LEGAL & COMPLIANCE

Data Protection Policy

Author: Carrie Robertson
Version Date: 27 June 2023
Version Number: 1

Definitions

CWL	means Castle Water Limited (registered number SC475583) having its registered office at 1 Boat Brae, Rattray, Blairgowrie PH10 7BH.
CWL Group	means CWL and any of its subsidiaries, holding companies or any subsidiaries of such holding company.
Data Protection Legislation	means the United Kingdom General Data Protection Regulation (UK GDPR), Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003
Data Protection Officer	Euan Mitchell
Data Subjects	current, former, or prospective customers, employees, contractors, agency, workers, volunteers, trainees and apprentices, supplies and third parties.
Personal Data	means information relating to natural persons who: • can be identified or who are identifiable, directly from the information in question; or • who can be indirectly identified from that information in combination with other information.
Privacy Policy	means the policy contained at https://www.castlewater.co.uk/privacy-policy as updated from time to time.
Sensitive Personal Data	means data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
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.

1. Introduction

1.1 The CWL Group obtain, use, and retain Personal Data as part of our day-to-day activities and for various, specific, lawful purposes as set out in our Privacy Policy. That Personal Data relates to the Data Subjects.

1.2 Accordingly, the CWL Group are subject to the Data Protection Legislation which sets out how the CWL Group, as data controllers and data processors, should obtain, deal with and retain Personal Data. The CWL Group are committed to complying with those provisions and to being concise, clear, and transparent with how we obtain, use and delete (where appropriate) that Personal Data.

2. Scope

2.1 This policy applies to the Personal Data of all those identified as Data Subjects, whether it is on paper, or stored electronically and whether it is in writing or stored as verbal messages. It applies whether the Personal Data is stored on our network, on individual desktop, or laptop, computers, on mobile devices, phones, or tablets, in paper files or in any other way.

2.2 The purpose of this policy is to set out how the CWL Group complies with our data protection obligations and the means by which we protect Personal Data relating to Data Subjects. This includes our obligations as to the collection, processing, transfer, storage, and disposal of that Personal Data.

2.3 This policy will also set out what the CWL Group expects to be done by our directors, managers, employees, contractors, agency workers, interns, volunteers and trainees and apprentices.

2.4 This policy should be read in conjunction with the following:

2.4.1 Data Subject Access Request Policy
2.4.2 Data Breach Policy
2.4.3 Privacy Policy
2.4.4 Information Security Policy
2.4.5 Communication Security Policy
2.4.6 Data Retention Policy

2.5 All employees should be aware of, and comply with, these policies in addition to complying the terms contained within this policy.

3. Roles & Responsibilities

3.1 The Data Protection Officer has the following responsibilities:

3.4.1 Informing and advising the CWL Group on its data protection obligations.
3.4.2 For monitoring compliance with, and reviewing, this policy and the Data Protection Legislation.
3.4.3 Ensuring the Data Subject Access Request Policy is complied with.
3.4.4 Ensuring the Data Breach Policy is complied with.

3.4.5 Ensuring that data protection induction and employee training takes place at regular intervals.
3.4.6 Ensuring that Data Protection Impact Assessments are carried out as and when necessary.
3.4.7 Reviewing, and approving (if appropriate), contracts with third party data processors.
3.4.8 Responding to issues relating to:
i. the lawful basis which is to be applied to Personal Data collected;
ii. use of Personal Data having regard to the purpose for which it was acquired;
iii. periods of retention of Personal Data;
iv. privacy notes and when these are required.

3.4.9 Addressing any other issues that arise relating to the processing, collection, and retention of Personal Data.

3.2 The Chief Technology Officer has the following responsibilities:

3.4.10 Designing and implementing programmes for the purposes of data protection training to employees, volunteers, trainees, and apprentices; and
3.4.11 Establishing procedures and standards which ensure compliance of the Data Protection Legislation by vendors, suppliers and third parties who receive Personal Data from, or have access to the Personal Data stored and processed by, the CWL Group for any reason.

4. Processing Personal Data

Requirements

4.1 When processing Personal Data, the CWL Group must ensure that we:

4.1.1 process personal information lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
4.1.2 only collect Personal Data for specified, explicit, and legitimate purposes and not process that data in a way that is incompatible with those legitimate purposes ('purpose limitation');
4.1.3 only process the Personal Data that is adequate, relevant and necessary for the purpose ('data minimisation');
4.1.4 keep the Personal Data accurate and up to date and take all reasonable steps to delete or correct inaccurate Personal Data without delay ('accuracy');
4.1.5 keep Personal Data in a way that permits identification of Data Subjects for no longer than is necessary for the purpose for which it is processed, subject to certain exceptions ('storage limitation'); and
4.1.6 process the Personal Data in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4.2 The CWL Group must only process data in accordance with the data protection principles and in such a way that at least one of the following bases applies:

4.2.1 the Data Subject has given consent to the processing of their Personal Data for one or more specific purposes ('consent');

4.2.2 the processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract ('contract');

4.2.3 the processing is necessary for compliance with a legal obligation to which we are subject ('legal obligation');

4.2.4 the processing is necessary for the protection of the vital interests of the Data Subject or another natural person ('vital interest');

4.2.5 the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority ('public interest');

4.2.6 the processing is necessary for the purposes of the legitimate interests pursued by the CWL Group or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data ('legitimate interest')

4.3 Other than where the processing is based on consent, the CWL Group must satisfy ourselves at all times that the processing is necessary for the purposes of the relevant lawful basis set out above and that there is no other reasonable way to achieve that purpose. To demonstrate compliance, the CWL Group must document our decision as to which lawful basis applies and record information both detailing the purposes of the processing and the lawful basis relied upon.

Consent

4.4 Where processing is based on consent, the CWL Group must be able to demonstrate that the Data Subject has consented to the processing of their Personal Data and that consent has been given in circumstances that it is able to be clearly distinguishable from the other matters and in an intelligible and easily accessible form, using clear and plain language.

4.5 The Data Subject shall have the right to withdraw their consent at any time which shall not, however, affect the lawfulness of processing based on consent before its withdrawal.

4.6 When assessing whether consent is freely given, regard must be had to the fact that the performance of a contract or provision of a service must not be made conditional on consent to the processing of Personal Data that is not necessary for the performance of that contract.

Sensitive Personal Data

4.7 Where Sensitive Personal Data is to be processed, the CWL Group must, in addition to the bases set out above, identify a lawful special condition for processing that information, as set out below, and document it:

4.7.1 the Data Subject has given their explicit consent to the processing of such Sensitive Personal Data for one or more specified purposes;

4.7.2 processing is necessary for the purposes of carrying out our obligations and exercising specific rights or those of the Data Subject with regards to their employment, social security and social protection in so far as it is authorised by UK domestic law or a collective

agreement pursuant to UK domestic law providing for appropriate safeguards for the fundamental rights and interests of the Data Subject;

4.7.3 processing relates to Sensitive Personal Data or Personal Data which is manifestly made public by the Data Subject;

4.7.4 processing is necessary to establish, exercise, or defend legal claims or whenever courts are acting in their judicial capacity;

4.7.5 the processing is necessary for substantial public interest reasons, on the basis of UK domestic law and it is proportionate to the aim pursued, respects of the essence of the right to data protection and provides suitable and specific measures to safeguard the fundamental rights and interests of the Data Subject;

4.7.6 the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the management of health on the basis of UK domestic law or pursuant to contract and subject to the conditions and safeguards referred to in Article 9(3) of the UK; or

4.7.7 the processing is necessary for public interest reasons in the area of public health.

4.8 If the data is Sensitive Personal Data then the Data Protection Officer must be notified, before processing commences, of the proposed processing so that they may assess whether the processing complies with the criteria set out above. No processing will commence until that assessment has taken place and the Data Subject has been informed and no automated decision-making (including profiling) will be based on any Data Subject's Sensitive Personal Data.

5. Data Protection Impact Assessments

5.1 The CWL Group must apply privacy by design principles to all new projects or uses of Personal Data, especially where they involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms to the Data Subjects.

5.2 A data protection impact assessment (DPIA) shall in particular be required in the case of:

5.2.1 a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produced legal effects concerning the natural person or similar significantly affect the natural person; or

5.2.2 processing on a large scale of Sensitive Personal Data, or of Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR.

5.3 In such circumstances, the CWL Group will carry out a DPIA to assess:

5.3.1 the purposes of the processing, including, where applicable, the legitimate interest we are pursuing;

5.3.2 whether the processing is necessary and proportionate in relation to its purpose;

5.3.3 the risk to Data Subjects; and

5.3.4 the measures that can be put in place in order to address those risks and protect Personal Data.

5.4 In doing so, regard will be had to:

5.4.1 the nature, scope, context, and purpose(s) of the collection, holding, and processing;
5.4.2 the state of the art of all relevant technical and organisational measures to be taken;
5.4.3 the cost of implementing such measures; and
5.4.4 the risk posed to Data Subjects and this organisation, including their likelihood and severity.

5.5 The DPIA will be overseen by the Data Protection Officer and shall address:

5.5.1 the type of Personal Data collected, held and processed;
5.5.2 why and how Personal Data is to be used;
5.5.3 our objectives;
5.5.4 who is to be consulted;
5.5.5 the necessity and proportionality of the data processing
5.5.6 the risk to Data Subjects and to the CWL Group; and
5.5.7 the measures taken to minimise and deal with those risks identified.

6. Information provided to, and the rights of, Data Subjects

6.1 The CWL Group will issue privacy notices from time to time, informing Dated Subjects as to the Personal Data that the CWL Group collects about them, how it is held and how they can expect that Personal Data to be used and for what purposes.

6.2 Any information provided in privacy notices will be in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

6.3 The CWL Group will ensure that Data Subjects are informed that they have the following rights in relation to their Personal Data, via a privacy notice:

6.3.1 to be informed how, why and on what basis their Personal Data is processed;
6.3.2 to obtain confirmation that their Personal Data is being processed and to obtain access to it and certain other information, by making a subject access request;
6.3.2 to have Personal Data corrected if it is inaccurate or incomplete;
6.3.3 to have Personal Data erased if it is no longer necessary for the purposes for which it was originally collected/processed, or if they have no overriding legitimate grounds for processing;
6.3.4 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but they do not want the Personal Data to be erased), or where the Personal Data is no longer needed but it is required to be retained to establish, exercise or defend a legal claim;
6.3.5 to restrict the processing of Personal Data temporarily where they do not think it is accurate or where they have objected to the processing and we are considering whether our legitimate aims override their interests;
6.3.6 to receive the Personal Data concerning themselves, which they have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller without hindrance from us.

6.4 A Data Subject may:

6.4.1 make a subject access request at any time to find out more about the Personal Data which we hold about them, the processing we carry out and the purpose of that processing;
6.4.2 require us to rectify any Personal Data that is inaccurate or incomplete; or
6.4.3 request that we erase the Personal Data that we hold about them where it is (i) no longer necessary for us to retain that Personal Data having regard to the purpose for which it was originally collected or processed; (ii) consent has been withdrawn from the Data Subject; (iii) where the Data Subject objects to us holding and processing their Personal Data and no overriding legitimate interest permitting us to continue doing so exists; (iv) the Personal Data has been processed unlawfully; and (v) we need to erase the Personal Data in order to comply with a particular legal obligation.

6.5 The CWL Group will comply with any requests listed in 6.4 in accordance with the Subject Access Request Policy.

7. Confidentiality & Information Security

7.1 The CWL Group must keep the Personal Data about all Data Subjects for which they are responsible confidential. All employees of the CWL Group who have access to Personal Data about Data Subjects must keep that Personal Data confidential. Failure to do so would be a breach of the CWL Group's duties under the Data Protection Legislation.

7.2 All employees who have access to Personal Data must:

7.2.1 only access the Personal Data which they are authorised to access, and only for authorised purposes;
7.2.2 only allow other personnel to access Personal Data if they have appropriate authorisation;
7.2.3 only allow individuals who are not employees of the CWL Group to access Personal Data if specific authority exists;
7.2.4 keep Personal Data secure. For example, by complying with the rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in our Information Security Policy;
7.2.5 whenever passwords are used to protect Personal Data, they must be changed regularly and common or easily guessed words or phrases should not be used;
7.2.6 not remove Personal Data, or devices containing Personal Data, from our premises unless appropriate security measures are in place to secure the data and the device and they have authority to do so;
7.2.7 ensure that 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, that the computer and screen are locked before the user leaves it.
7.2.8 not store their own personal information on local drives or devices that are used for work purposes.

7.3 In the event that any employees have any concerns or suspicions that any of the matters set out below are taking place, they should immediately inform the Data Protection Officer of those concerns or suspicions:

7.3.1 Personal Data is being processed without a lawful basis or, in the case of Sensitive Personal Data, without one of the conditions in paragraph 4.7 above being met;
7.3.2 a Personal Data Breach
7.3.3 Personal Data is being accessed without the proper authorisation;
7.3.4 Personal Data is not being retained or deleted securely;
7.3.5 Personal Data, or devices containing Personal Data, are being removed from our premises without appropriate security measures being in place; or
7.3.6 any other breach of this policy or of any of the data protection principles set out in paragraph 4.1 – 4.3 above.

7.4 The CWL Group will use all appropriate technical and organisational measures in order to keep Personal Data secure and to protect it from unauthorised or unlawful processing and accidental loss, destruction or damage. Those measures may include:

7.4.1 ensuring that wherever possible Personal Data is pseudonymised or encrypted;
7.4.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
7.4.3 ensuring that, in the event of a physical or technical incident, availability and access to Personal Data can be restored in a timely manner; and
7.4.4 the regular testing, assessing and evaluating of effectiveness of technical and organisational measures for ensuring the security of the processing.

7.5 In the event that we use external organisations to process Personal Data on our behalf, we will ensure that additional security arrangements are implemented in contracts with those organisations in order to safeguard the security of Personal Data.

7.6 No one may enter into an agreement with an external organisation to process Personal Data on behalf of the CWL Group without the consent of the Data Protection Officer.

8. Storage and Retention of Personal Data

8.1 We must not retain Personal Data (and in particular, Sensitive Personal Data) for any longer than necessary. The length of time over which Personal Data may be retained is dependent upon the circumstances including why the personal information was obtained in the first place.

8.2 We provide details of the retention periods for different types of Personal Data or the criteria that should be used to determine that retention period in our Data Retention Policy.

8.3 We will ensure that all measures listed in Section 7 are taken as to the storage of Personal Data.

8.4 We must delete permanently from our information systems any Personal Data (and Sensitive Personal Data) that is no longer required and destroy any hard copies securely in accordance with our Data Retention Policy.

9. Transfer of Personal Data to outside the UK

9.1 The CWL Group will under no circumstances transfer Personal Data outside of the UK.

10. Data Breaches

10.1 A Personal Data Breach is any loss of Personal Data or information in whatever form it is held and by whatever means the Personal Data was lost including data that is destroyed or rendered unusable. It may take many different forms, including:

10.1.1 loss or theft of Personal Data or equipment on which Personal Data is stored;
10.1.2 unauthorised access to or use of Personal Data either by an employee or third party such as from hacking;
10.1.3 loss of Personal Data resulting from an equipment or systems (including hardware and software) failure;
10.1.4 human error, such as accidental deletion or alteration of Personal Data;
10.1.5 unforeseen circumstances, such as a fire or flood;
10.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
10.1.7 social engineering such as phishing and vishing, where information is obtained by deception.

10.2 All Personal Data breaches must be handled in accordance with the Data Breach Policy and reported immediately to the Data Protection Officer.

11. Training

11.1 The CWL Group will ensure that all employees receive adequate training as to their data protection responsibilities and as to how to act and respond as and when they receive requests for matters such as subject access requests, objections and requests for erasure and rectification. Those whose roles require regular access to Personal Data, or who are responsible for implementing this policy or responding to subject access requests, will receive additional training to help them understand their duties and how to comply with them.

11.2 Information will be provided to all new employees as part of their induction training.

12. Failure to Comply

12.1 The CWL Group regard compliance with this policy as an extremely serious matter. Failing to comply puts at risk those individuals whose Personal Data is being processed, carries the risk of significant civil, criminal and regulatory sanctions for the CWL Group and our employees and may, in some circumstances, amount to a criminal offence.

12.2 Any failure to comply with provisions set out in this policy by any employees will be taken seriously and may lead to disciplinary action being taken against that person under our usual disciplinary processes. Breaches may result in dismissal for gross misconduct for employees and immediate contract termination for non-employees.

13. Policy Review

13.1 This policy will be reviewed and updated regularly to ensure that the CWL Group continue to act in accordance with our data protection obligations. Revised versions will be brought to the attention of all employees, as, and when, necessary.