Data Protection Policy – THREAD RETAIL UK LTD
T/A "AFIELD"

Policy information	
Organisation	Thread Retail UK Ltd "the Data Controller" (see notes).
Scope of policy	The policy applies to all operational branches (including offices overseas) which the Data Controller is responsible for.
Policy operational date	Takes effect 01.09.16
Policy prepared by	Anthony Wands
Date approved by Board/ Management Committee	Approved by Board: 25 August 2016
Policy review date	Next due: 25 August 2018

Introduction	
Purpose of policy	• complying with the law • following good practice • protecting clients, staff and other individuals • protecting the organisation
Brief introduction to Data Protection Act 1998	Taken as read and available to staff
Data Protection Principles	Over-riding principal is to be full compliance with best practice
Personal data	Applies to all data in respect of clients, members of public, 3rd parties which interface with Thread and Thread staff themselves.
Policy statement	We commit to: • comply with both the law and good practice • respect individuals' rights • be open and honest with individuals whose data is held • provide training and support for staff who handle personal data, so that they can act confidently and consistently • Notify (see notes) the Information Commissioner voluntarily, even if this is not required
Key risks	• Public names, addresses, e mails and phone numbers • Public credit card information (redacted on reports; complete if over telephone) • Banking details (if refunds requested by BACS) • Data on our staff • We note that such information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information is a grave concern as well as which individuals may be harmed through data being inaccurate or insufficient

Responsibitilies	
Trustees	The Trustees are the Board of the Company TA Wands; M Scholes, Christopher Scholes
Data Protection Officer	TA Wands responsible for • Briefing the board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification (see notes) • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors (see notes)
Specific other staff	None
Team/Department managers	N/A Though Mark Scholes accepts responsibility for any data held in our Sri Lanka or Turkey offices and reports to TA Wands in this respect
Staff & volunteers	All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'staff' is used, this includes both paid staff and volunteers.)
Enforcement	Failure by Staff will result in disciplinary action and reporting any breach to the authorities.
Confidentiality	
Scope	• Information about the organisation (and its plans or finances, for example) • Information about other organisations, since Data Protection only applies to information about individuals • Information which is not recorded, either on paper or electronically • Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a "relevant filing system" in the Data Protection Act
Understanding of confidentiality	The Data officer keeps a list of access, to which data, for which purposes. Access in this case means not just by staff, but also by people outside the organisation. Access is granted on a "need to know" basis; no one should have access to information unless it is relevant to their work. If there are doubts as to what constitutes confidentiality, The Data officer should be contacted. There is be a procedure for deciding on a case-by-case basis whether this is appropriate but all rulings will be reported to Trustees.
Communication with Data Subjects	Data Officer will communicate with all staff directly
Communication with staff	See above
Authorisation for disclosures not directly related to the reason why	1) those likely to be at the instigation, or in the interests, of the Data Subject, and 2)those which are made in the course of official investigations.

data is held	For the first (such as a financial reference request from a bank), consent from the Data Subject is likely to be the normal authorisation. This consent should be recorded. For the second, it may be appropriate for the Data Subject not even to be informed; authorisation should be made only by the Board

Security	
Scope	Security must not be confused with confidentiality. The latter is about defining what is allowed — setting the boundary; the former is about ensuring that the boundary is maintained. However, there must be a relationship between the two. Like confidentiality, security is not wholly a Data Protection issue. Again, a separate policy may be preferable. The entries for business continuity and personal security below are those with least Data Protection relevance.
Setting security levels	The greater the consequences of a breach of confidentiality, the tighter the security should be.
Security measures	• password protection on all applications • clear desk policy at lunchtime and night • entry control to data room • Inadmissable any photocopying, manual copying of data •
Business continuity	Data is held remotely in Brighton (2 locations); Manchester and Pofrtugal
Specific risks	Those associated with online transactions
Personal safety	Separate policy is in place

Data recording and storage	
Accuracy	Where information is taken over the telephone, it must be repeated back with the individual? If information is supplied by a third party, we will specifically request their guarantee of such data
Updating	Data is reviewed and stored remotely monthly.
Storage	See above.
Retention periods	5 years for all data.
Archiving	Hard copy data is stored in ther Company's warehouse; it is protected by fire and alarm systems in common with all warehouse goods

Subject access	
Responsibility	TA Wands is responsible for all data and to ensure it will be handled within the legal time limit of 40 days.
Procedure for making request	Subject access requests must be in writing. There is a clear responsibility on all staff to pass on anything which might be a subject access request to the appropriate person without delay.
Provision for verifying identity	n/a (small enterprise).
Charging	No charge
Procedure for granting access	Normally provision is for the required information to be provided "in permanent form".

Consent	
Underlying principles	Consent from the individual is one way of complying with the Fair Processing Conditions. Where data is being processed without consent it is still very important to ensure that the Data Subject knows what is being done.
Forms of consent	Consent implicit and in terms of website display
Opting out	Even where the organisation is not relying on consent, it may wish to give people the opportunity to opt out of their data being used in particular ways.
Withdrawing consent (eg marketing)	Consent can be withdrawn, but not retrospectively. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

Direct marketing	
Underlying principles	We apply this to all instances of marketing using e mails, mailing lists, social media etc
Opting out	Data Subjects have the right to require their data not to be used for marketing, we follow good practice to make it clear when there is an intention to use their data for marketing and offer them an opt-out (via a tick-box or an easy-to-use alternative) at the earliest opportunity.
Sharing lists	Not envisaged nor contemplated
Electronic contact	Because of the Data Protection and Privacy (EC Directive) Regulations 2003 most electronic marketing (by phone, fax, e-mail or text message) either requires consent in advance, or it is good practice (and administratively easier) to obtain consent. See above

Staff training & acceptance of responsibilities	
Documentation	Induction pack.
Other related policies	Treating client fairly
Induction	Part of protocol
Continuing training	If there are opportunities to raise Data Protection issues during staff training, team meetings, supervisions, etc, this will take place.
Procedure for staff signifying acceptance of policy	Implicit in terms of employment contract

Policy review	
Responsibility	The Board
Procedure	Data Officer (TA Wands) to table report to Board and make recommendations (if any) and allow Board time to review current policy.
Timing	Review in a period of at least 2 months prior to Board Meeting.