CASTLE WATER

Process Sign Off
I can confirm that as the Process Owner for this process I have reviewed and accepted this process:

Name A. Caddick

Signature A. Caddick

Date 16/4/18

I can confirm that as the Team Leader/Manager overseeing this activity, I have reviewed and accepted this process:

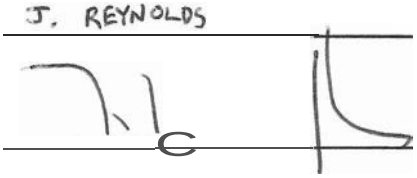
Name M.Haviland

Signature M.Haviland

Date 16/04/18

I can confirm that as the Director overseeing this activity, I have reviewed and accepted this process:

Name J. REYNOLDS

Signature 

Date 23/4/18

CASTLE WATER

Data Protection Policy

Date: 13th April 2018

Author: Adrian Caddick

V1.0

Contents

CASTLE WATER

1. Introduction

1.1 Castle Water needs to keep certain information about its employees, customers, suppliers and other users to allow it to monitor performance, achievements, and health and safety, for example. It also needs to process information so that workers can be recruited and paid, customers can be billed, payments processed, marketing undertaken, and legal obligations complied with.

1.2 To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Castle Water must comply with the Data Protection Principles, which are set out in the General Data Protection Regulation (GDPR), EU Regulation 2016/679. Article 5 sets out seven principles:

1. Lawfulness, fairness and transparency;
2. Purpose limitation;
3. Data minimisation;
4. Accuracy;
5. Storage limitation;
6. Integrity and confidentiality;
7. Accountability.

1.3 Anyone who processes data on behalf of Castle Water, including but not limited to, employees; temporary workers; consultants; contractors or others who process or use any personal information must ensure that they follow these principles at all times. To ensure that this happens, Castle Water has developed this Data Protection Policy, and accompanying procedure.

2. Scope

2.1 This document provides the policy framework for the proper processing of personal information at Castle Water, through which the appropriate processing of personal information can be achieved and audited. It provides information to employees, temporary workers, contractors and consultants at Castle Water regarding their responsibilities, in respect of the processing of personal information and the means of support available.

2.2 This policy applies to all processing of personal information in Castle Water regardless of the actual or intended purpose of that processing. Personal information is defined as recorded information, in any form and regardless of media, created or received by Castle Water in the transaction of business or conduct of affairs pertaining to any living individual, or which could pertain to any living individual when aggregated with other information in the possession of Castle Water. The GDPR requires that the specific needs of micro, small and medium sized enterprises must be taken into account.

3. Responsibilities

3.1 Castle Water is identified as the Data Controller for the information in its charge for the purposes of the GDPR. It is also identified as a Data Processor. Overall responsibility for compliance with Data Protection lies with the Chief Operating Officer. All employees, temporary workers, consultants and contractors of Castle Water are responsible for ensuring that any personal information processed in the course of their duties, is processed in accordance with the requirements of the GDPR.

3.2 All employees, temporary workers, consultants and contractors are responsible for:

i. Checking that any information that they provide to Castle Water in connection with their employment is accurate and up to date;
ii. Informing Castle Water of any changes to information, which they have provided, e.g. changes of address;
iii. Informing Castle Water of any errors or changes in employee information. Castle Water cannot be held responsible for any such errors unless the employee has informed Castle Water of them.

4. Rights to access information

4.1 The GDPR applies to personal data held by an organisation. It allows people 12 years of age and over, to find out what personal information is held about them and why it is held, by making a Subject Access Request (SAR). Personal data is any information which is capable of identifying a living individual e.g. name and address, audio or video recording, CCTV image, email address, postcode, photograph etc. A SAR can include both electronic information and paper records.

4.2 Information about making a subject access request is contained within the Data Protection procedure, and on Castle Water's website.

5. Other rights

5.1 The GDPR has introduced some new rights for individuals, where they can request the data processor to:

- restrict or suppress their personal data;
- have their data erased. This is known as "the right to be forgotten";
- have inaccurate personal data rectified or completed if it is incomplete.

5.2 None of these rights are absolute and only apply in certain circumstances. An individual can make a request verbally or in writing. Castle Water then has one calendar month to respond to a request.

5.3 The GDPR also provides individuals the right to object to the processing of their data in certain circumstances. It also has provisions on automated decision-making processes. More specific guidance is contained within the Data Protection procedure.

6. Consent

6.1 The GDPR requires that clear and unambiguous consent must be obtained from the data subject. The Data Controller should be able to demonstrate that the data subject has given their consent to the processing of their data. Individuals should be informed of the processing, especially where profiling and direct marketing is undertaken.

6.2 More specific guidance on consent is contained within the Data Protection procedure.

7. Processing sensitive information

7.1 Sometimes it is necessary to process sensitive personal information. This may be to ensure that Castle Water is a safe place for everyone, or to operate other Castle Water policies, such as the sick pay policy or equality policies. Castle Water will also ask for information about health needs, such as allergies to forms of medication, or any health conditions or disabilities. Because this information is considered sensitive, and it is recognised that the processing of it may cause concern or distress to individuals, employees will be asked to give express consent for Castle Water to process this information.

8. Retention of data

8.1 Castle Water will keep some forms of information for longer than others. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. For more detail please refer to the Records & Information Management Policy and procedure.

9. Privacy

9.1 The GDPR ensures that individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

9.2 Castle Water must provide individuals with information including: the purposes for the processing of their personal data; our retention periods for that personal data, and who it will be shared with. The GDPR calls this ‘privacy information’.

9.3 GDPR requirements are about ensuring that privacy information is clear and understandable for individuals. The GDPR says that the information you provide to people about how you process their personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

9.4 Under the GDPR consideration must be given whether to undertake a Data Protection Impact Assessment (DPIA) where there is a risk to the rights and freedoms of natural persons. It is a process to help identify and minimise the data protection risks of a project.

9.5 More specific guidance on privacy and DPIA is contained within the Data Protection procedure.

10. Contracts

10.1 Castle Water as the data controller must ensure that when using third party data processors, it has written contracts in place. The contract is important so that both parties understand their responsibilities and liabilities under GDPR.

10.2 As the data controller Castle Water is responsible for compliance with the GDPR and must only appoint data processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of individuals protected. In the future it is envisaged that Castle Water will require third party data processors to adhere to an approved code of conduct or certification scheme. No such schemes are currently available.

10.3 Data processors must only act on the documented instructions of Castle Water acting as the data controller.

11. Compliance

11.1 Compliance with the GDPR is the responsibility of employees, temporary workers, consultants and contractors working at Castle Water. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or even a criminal prosecution. It may also result in personal liability for the individual. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer (DPO).

11.2 The Compliance Manager has been appointed as Castle Water's DPO. Any breaches of the GDPR could result in fines levied by the ICO. These could range from £500,000 to a maximum of 4% of turnover.

12. Data breaches

12.1 The GDPR introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, where feasible. The DPO will undertake this.

12.2 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. In short, 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, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

12.3 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, Castle Water must also inform those individuals without undue delay. A record of any personal data breaches, regardless of whether they are reportable to the ICO should be maintained by the DPO. Further information about data breaches is contained within the Data Protection procedure.