# PERSONAL DATA PROTECTION AND PRIVACY POLICY

Last reviewed: 12 February 2020

Next review due: 13 February 2021

## 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:

1.4.1 All staff of Wickenstones
1.4.2 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 The company's CEO is ultimately accountable for ensuring that Wickenstones meets its legal obligations.

2.3.2 The head of business support and managing director 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 dealing with subject access requests and requests for data erasure

2.3.2.4 reporting any data breach to the appropriate authorities

2.3.2.5 checking and approving any contracts or agreements with third parties that may handle 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 Client 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 business support team 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.

2.3.3.5 If gathering personal data directly from data subjects, issuing those individuals with a suitable privacy notice, in consultation with the business support team.

## 3. General staff guidelines for data storage and access

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

3.1.1 The only people able to access data covered by this policy should be those who need them for their work.

3.1.2 Data that are no longer in use should be deleted. They may be backed up to secure offline storage first, only under the following circumstances:

3.1.2.1 If the data may be required for legal reasons or the fulfilment of a contractual obligation

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

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

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

## 4. Subject access requests

4.1 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.

4.2 The business support team 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 business support team.

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

4.4 Except where an exemption in the GDPR legislation applies, the business support team 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, business support team will respond to the requester explaining this within one month.

4.5 The names of individuals who have made subject access requests will be stored by the business support team 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 business support team will be responsible for informing requesters of this.

## 5. The right to erasure

5.1 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 business support team will decide whether to process the request as a right to erasure request.

5.2 The business support team 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 business support team.

5.3 Except where an exemption in the GDPR legislation applies, the business support team 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. If deleting all data may put the requester at risk of being having their data processed by us again in the future, the business support team will inform the requester of that risk and give them the option of having their name and their preference to not have their data stored, retained. If a GDPR exemption applies, the business support team will respond to the requester explaining this within one month.

## 6. The right to object to processing

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

6.2 The business support team 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 business support team.

6.3 Except where an exemption in the GDPR legislation applies, the business support team 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 business support team will respond to the requester explaining this within one month.

## 7. Data breach reporting

7.1 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.

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

7.3 The head of business support (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 the data controller, or data for which a third party such as a client is the data controller:

7.3.1 If Wickenstones is the data controller, the head of business support will consult with the CEO, and if necessary will report the breach to the ICO within 72 hours. If the data breach is likely to be detrimental to the data subjects, then the head of business support and managing director will agree to inform the data subjects of the breach and the head of business support will be responsible for actioning this.

7.3.2 If a third party is the data controller, or a co-controller, the head of business support will be responsible for consulting with the managing 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 or managing director will inform the client.

## 8. Data protection and privacy awareness and training

8.1 The head of business support is responsible for arranging data protection and privacy training, ensuring that:

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

8.1.2 All staff know what constitutes personal data

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

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

8.1.5 Client leads understand their responsibilities in relation to data protection within their projects and client relationships

8.2 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.

## 9. 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.

| Type of data (in digital format unless otherwise specified) | Maximum duration of storage |
|---|---|
| Applicant CVs and associated documents e.g. cover letters | If unsuccessful: six months<br>If successful: for duration of employment plus one year |
| Printed CVs/associated documents | 24 hours |
| Names and email addresses of 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 one year |
| Staff out of pocket expenses | If against a project: two complete tax years after the end of the project<br>If not against a project: 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 two months |
| Expert adviser/ KOL basic details | Indefinitely unless the adviser/KOL doesn't 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 | Two complete tax years after the end of the project |
| Client names and contact details on CRM | Indefinitely |
| 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 |
| Emails in Outlook | One year |
| Emails in secure back-up storage | Ten years |