General Data Protection Regulation (GDPR) Policy

1. General Policy Statement

This Policy applies to all employees, any breach of this Policy or of the General Data Protection Regulation will be considered an offence and the Leisure Energy Disciplinary Procedures will be invoked. This Policy is linked the Data Protection Policy (within the Staff Handbook).

The GDPR legislation came in to force on the 25th May 2018. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals, for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

Leisure Energy Ltd will be the 'Data Controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. Leisure Energy will register with the Information Commissioner's Office and pay the relevant fee.

The Data Protection Officer (DPO), Michael Worsnop, is available to address any concerns regarding the data held by Leisure Energy and how it is processed, held and used.

Michael Worsnop is responsible for all day-to-day data protection matters, and is responsible for ensuring that all employees and relevant individuals abide by this Policy. The MD is also responsible for ensuring that any breaches are documented, investigated and notified to the Information Commissioners Office (ICO) where applicable.

2. Collection and Storage of Data

All employee data collected and stored by Leisure Energy is for the sole purposes of Leisure Energy business requirements and an individual's relationship with Leisure Energy.

All personnel records are kept in a secure filing cabinet and on the cloud based "OneDrive Secure Documents". Only the Chairman, Managing Director and the Accountant have access to personnel records on this OneDrive.

3. Data Protection Principles

The legislation places a responsibility on a data controller to process any personal data in accordance with the eight principles. In order to comply with its obligations, Leisure Energy undertakes to adhere to the eight principles:

3.1 Process personal data fairly and lawfully.

Leisure Energy will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an

indication of the period for which the data will be kept, and any other information which may be relevant.

3.2 Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.
Leisure Energy will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3.3 Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.
Leisure Energy will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

3.4 Keep personal data accurate and, where necessary, up to date.
Leisure Energy will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify LE, if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of Leisure Energy to ensure that any notification regarding the change is noted and acted on.

3.5 Only keep personal data for as long as is necessary.
Leisure Energy undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. Leisure Energy will undertake a regular review of the information held and implement a process to delete data in accordance to HMRC guideline on the retention of data.
Leisure Energy will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

3.6 Process personal data in accordance with the rights of the data subject under the legislation.
Individuals have various rights under the legislation including a right to:
• be told the nature of the information Leisure Energy holds and any parties to whom this may be disclosed.
• prevent processing likely to cause damage or distress.
• prevent processing for purposes of direct marketing.
• be informed about the mechanics of any automated decision-taking process that will significantly affect them.
• not have significant decisions that will affect them taken solely by automated process.
• issue for compensation if they suffer damage by any contravention of the legislation.
• take action to rectify, block, erase or destroy inaccurate data.
• request that the ICO assess whether any provision of the Act has been contravened.
Leisure Energy will only process personal data in accordance with individuals' rights.

3.7 Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.
Employees are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.
Leisure Energy ensure that all personal data is accessible only to those who have a valid reason for using it.
Leisure Energy have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access:
• keeping all personal data in a lockable cabinet with key-controlled access and/or on the OneDrive which is accessible only by the Chairman, Managing Director and the Accountant
• password protecting personal data held electronically
• archiving personal data which are then kept securely (lockable cabinet)
• placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff
• ensuring that PC screens are not left unattended

In addition, Leisure Energy will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.
This policy also applies to employees and consultants who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

3.8 Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Leisure Energy will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA – and Leisure Energy will always seek the consent of individuals before placing any personal data (including photographs) on its website.
If Leisure Energy collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

4. Consent
Consent is especially important when Leisure Energy is processing any sensitive data, as defined by the legislation.
Leisure Energy understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via the Personal Details Form) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication

Leisure Energy will ensure that any forms used to gather data on an individual will contain a statement explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.
Leisure Energy will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

5. Breaches in Personal Data
The GDPR introduces a duty to report certain types of personal data breach to the relevant supervisory authority. Leisure Energy must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, Leisure Energy must also inform those individuals without undue delay. It is, therefore, essential that a robust breach detection, investigation and internal reporting procedures are in place. This facilitates the decision-making about whether or not Leisure Energy are required to notify the relevant supervisory authority and the affected individuals.
Individuals who provide personal data to Leisure Energy are responsible for ensuring that the information is accurate and up-to-date.
It is the duty of employees to notify any breach of personal data to the Data Controller immediately the breach is identified.

6. What is a personal data breach?
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
Example
Personal data breaches can include:

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

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In essence there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, or for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

7. What breaches require notifying to the ICO?
When a personal data breach has occurred, Leisure Energy need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then Leisure Energy must notify the ICO; if it's unlikely then it does not have to be

reported. Leisure Energy will keep a record of any personal data breaches, however, regardless of whether the breach is required to be notified in order to justify this decision.
In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:
"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."
This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. Leisure Energy will assess this case-by-case, looking at all relevant factors.

Example
The theft of an employee database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. Leisure Energy would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of an employee telephone list.
On becoming aware of a breach you must report it to the Data Controller, who will attempt to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

8. What role do processors have?
On such occasions where Leisure Energy uses a data processor, and this processor suffers a breach, then it must inform Leisure Energy without undue delay as soon as it becomes aware.
Example
Leisure Energy (the controller) contracts an IT services firm (the processor) to archive and store employee records. The IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed. As this is a personal data breach, the IT firm promptly notifies Leisure Energy that the breach has taken place and Leisure Energy will in turn notify the ICO.
If Leisure Energy use a processor, the requirements on breach reporting should be detailed in the contract between you and your processor.

9. How much time has Leisure Energy to report a breach?
LE must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. Leisure Energy must give reasons for the delay if it takes longer than this.
It is the duty of employees to notify any breach of personal data to the Data Controller immediately the breach is identified.

10. What information must a breach notification to the supervisory authority contain?

When reporting a breach, the GDPR stipulates the following are provided:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

11. What if all the required information is available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. It is acceptable to provide the required information in phases, as long as this is done without undue further delay.

However, Data Controllers are expected to prioritise the investigation, give it adequate resources, and expedite it urgently. Leisure Energy must still notify the ICO of the breach when becoming aware of it, and submit further information as soon as possible. If Leisure Energy are aware that it is unable to provide full details within 72 hours, the reasons for a delay should be reported with an indication of when further information may be submitted.

Example

Leisure Energy detect an intrusion into the network and become aware that files containing personal data have been accessed, but don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system.

LE must notify the ICO within 72 hours of becoming aware of the breach, explaining that all of the relevant details are not yet available but expect to have the results of an investigation within a few days. Once the investigation uncovers details about the incident, Leisure Energy will give the ICO more information about the breach without delay.

12. When do Leisure Energy need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR stipulates individuals must be informed directly and without undue delay. This should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Leisure Energy will assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, Leisure Energy will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

If Leisure Energy decide not to notify individuals, Leisure Energy will still need to notify the ICO unless it can be demonstrated that the breach is unlikely to result in a risk to rights and

freedoms. ICO has the power to compel Leisure Energy to inform affected individuals if it is considered there is a high risk. In any event, Leisure Energy will document the decision-making process in line with the requirements of the accountability principle.

13. What information must Leisure Energy provide to individuals when telling them about a breach?

A clear and plain description of the nature of the personal data breach and, at least:

- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

14. Does the GDPR require Leisure Energy to take any other steps in response to a breach?

LE need to ensure that all breaches are recorded, regardless of whether or not they need to be reported to the ICO.

The facts relating to the breach must be documented, its effects and the remedial action taken. This is part of the overall obligation to comply with the accountability principle and allows the ICO to verify LE's compliance with it's notification duties under the GDPR.

As with any security incident, there will be an investigation as whether or not the breach was a result of human error or a systemic issue and to check how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

15. GDPR in relation to COVID 19

If staff/sub-contractors have been requested to complete a Wellness Checklist in relation to their work with Leisure Energy, we will explain why this necessary. Information will be held on file but not shared outside of the organisation.

If a member of staff contracts COVID-19, their personal information does not need to be shared with other staff but staff will be made aware of the case if they have come in contact with the person who has contracted COVID-19.

If there is a case of Covid-19 on site, we will advise other staff/sub-contractors of the precautions they need to take. If there is more than one case of COVID-19, the local health protection team will need to be contacted and the leisure operator. It is therefore important that sign in sheets are filled in correctly and retained as necessary.

16. Failure to notify the ICO

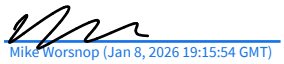
Failing to notify a breach when required can result in a significant fine.

It is, therefore, the duty of employees to notify any breach of personal data to the Data Controller immediately the breach is identified.

All Company personnel must comply fully with this policy and with any complementary instructions received from the Company.

This policy will be reviewed annually or when there is a change in circumstances in work practices or the introduction of new legislation.

Signed:



Michael Worsnop
Director

Address: Units 6-8, Site 8, Gemini Business Park,
Off Walter Nash Road West, Kidderminster,
DY11 7HJ
Tel: 01865 306688

Company No: 08938136
VAT No: 190 9674 67
www.leisure-energy.com
info@leisure-energy.com

LE - GDPR Policy - 2026 2027

Final Audit Report 2026-01-08

Created:	2026-01-08
By:	Sandie Osborne (sandie.osborne@leisure-energy.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAADi_RyfrINv-rMeddZd5lF5qXr7hFilF8

"LE - GDPR Policy - 2026 2027" History

Document created by Sandie Osborne (sandie.osborne@leisure-energy.com)
2026-01-08 - 3:29:38 PM GMT

Document emailed to Mike Worsnop (mike.worsnop@leisure-energy.com) for signature
2026-01-08 - 3:29:41 PM GMT

Email viewed by Mike Worsnop (mike.worsnop@leisure-energy.com)
2026-01-08 - 7:15:28 PM GMT

Document e-signed by Mike Worsnop (mike.worsnop@leisure-energy.com)
Signature Date: 2026-01-08 - 7:15:54 PM GMT - Time Source: server

Agreement completed.
2026-01-08 - 7:15:54 PM GMT