SERENA FORDHAM ENTERPRISES LTD, FOR HER GROUP LTD & NORFOLK MUMS

Records Management Policy

RECORDS MANAGEMENT POLICY

Table of Contents:

1 Document Control

Document owner	Serena Fordham Managing Director and Founder
Prepared by	John Fordham Glow Virtual Assistants Operation Manager
Reviewed by	Serena Fordham Managing Director and Founder
Approved by	Serena Fordham Managing Director and Founder
Approved on	1st May 2018 (Updated 30th October 2018)
Next review date	1st April 2019
Reference	RMP_002
Version	1.0
Classification	Public

Distribution list	
Managing Director	To approve and authorise
All Staff	To understand and comply

Communication	The Records Management Policy is communicated to all members of staff via email and records management awareness training.

2 Introduction

Serena Fordham Enterprises Limited, For HER Group Limited and Norfolk Mums ('The Companies') is registered with the Information Commissioners Office (ICO).

The Companies recognise the General Data Protection Regulation (GDPR) and will endeavour to ensure that all personal data is processed in compliance with this regulation from 25 May 2018, the date the regulation comes into force.

This Records Management Policy is written specifically to ensure appropriate compliance with the GDPR and has used the ICO self-assessment guidance for small organisations as at February 2018 for guidance as to the requirements.

3 General Statement of The Companies Scope

The Companies process relevant personal data regarding their members of staff, their clients and their client's customers, or their client's prospective customers, as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Should the scope of the business undertaken by The Companies change, this Policy will be updated to reflect the changes in relation to compliance with the GDPR.

The Companies only operate within the European Union.

4 Purposes of this policy

The Companies records are important sources of The Companies and client information, and therefore crucial to the current and future operations of the business. This Policy has been implemented to help the business:

- Meet its legal obligations under the appropriate regulations,
- Support the objective of maintaining the business as an effective and developing going concern; and
- Manage information resources effectively, by making sure records can be located, accessed, interpreted, trusted and maintained.

The Managing Director and managers of The Companies believe that administrative and management processes benefit from a system of records management that enables it to meet the purposes listed above.

This Policy should be read in conjunction with the Data Protection Policy and the Information Security Policy.

5 Scope of this Policy

The Managing Director has the overall responsibility for the implementation of this policy in the business, with day-to-day responsibility delegated to the managers and other staff.

A record is information created, received and maintained as information by The Companies or their staff in pursuance of the transaction of business.

Records can be in either paper or electronic format and both formats are covered by this policy.

This document sets out the overall framework within which staff should manage records.

Should it become necessary, the Managing Director or designated manager will produce operational procedures and guidance to help members of staff implement the objectives of this policy.

6 Responsibility for Records Management

All members of staff who create, store, receive and use records must:

- Treat all records as The Companies resource;
- Ensure as far as practicably possible that records are accurate and filed in such a way that they can be easily located, either electronically or physically;
- Keep records no longer than they are needed;
- Keep confidential records in a secure environment;
- Keep records stored in a safe and cost-effective way;
- Allow people to access information only if they need or have a right to do so;
- Create records that are accurate and that do not defame another individual, expose the business to unnecessary risk or to tamper with records in a way that risks them becoming inaccurate;
- Save long term records in an open source or archival format to ensure readability even if systems change.

Where appropriate, managers are responsible for ensuring that the actions listed above are communicated to, and carried out by, the members of staff whom they manage.

All staff shall ensure that records kept are secure and in line with the Information Security Policy and relevant regulation. In addition, staff developing new procedures for records management will take account of the Information Security Policy.

The Managing Director and designated managers will advise on records management procedures and best practice and provide guidance on how to achieve best practice.

The Managing Director will be responsible for The Companies being compliant with regulations and professional standards which are relevant to the area of records management.

7 Standards and Processes

The following standards and processes are employed by The Companies in relation to records management undertakings:

7.1 Creation and storing of records

7.1.1 The Companies client records

Paper or electronic records related to The Companies clients, or potential clients, can only be established with written consent from the client, typically this will be in the form of a signed contract. Any deviation from this standard will be on a case by case basis and with the approval of the Managing Director or a designated manager.

7.1.2 Client customer records

Paper or electronic records related to The Companies client customer data, or client prospective customer data, can only be established with written consent from the client, typically this will be in the form of a signed contract. Any deviation from this standard will be on a case by case basis and with the approval of the Managing Director or a designated manager.

7.1.3 Permissions capture

Where client customer or prospective customer data is being captured electronically, typically through sign up forms on websites, the standard approach of The Companies is to use 'double opt-in' which is compatible with the GDPR principles. The use of double opt-in is accepted by existing clients and will be the approach recommended to new clients going forward.

Where client customer or prospective customer data is being captured manually, once collected, the manual records are captured electronically with a double opt-in request subsequently being issued.

7.1.4 Manual and electronic record keeping systems

The Companies manual record keeping comprises of capturing details on manual HER Business Revolution sign in sheet, which is then captured electronically with a double opt-in request subsequently being issued.

The Companies electronic recording keeping largely comprises of data related to staff (e.g. for salary payment), to clients (e.g. for raising of invoices, access to software and systems) and to client's customers or prospective customers (e.g. for marketing purposes).

Electronic data is stored across a number of systems. The Companies will conduct an information audit with associated data flows to identify the systems on which it has data stored. The information audit is retained centrally and updated at least annually.

7.1.5 Data is accurate, adequate, relevant and not excessive

The Companies will strive to ensure that the personal data they collect is accurate, adequate, relevant and not excessive.

Where data relates to The Companies staff and clients, only the minimum required to perform the relevant task is collected and stored.

Where data relates to a client's customers or prospective customers, The Companies staff will work with the requesting client to ensure that the data is fit for purpose and is not excessive, raising any concerns with the Managing Director for further consideration.

7.2 Movement of manual records

Manual records are only kept as sign in sheets for HER Business Revolution meetings, which are stored for accounting purposes in the company invoice folder, and destroyed in line with regulation.

7.3 Retention and deletion of records

The Companies will only retain records for the purpose of their business, that is, records related to The Companies staff and for the completion of client instructed tasks, within regulatory guidelines.

Deletion of records will employ best practice as is appropriate at the time. Generally, manual records will as a minimum be shredded, with electronic records being deleted and removed from any history files (deletion from 3rd party systems will utilise the 3rd party deletion routines).

8 Training

The Managing Director and designated managers will be responsible for organising an appropriate amount and level of records management training for relevant members of staff. Training will be delivered periodically alongside related training (Data Protection and Information Security).

Training will be tailored to meet the requirements for the induction of new staff and refresher training for existing staff.

The training will be allocated a dedicated agenda item at the regular team meetings.

9 Contractual Requirements

Written agreements with clients and with 3rd party service providers will include information security conditions where this is considered to be appropriate.

Where The Companies have control over contractual arrangements, for example, contracts with its clients, The Companies will endeavour to ensure that appropriate information security conditions are considered and accepted.

Where The Companies generally have no control over contractual conditions with 3rd party service providers, The Companies will review the contractual terms and consider on a case by case basis whether it is appropriate to agree to the terms or to seek another provider.