accountability and Record Keeping

We are responsible for, and must be able to demonstrate, compliance with the data protection principles. In practice this means that we need to be proactive and organised about our approach to data protection and evidencing the steps that have been taken to comply.

OnPath Energy's Personal Data inventory log is a log of all the types of Personal Data we process, why we process it, who we share it with and how long we keep it. The log is administered by the Data Protection Manager, and can be disclosed to the ICO in the event of an audit or investigation.
If an employee of OnPath Energy creates their own system or record for example a spreadsheet or database, whether electronic or on paper, for the purpose of processing Personal Data, this must be notified to the Data Protection Manager. The Data Protection Manager will ensure it complies with the requirements under the UK GDPR and that appropriate security is applied to it.

Provided that the identification of individuals cannot be ascertained or is not disclosed, aggregate or statistical information may be used to respond to legitimate internal or external requests for data, such as surveys, and manpower figures.

Privacy By Design and Data Protection Impact Assessment (DPIA)

In certain circumstances we are required to implement privacy by design measures when processing Personal Data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with the data protection principles (described in this Policy above).
Privacy by design means that, for example, when considering new purposes for processing Personal Data or implementing new technology, you need to consider the impact the processing will have on individuals for the whole lifecycle of the processing (i.e. from start to finish of the processing of the Personal Data).

We must assess what privacy by design measures can be implemented on all programs / systems / processes that process Personal Data by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of processing; and
- the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing.

Controllers must also conduct a DPIA in respect of high-risk processing. Some potential examples of high-risk processing include, systematic and extensive profiling with significant effects on individuals; when processing biometric data; or data matching by combining, comparing or matching Personal Data obtained from multiple sources.

Before implementing major systems or business change programs involving the processing of Personal Data, a DPIA may be required and you should contact our Data Protection Manager to conduct it.

Direct Marketing and Personal Data

In addition to the UK GDPR there are other rules and privacy laws that apply when direct marketing to our customers and other stakeholders. These are complex and vary depending on the method of marketing (for example, marketing by email, text or automated calls) and the type of recipient (for example, private individuals or corporate bodies and their personnel).

OnPath Energy may use an individual's Personal Data to form a view on what we think they may want or need, or what may be of interest to them. This is how we decide which developments, products, services and offers may be relevant for individuals (we call this marketing). Individuals may receive marketing communications from us if they have requested information from us, supported our energy developments, or purchased similar goods or services from us in the past and they have not opted out of receiving that marketing. We will get your express opt-in consent before we share an individual's Personal Data with any third party for marketing purposes. An individual can ask us or third parties to stop sending them marketing messages by contacting OnPath Energy at any time. Where an individual decides to opt out of receiving these marketing messages, this will not apply to Personal Data provided to us as a result of their support for an energy development, a product/service purchase, product/service experience or other transactions.

If you require further information about direct marketing you should contact Data Protection Manager for advice and guidance using the contact details provided below.

Transfer of Personal Data outside the UK

The UK GDPR restricts transfers of Personal Data to separate countries or international organisations outside the UK in order to ensure that the level of protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that Personal Data in, to, or from a different country.
The "transfer" of Personal Data includes sending Personal Data to another country or region or allowing that Personal Data to be accessed remotely in another country, regardless of whether OnPath Energy transfers Personal Data outside the relevant country itself or a data processor does so when acting on our behalf.

Before any restricted transfers take place, you must first check with the Data Protection Manager to determine whether such transfer is lawful and ensure that the necessary transfer arrangements are in place, as applicable.

Use and Purpose of CCTV

All CCTV monitoring will be operated fairly and lawfully and only for the purposes defined in this Policy.

All monitoring will be operated with due regard for the privacy of all individuals at all times.

The overall purpose for the use of CCTV is to protect our premises from criminal activities and:

- to assist in the prevention and detection of crime against both persons and property;
- to facilitate the identification, apprehension and prosecution of offenders in relation to crime;

- to ensure the security of property belonging to OnPath Energy, employees and visitors to OnPath Energy premises; and

- to investigate health and safety in relation to incidents that have occurred on our premises or sites.

Only for specifically defined instances (e.g. the gathering of evidence in relation to a criminal activity) may surveillance equipment be used for targeted observation. The law regulates the use of covert monitoring of this type, and any such activity may also be subject to strict codes of practice.
Covert monitoring must be for a specific purpose and within a limited timeframe. Once sufficient evidence has been gathered the equipment must be removed.

No one can place a camera anywhere on OnPath Energy premises or sites without the written permission of the Grid and Operations Director and / or landlord.

Data Protection and Microsoft Teams

We use the Microsoft Teams tool to conduct online meetings. Microsoft Teams is a feature of Microsoft 365. When using Microsoft Teams (or any equivalent medium), various Personal Data and types of data are processed. The scope of the data also depends on the information you provide before or when participating in an online meeting. Some project meetings are being recorded by us to ensure minutes are produced if a diary clash occurs. If we record a meeting, this will be communicated to you before the start of the recording and you will be asked for your consent. If you do not wish to be recorded, you may deactivate your camera.

Once the minutes of the recorded meeting have been uploaded to our central document management system, the video will be deleted from the relevant Teams channel by the Project Secretary. Copying of any of the recordings made is strictly prohibited.

The Data Protection Manager will, in the course of a data protection audit, ensure that all recordings are not being retained beyond their retention period of 60 days.

Data Protection and Bring Your Own Device
The use of employee-owned devices to process business information and data creates issues that need to be addressed particularly in the area of data security.

As Controller, OnPath Energy must remain in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing.

As an employee, you are required to keep secure the organisation's information and data. This applies equally to information held on the organisation's systems and to information held on an employee's own device.

OnPath Energy does not support the use of personal devices for the purpose of accessing and processing company data. However, it is acknowledged that it is technically possible, and where personal devices are used for work purposes, that this usage must comply with the principles of the UK GDPR which stipulate that 'appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data'.

Employees are expected to use their device in an ethical manner and in accordance with the organisation's Information Security Policy.

If you do use your own device for work purposes then you are expected to adhere to the following security measures:

- your device must lock itself with a PIN (personal identification number) set by you;

- if left idle, your device must automatically activate its PIN after a maximum time-out period of 5 minutes; and

- in the event of loss or theft of your device, you must inform the Head of IT within 1 working day.

The organisation will not monitor the content of user owned devices for threats to the technical infrastructure of the business. However, the organisation reserves the right to prevent access to the network by any device that is considered a risk.

Responsibilities

All employees who provide OnPath Energy with Personal Data are responsible for:

- checking that any Personal Data that they provide is accurate and up to date; and

- informing the organisation of any changes to their Personal Data e.g. change of address, marital status, bank account details.

All employees who process Personal Data on behalf of OnPath Energy should:

- not disclose Personal Data over the telephone, in emails, by post [or fax] unless absolutely certain who the requestor is and the purpose for which they require the information. If in doubt, consult the Data Protection Manager;

- ensure that any data collected is only used for its original intended purpose;

- apply the appropriate retention schedule to the Personal Data that is being processed;

- mark all information that contains Personal Data as confidential;

- not send sensitive Personal Data by fax unless it is to a confidential or direct fax number, the fax is marked confidential and the recipient has been notified in advance of it being sent; and

- ensure that any Personal Data taken off site in paper format or any electronic information saved onto a company laptop is safeguarded as far as possible from loss or theft, (e.g. do not leave laptops or paper files containing sensitive and confidential information unattended in company vehicles).

The privacy and confidentiality of email messages cannot be guaranteed. It is the responsibility of all members of staff to exercise their judgement about the appropriateness of using email when dealing with Personal Data. More specifically:

- staff must ensure that all information of a sensitive nature that is sent via email is treated with care in terms of drafting and addressing;

- email messages containing information that is not intended for general distribution should be clearly marked either in the title or at the beginning of the message, and for example email correspondence containing comments about the performance of a specific staff member or a group of staff should be avoided. This should decrease the likelihood of the message being forwarded to unintended recipients;

- email messages containing Personal Data are covered by the UK GDPR and must be treated in line with the principles outlined in the UK GDPR. Under the UK GDPR, Personal Data includes opinions about an individual or the personal opinions of an individual. Email messages containing this type of information should only be used for the purpose for which the information was provided, be accurate and up to date, and must not be disclosed to third parties without the express permission of the individual concerned; and

- email messages that contain information that is not supported by fact should indicate that it is the sender's opinion that is being expressed.

All managers are responsible for:

- ensuring that staff who process Personal Data are aware of this Policy and their duties under it; and

- ensuring that staff who handle Personal Data are appropriately trained to do so and aware of the basic provisions of the UK GDPR.

All contractors, consultants and other third parties processing Personal Data on behalf of OnPath Energy must:

- ensure that they and their staff who have access to Personal Data held or processed for or on behalf of OnPath Energy are fully trained in and aware of their duties under the UK GDPR; and

- sign a declaration of confidentiality and undertake to process the data in accordance with this Policy.

OnPath Energy shall take appropriate steps to ensure that all relevant and necessary contractual terms are put in place with any relevant service providers, contractors and other third parties; you should contact internal legal counsel for advice as to what these contractual clauses should include.

Personal Data released to a third party for processing on its own behalf must only be released with the individual's consent. The third party must apply in writing before Personal Data is released to it.

Under no circumstances must information be released about an individual to any person requesting the information by telephone, fax, or post unless the identity of the person making the request is confirmed and that they are entitled to receive the information requested. Please note that parents (unless in relation to children under 16), spouses, partners and children are not entitled to information about another individual.

Complaints

Where you receive a complaint from an individual, no communications should be sent out in response without first consulting our Data Protection Manager.

Controls

This Policy will be reviewed regularly by the Data Protection Manager and updates made in line with changing business needs or new legislation. Any updates to this Policy will be uploaded to the OnPath energy intranet site. It is your responsibility to check back regularly to obtain the latest version of this Policy.

Data protection audits will be carried out regularly across the organisation. Gaps in awareness, lack of information security measures or inadequate processing practices will be highlighted and the appropriate remedial action taken.
Data protection training is available to those members of staff who process personal information.

Awareness

OnPath Energy has a legal liability to ensure that Personal Data is processed in accordance with applicable data protection legislation. Any breach will be taken seriously and may result in formal disciplinary action.

This Policy was last updated in April 2024.

Signed for and on behalf of the board by:
RICHARD DUNKLEY • CEO
April 2024

OPE/0/2950. Published April 2024. Printed on paper from sustainable sources.
Registered office: Chase House, 4 Mandarin Road, Houghton-Le-Spring, DH4 5RA