PERSONAL DATA PROTECTION AND PRIVACY POLICY

Last reviewed: 23 February 2024

Next review due: 22 February 2024

1. Introduction

1.1 Wickenstones needs to gather and use certain information about individuals, including clients, employees, job applicants, external experts and patients.

This policy describes how these personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

1.2 The appendices to this policy are privacy notices that describe in detail how different types of data must be handled. These notices must be accessible to the individuals about whom we hold data. Wherever possible, they should be actively sent to those they concern.

1.3 This data protection policy ensures that Wickenstones:

1.3.1 Complies with the EU general data protection regulation and follows good practice
1.3.2 Protects the rights of staff, customers and partners
1.3.3 Is open about how it stores and processes individuals' data
1.3.4 Protects itself from the risks of a data breach

1.4 This policy applies to all three entities of Wickenstones: Wickenstones Ltd registered in the UK under company number 8576674, Wickenstones Ltd registered in Ireland under company number 651480, and Wickenstones Ltd registered in the United States of America under company number 7411481. Within this policy, unless otherwise stated, 'Wickenstones' means all three entities collectively. Separately, the entities will be referred to in this policy as 'Wickenstones UK', 'Wickenstones EU' and 'Wickenstones US', respectively.

1.5 This policy applies to:

1.5.1 All staff of Wickenstones
1.5.2 All contractors, suppliers and other people working on behalf of Wickenstones

It applies to all data that the company holds relating to identifiable individuals.

2. Responsibilities

2.1 Everyone who works for or with Wickenstones has responsibility for ensuring data are collected, stored and handled appropriately.

2.2 Each team that handles personal data must ensure that they are handled and processed in line with this policy and GDPR principles.

2.3 The following people have key areas of responsibility:

2.3.1 Wickenstones' Directors are ultimately accountable for ensuring that Wickenstones meets its legal obligations.

2.3.2 They are responsible for:

2.3.2.1 ensuring that all staff understand their duties under GDPR

2.3.2.2 reviewing and updating the data protection policy as required

2.3.2.3 ensuring that requests from data subjects to exercise their rights under GDPR are handled appropriately

2.3.2.4 reporting any data breach to the appropriate authorities

2.3.2.5 ensuring appropriate agreements are in place with any third parties that process personal data on Wickenstones' behalf or with whom Wickenstones shares personal data

2.3.2.6 writing and updating Wickenstones' privacy notices

2.3.2.7 regularly reviewing data protection practices with staff responsible for handling personal data

2.3.3 Cluster leads are responsible for the following actions for every project (which may be delegated to a team member)

2.3.3.1 Identifying any personal data and completing a data protection plan (see appendix F) before the project commences, seeking advice from the project support lead, if required.

2.3.3.2 Deciding how personal data will be stored and ensuring that no one that does not need them may access them.

2.3.3.3 Ensuring that each member of the project team knows which data are personal data and understands the plan for processing them.

2.3.3.4 Ensuring that no member of the project team moves, shares or copies the personal data unnecessarily or outside of the scope of the data protection plan.

2.3.3.5 Where applicable, issuing data subjects with a suitable privacy notice, in consultation with the project support lead.

3. General staff guidelines for data storage and access

3.1 Wickenstones staff should keep all data secure, by taking sensible precautions and following the guidelines below.

3.1.1 The only people able to access personal data should be those who need them for their work.

3.1.2 Data that are no longer in use should be deleted, taking into account standard retention times which are provided in this policy. They may be backed up to secure archive storage first, only under the following circumstances:

3.1.2.1 the data are needed to fulfil a legal obligation;

3.1.2.2 the data are covered by a privacy notice which has been made reasonably available to the data subjects, and which explains Wickenstones' lawful basis for retaining the data.

3.1.3 Secure archive storage is cloud storage in the UK with additional security, that is only accessible to a small number of Wickenstones team members.

3.1.4 Wickenstones' policy for information security must be followed in order to keep personal data secure.

3.1.5 Personal data should not be disclosed to unauthorised people, either within the company or externally.

3.1.6 Employees should request help from their client lead, personal development manager, or the project support lead if they are unsure about any aspect of data protection.

4. Data protection authorities and representatives

4.1 The data protection authority for Wickenstones UK is the Information Commissioner's Office (ICO) in the UK.

4.2 The data protection authority for Wickenstones EU is the Data Protection Commission in Ireland.

4.3 Wickenstones US has appointed Wickenstones EU as its data protection representative in the European Union. Wickenstones US nominates the Data Protection Commission in Ireland as its data protection authority.

5. Subject access requests

5.1 A subject access request is a request by a person to see all of the data Wickenstones holds about them. The requester does not have to use the phrase 'subject access request' for their request to be considered and processed as a subject access request.

5.2 The project support lead is responsible for handling subject access requests. The main method of making a subject access request is to email GDPR@wickenstones.co.uk. However, subject access requests that arrive through other channels, including by post, on the telephone or by email to a different member of staff, should be immediately passed on to the project support lead.

5.3 There is no charge for a subject access request unless that request is manifestly unfounded or excessive.

5.4 Except where an exemption in the GDPR legislation applies, the project support lead will be responsible for verifying the identity of the requester, gathering all data held about the requester, which may include instructing other members of staff to search for and supply data, and submitting data to the requester within one month of the request being received. If a GDPR exemption applies, the project support lead will respond to the requester explaining this within one month.

5.5 Unless otherwise specified by the requester, we will assume that any subject access request pertains to data held by all three Wickenstones entities and will respond accordingly.

5.6 The names of individuals who have made subject access requests will be stored by the project support lead indefinitely, for the purpose of identifying repetitive requests, and as proof of compliance with GDPR. These names will be treated as personal data, and stored and processed according to this policy. The project support lead will be responsible for informing requesters of this.

6. The right to erasure

6.1 The individuals about whom Wickenstones holds personal data have the right to ask us to permanently delete their data. This is also known as the right to be forgotten. Where the terms 'right to erasure' or 'right to be forgotten' are not used in the request, the project support lead will decide whether to process the request as a right to erasure request.

6.2 The project support lead is responsible for handling right to erasure requests. The main method of making a right to erasure request is to email GDPR@wickenstones.co.uk. However, right to erasure requests that arrive through other channels, including by post, on the telephone, or by email to a different member of staff, should be immediately passed on to the project support lead.

6.3 Except where an exemption in the GDPR legislation applies, the project support lead will be responsible for verifying the identity of the requester, ensuring the deletion of all personal data

relating to them within one month, and responding to the requester. This may include instructing other members of staff to search for and delete data. It is not possible to guarantee that personal data will not be collected and processed again in the future, if it continues to be available from public domain sources.

6.4 Unless otherwise specified by the requester, we will assume that any erasure request pertains to data held by all three Wickenstones entities and will respond accordingly.

7. The right to object to processing

7.1 The individuals about whom Wickenstones holds personal data have the right to object to us processing their data.

7.2 The project support lead is responsible for handling objections to data processing. The main method of objecting to data processing is to email GDPR@wickenstones.co.uk. However, objections to data processing that arrive through other channels, including by post, on the telephone, or by email to a different member of staff, should be immediately passed on to the project support lead.

7.3 Except where an exemption in the GDPR legislation applies, the project support lead will be responsible for verifying the identity of the requester, ensuring the processing of their data to which they are objecting is stopped within one month, and responding to the requester. If a GDPR exemption applies, the project support lead will respond to the requester explaining this within one month.

7.4 Unless otherwise specified by the requester, we will assume that any objection to processing pertains to data held by all three Wickenstones entities and will respond accordingly.

8. Data breach reporting

8.1 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.

8.2 Any member of staff or person acting on behalf of Wickenstones that becomes aware of a data breach must report it to the umbrella cluster lead as a matter of urgency, even on a non-working day or outside of working hours. If the umbrella cluster lead is not immediately available, the director must be contacted, and failing that, another member of the senior leadership team.

8.3 The umbrella cluster lead (or other member of the senior team, if not available) will be responsible for identifying whether the breach was of data for which Wickenstones is a data controller, and/or if a third party such as a client is a data controller:

8.3.1 If Wickenstones is a data controller, the umbrella cluster lead will consult with the director, and if necessary will report the breach to the appropriate data protection authority within 72 hours. If the data breach is likely to be detrimental to the data subjects, then the umbrella cluster lead and director will agree to inform the data subjects of the breach and the umbrella cluster lead will be responsible for actioning this.

8.3.2 If a third party is a data controller, or a co-controller, the umbrella cluster lead will be responsible for consulting with the director and if necessary, arranging for that third party to be informed, within 24 hours wherever possible. If the third party is a client, then the corresponding client lead will inform the client.

9. Data protection and privacy awareness and training

9.1 The project support lead is responsible for arranging data protection and privacy training, ensuring that:

9.1.1 All staff are aware of the need to protect personal data

9.1.2 All staff know what constitutes personal data

9.1.3 All staff understand the actions they need to take to comply with this policy and with best practice

9.1.4 All staff know how to find out further information and guidance on data protection issues

9.1.5 Cluster leads understand their responsibilities in relation to data protection within their projects and client relationships

9.2 Training should take place at least once a year to provide a refresher and encompass any updates to data protection legislation or to this policy.

10. Data transfers

10.1 Wickenstones seeks to minimise the transfer of personal data wherever possible. This includes, but is not limited to, use of cloud-based software or services and third party suppliers to process data, as well as sharing personal data with clients.

10.2 When transferring personal data is necessary to the running of our business or the execution of our project work, we enact the following safeguards:

10.2.1 Before the transfer, we confirm that recipients have appropriate data protection measures in place, including written processes, notices or policies for the protection of data which are at least as robust as the requirements of the GDPR

10.2.2 Before the transfer, recipients are required to sign an agreement which stipulates their role (processor or co-controller) and how they will process the data.

10.2.3 Where applicable, organisations to whom data are transferred are named in privacy notices to the data subjects

10.3 Wickenstones avoids making restricted transfers (transferring personal data outside of the EU and UK) wherever possible. One way we do this is by considering whether the same purpose can be achieved without sending personal data, or whether we can use a data processor in the UK or EU instead.

10.4 When we make restricted transfers from Wickenstones UK or Wickenstones EU to Wickenstones US, we use standard contractual clauses (SCCs) as the safeguard for the transfer.

10.5 In other instances, we ensure that appropriate safeguards are in place with the third party, such as SCCs or a UK/EU GDPR adequacy decision for the destination country.

10.6 When we make a restricted transfer, we will make all reasonable attempts to inform the data subjects of the transfer and of the safeguard(s) in place, if possible before the transfer occurs.

11. Data retention times – summary

The summary below is intended as a quick reference for Wickenstones staff. It is not exhaustive and does not supersede anything stated elsewhere in this policy or the attached privacy notices. Where applicable legislation requires us to keep data longer than listed below, the legislation must be followed.

Type of data (in digital format unless otherwise specified)	**Maximum duration of storage**
Job applicant CVs and associated documents e.g. cover letters	If unsuccessful: six months If successful: for duration of employment plus three years
Names and email addresses of job applicants	Two years
Staff name, salary/payment, dates of employment/contract, and reason for leaving	For duration of employment/contract plus 10 years
Staff performance management, disciplinary, grievance, sickness, salary and bonus details, right to work in UK, copy of passport and permits, contact details	For duration of employment plus three years
Staff out of pocket expenses	10 complete tax years
Staff out of pocket expenses with names removed	Indefinitely
Staff national insurance number, bank details, tax code, childcare voucher claims, date of birth, names and contact details of references	For duration of employment plus six months
Expert adviser/ KOL basic details (data that can be or has been found in the public domain, such as name, job title, country of practice, email address, work place and areas of expertise)	Indefinitely unless the adviser/KOL does not agree to participate in three consecutive projects, then up to three months after third failed attempt.
Adviser personal details supplied for a particular project e.g. professional registration numbers, bank details, passport number	One month after end of project
Project participant name, confirmation of attendance, opinions, contact details for follow up	As per project data protection plan
Honoraria and out of pocket expenses paid to advisers	Six complete tax years after the end of the project
Client names and contact details on CRM	Indefinitely (recipients of CRM communications are given regular notifications and opportunities to exercise their rights under GDPR)
Client contact details outside of CRM	Up to three years after last collaboration
Client names outside of CRM	Up to ten years after last collaboration
Patient data	As per project data protection plan