6.5 Data Protection Policy

- **Introduction**

The Data Protection bill will replace the Data Protection Act (1998) and becomes enforceable beginning 25 May 2018
GDPR applies to how and why data is processed. It aims to give control back to citizens over their personal data and unify regulations within the EU. In addition, it places significantly more legal liability on the organisation (data controller) in relation to any breach. The legislation requires that each organisation shall be responsible for and be able to demonstrate, compliance with the principles. Information that applies to the GDPR is:

- Personal Data (Information relating to an individual whether it relates to his / her private, professional or public life – it can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking sites, medical information or an IP address.
- Sensitive Personal Data (Genetic data and biometric data that uniquely identifies an individual)

This policy has been written to guide staff and sets out the protocol for processing personal data and safeguarding individual's rights. Designed to help and encourage all employees of the company to achieve and maintain standards of conduct in their work in complying with GDPR legislation on behalf of The Braunstone Foundation (trading as b-inspired Ltd).

Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes: further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and where necessary, kept up to date: every reasonable step must be taken to ensure personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical

purposes subject to implementation of the appropriate technical and organisational freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Managers are responsible for ensuring that staff observe the standards set for working with personal data and should be able to demonstrate due diligence to customers, suppliers, volunteers and other contacts on behalf of the company.

The policy is subject to regular review to reflect, for example, changes to legislation or to the structure or amended policies of the Braunstone Foundation.

All staff are expected to apply the policy and to seek advice from their line manager when required.

- ## Implementing GDPR

The Braunstone Foundation needs to collect and use certain types of information about people with whom it deals in order to operate. These include current, past and prospective individuals within the community, The Braunstone Foundation's own employees, suppliers, students and others with whom The Braunstone Foundation conducts business. In addition, the Braunstone Foundation may occasionally be required by law to collect and use certain types of personal information to comply with the requirements of government departments, funding authorities and the Charities Commission. This personal information must be dealt with properly – whether it is collected on paper, electronically, or other means.

The Braunstone Foundation considers the lawful and correct treatment of personal information as important to the achievement of our objectives and to the success of our operations, in order to maintain confidence between those with whom we deal and ourselves.

Our data policy sets out our commitment to protecting personal data and how we safeguard and implement that commitment with regards to the collection and use of personal data ensuring it complies with GDPR

Processing Data

Within GDPR, there is a distinct difference between business to consumer (B2C) and Business to Business (B2B) marketing. Under GDPR, there are six equally valid grounds to process personal data:

The lawful basis for processing data are:

- The data subject has given consent to the processing of his/ her personal data for one or more specific purposes.

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority
- Processing is necessary for the purpose of the legitimate interests pursued by the controller.

There are two of these that are relevant to direct B2B marketing, they are *consent* or *legitimate interest.* GDPR states that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

Using *legitimate interest* as the basis for B2B marketing involves ensuring key conditions are met:

- The processing must relate to the legitimate interests of your business or a specified third party, providing that the interests or fundamental rights of the data subject do not override the businesses legitimate interest.
- The processing must be necessary to achieve the legitimate interests of the organisation.

Right of Access

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why we are using their data, and check it is being done lawfully.

Individuals have the right to obtain the following:

- Confirmation that we are processing their personal data;
- A copy of their personal data; and other supplementary information – this largely corresponds to the information that is provided in a privacy notice.

Personal data of the individual

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that we establish whether the information requested falls within the definition of personal data.

In addition to a copy of their personal data, we also have to provide individuals with the following information:

- the purposes of processing;
- Categories of personal data concerned;
- Recipients or categories of recipient you disclose the personal data to;
- Retention period for storing the personal data or, where this is not possible, criteria for determining how long it will be stored.
- Confirmation of the right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- The existence of automated decision-making (including profiling); and
- Safeguards you provide if Data is transferred.

An individual can make a subject access request verbally or in writing. It can also be made to any part of the organisation (including by social media) and does not have to be to a specific person or contact point. The GDPR does not prevent an individual making a subject access request via a third party. In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request.

A request does not have to include the phrase 'subject access request' as long as it is clear that the individual is asking for their own personal data.

All requests received whether verbal or in writing should be recorded on the form contained in this policy, dated and forwarded to the Head of Operations.

All requests received must be acted on at the latest within one month of receipt.

This timeframe can be extended by a further two months if the request is complex or the organisation has received a number of requests from the individual. The organisation must let the individual know within one month of receiving their request and explain why the extension is necessary.

If you have doubts about the identity of the person making the request - ask for more information. However, it is important that you only request information that is necessary to confirm identity.

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. The organisation does not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

The other individual has consented to the disclosure; or it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, the organisation must take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;

In the event that a request is manifestly unfounded or excessive The Braunstone Foundation will charge an administration fee and will not comply with the request until the fee has been received.

Control of Data

- **Staff responsibilities**
- Braunstone Foundation staff should acquaint themselves with the data protection policy and abide by recognised good practice in regard to data protection principles.
- Service Managers shall act as point of contact in ensuring that staff understand how to conform to the required standard. Ensuring that in any data captured complies with and is treated in accordance with the act.
- Head of Operations will ensure that adequate training and support is made available for all staff responsible for personal data, and ensure that staff know where to find/obtain further guidance ensuring that both internal and external queries about data protection, to the organisation, are dealt with effectively and promptly and individuals rights in regard to safeguarding data and the individual's right to inspect personal data are adhered to.
- The company will regularly review data protection procedures and guidelines.

Best –Practice Guidelines for employees of The Braunstone Foundation

- Acquisition of personal data. - Those wishing to obtain personal data must comply with guidelines issued from time to time by The Company and in particular:
    - Should outline to data subjects the purpose (s) for which they are gathering data, obtaining their explicit consent, and inform them that The Braunstone Foundation will be the controller for the purposes of GDPR. In addition, data subjects should be aware of any other persons/organisations to whom the data may be disclosed.
    - If personal data is collected, explicit consent is not only best practice, it is mandatory. No more data should be collected than is necessary for the purpose(s) declared.

- Holding / safeguarding / disposal of personal data
    - Data should not be held for longer than is necessary. For further information please see The Braunstone Foundations document retention policy or contact your line manager for guidance.
    - Personal data should be reviewed periodically to ensure it is up to date and accurate and to determine whether retention is necessary.
    - Where possible, personal data should be anonomised.
    - Adequate measures should be taken to safe guard data so as to prevent loss, destruction or unauthorised disclosure. The more sensitive the data, the greater the measures that need to be taken.

- Processing of personal data
    - In this particular context "processing is used in the narrow sense of editing, amending or querying data. In the context of the Act as a whole "processing" is very widely defined to include acquisition, passive holding, disclosure and deletion.
    - Personal data must not be processed except for the purpose (s) for which it was obtained or for a similar analogous (i.e. performing similar functions). If the new purpose is very different, the data subjects consent must be obtained.

- Disclosures and transfer of personal data

  The Braunstone Foundations policy is to exercise discretion under the GDPR to protect the confidentiality of those whose personal information is held.

    - Employees of The Braunstone Foundation may not disclose any information about its customers / suppliers / volunteers / contacts or employees, including information as to whether or not any person is or has been an a customer's / supplier / volunteer / contact or employee of The Braunstone Foundation unless they are clear that they have been given the authority to do so. Particular care should be taken in relation to any posting of personal information on the internet
    - No employee of The Braunstone Foundation may provide references to prospective employers/ customers / suppliers / volunteers / contacts or employees, or others without the consent of the individual concerned. It is therefore essential that where The Braunstone Foundation is given as a referee the subject of their reference should be provided to The Braunstone Foundation with the necessary notification and consent.
    - No employee may disclose personal data to the police or any other public authority unless that disclosure has been authorised by the Chief Officer, Head of Operations or Service Manager.

- Transfers

  Personal data should not be transferred outside The Braunstone Foundation, and in particular not to a country outside the EEA
    - except with the data subjects consent
    - unless that country's data protect laws provide adequate levels of protection
    - in consultation with the Chief Officer it is established that other derogations apply.

- Destruction of personal data

  Personal data must not be held for longer than specified in relation to its collection and when such data has been earmarked for destruction, appropriate measures must be taken to ensure that the data cannot be reconstructed and processed by third parties.

- **Review**

This policy will be reviewed periodically to take account of changes in the law and guidance issued by the Information Commissioner.

- **Data Protection Contacts**

  Angie Wright, Chief Officer or Linda Grubb, Head of Operations

  The Braunstone Foundation. Business Box,3 Oswin Road, Leicester LE3 1HR

- **Disciplinary Consequences of this Policy**

  Unlawful obtaining or disclosure of personal data (including the transfer of personal data outside the European Economic Area) in contravention or breach of the Data Protection Action 1998 by anyone connected with or to The Braunstone Foundation will be treated seriously by The Braunstone Foundation and may lead to disciplinary action up to and including dismissal

Request for personal information (Subject Access Request)

To be completed either by individual or Braunstone Foundation staff member where requests are made verbally. Please note, all forms should be dated.

Part A: Your details

We must be sure that we are releasing information to the right person. Please tell us the following information. We may ask you for further proof of identity or address details.

Full name:
Previous name(s) (if applicable):
Date of birth:
National Insurance number:
Full address (including postcode): Postcode:
Address, if different Please tell us about previous addresses (including postcode):

Part B: Personal information required

Please tell us what service you were supported by. This will help us deal with your request more quickly.

Tick the box to request information you require about your interaction with the Braunstone Foundation or use the space on the next page to describe any other information not listed below.

Please remember to tick **both** boxes if you require computer (system) **and** clerical (paper) records. If the box is not ticked, information will not be provided.

	Computer records	**Clerical records**
Summary of all personal and sensitive data This will provide you with list of all the data that we hold on you		

	Computer records	Clerical records
Summary of all case notes This will provide you with a copy of all case notes we hold on you		
Other Please list the names and addresses of the offices which may have your records. It would be helpful if you could also list the names / telephone or email addresses of staff you have dealt with.		
Other Please be as specific as possible for example information relating to an appeal, grievance or complaint made.		

Any other information:

Part C: Dates

What period you would like the personal information we send to you to cover?
This applies to **clerical records only**. Computer records will contain **all** data held on the Braunstone Foundations computer systems at the time of your request.
The Braunstone Foundation does not hold personal information indefinitely. It may be that some information has been destroyed in line with our Data Retention policies.

Personal information required for period	from: to:

Part D: Declaration

I declare that I have made a request for details of personal information held by the Braunstone Foundation as outlined above.

Signed:

Date :

Please return this form to a Braunstone Foundation office or via email to:

Mail: angie.wright@b-inspired.org.uk or to linda.grubb@b-inspired.org.uk

Address: Head Office, Business Box 3 Oswin Road. Leicester LE3 1HR or Neighbourhood Support team, 45 Wellinger Way. Braunstone, Leicester LE3 1RG

Request for personal information (Subject Access Request via a third party)

The Braunstone Foundation recognises that sometimes individuals agree to a third parties such as a solicitor, welfare rights organisation, government office or future employer seeking to obtain a copy of the personal information held by The Braunstone Foundation. However The Braunstone Foundation cannot disclose such information without lawful authority. The Braunstone Foundation takes the view that any consent to disclosure in these circumstances needs to be fully informed.

We have therefore developed a consent form which satisfies us that the individual is content for either all of some of the information to be realised to a third party. If you use this consent form in future applications for personal information, it will enable us to process applications without having to write to you for appropriate consent.

It is important that you complete as appropriate. The Braunstone Foundation may hold a large quantity of data about an individual and The Braunstone Foundation needs to ensure that we are providing only the information that is required.

Consent Form

- Please arrange for this consent form to be completed and returned to The Braunstone Foundation whose address can be found at the end of this form.
- The Braunstone Foundation needs to ensure that we have identified the correct individual and have traced the correct records. If you do not provide this information we may need to contact you to obtain it which will delay the receipt of the personal information you require.
- Both declarations **MUST** be completed. The Braunstone Foundation will not accept any consent form which uses another form of words.
- In the case of the individual having a disability which prevents them from completing section E please ask them to make contact with The Braunstone Foundation directly who may be able to arrange assistance with the issues.

Part A: Your details

We must be sure that we are releasing information to the right person. Please tell us who the information relates to. We will ask you, as a third party for proof of identity before we are able to release information.

Full name:
Previous name(s) (if applicable):
Date of birth:
National Insurance number:
Full address (including postcode): Postcode:
Address, if different Please tell us about previous addresses (including postcode):

Part B: Personal information required

Please tell us what service you were supported by. This will help us deal with your request more quickly.

Tick the box to request information you require about your interaction with the Braunstone Foundation or use the space on the next page to describe any other information not listed below.

Please remember to tick **both** boxes if you require computer (system) **and** clerical (paper) records. If the box is not ticked, information will not be provided.

	Computer records	**Clerical records**
Summary of all personal and sensitive data This will provide you with list of all the data that we hold on you		
Summary of all case notes This will provide you with a copy of all case notes we hold on you		
Other Please list the names and addresses of the offices which may have your records. It would be helpful if you could also list the names / telephone or email addresses of staff you have dealt with.		
Other Please be as specific as possible for example information relating to an appeal, grievance or complaint made.		

Any other information:

Part C: Dates

What period you would like the personal information we send to you to cover?
This applies to **clerical records only**. Computer records will contain **all** data held on the Braunstone Foundations computer systems at the time of your request.
The Braunstone Foundation does not hold personal information indefinitely. It may be that some information has been destroyed in line with our Data Retention policies.

Personal information required for period	from:	to:

To meet its obligations under the Data Protection Bill, The Braunstone Foundation needs to be satisfied that the individual named in section A has given consent to the release of personal information to a third party.

Part D: Declaration

I declare that I have made a request for details of personal information held by the Braunstone Foundation as outlined above via a third party and that the person listed in section E is my authorised representative.

Signed:

Date :

Part E – Consent

Insert the name of 3rd party	

Insert the position of the person or their relationship to you	
Inset the organisation name represented by 3rd party	
Insert the 3rd parties address	

Part E: Declaration

I declare that I am authorised to request details of personal information held by the Braunstone Foundation for the person named in section A.

Signed:
Date

Please return this form to a Braunstone Foundation office or via email to:

Mail: angie.wright@b-inspired.org.uk or to linda.grubb@b-inspired.org.uk

Address: Head Office, Business Box 3 Oswin Road. Leicester LE3 1HR or Neighbourhood Support team, 45 Wellinger Way. Braunstone, Leicester LE3 1RG

6.6 Document Retention

	RETENTION PERIOD
1. Bank Statements & Reconciliations	7 years
2. Cancelled Checks-(Important payments, purchases of property, tax payments large/significant contracts)	Permanent
3. Cancelled Checks (ordinary)	7 years
4. Cash Books	7 years
5. Construction Documents	Permanent
6. Contracts and Leases (current)	Permanent
7. Contracts and Leases (expired)	7 years
8. Corporate-Articles of Incorporation & By-Laws	Permanent
9. Corporate-Certificate of Incorporation and Related legal or government documents	Permanent
10. Corporate Minutes: Board/Committee meetings	Permanent
11. Correspondence (General)	3 years
12. Correspondence (Legal-important)	Permanent
13. Duplicate Bank deposit Slips	3 years
14. Email	5 years
15. Employee: employment records	7 years
16. Employee: Evaluations (current)	Permanent
17. Employee: Evaluations (after termination)	7 years
18. Employee: Payroll records	7 years
19. Employee: Payroll Reports (Fed./State)	7 years
20. Employee: Retirement records	Permanent
21. Employee: Workman's Comp. documents	11 years
21. Employment applications	1 years
22. Finance: Accounts payable-ledger/schedules	7 years
23. Finance: Accounts receivable-ledger/schedules	7 years
24. Finance: Audit reports of independent accountants	Permanent
25. Finance: General ledgers	Permanent
26. Finance: Tax returns—Federal 990's	Permanent
27. Finance: Tax returns—Federal (other)	Permanent
28. Finance: Tax returns---State/Local	Permanent
29. Finance: W-2, W-4,1099, etc.	7 years
30. Insurance: Policies (current)	Permanent
31. Insurance: Policies (expired)	Permanent
32. Invoices from vendors	7 years
33. Medical and Dental Claims	5 years

34. Paid Bills/Vouchers	7 years
35. Property documents-Deeds, appraisals, etc.	Permanent
36. Service provider contracts (current)	Permanent
37. Service provider contracts (expired)	7 years
38. Vendor payments	7 years
39. Vouchers	7 years

	RETENTION PERIOD
1. Bank Statements & Reconciliations	7 years
2. Cancelled Checks-(Important payments, purchases of property, tax payments large/significant contracts)	Permanent
3. Cancelled Checks (ordinary)	7 years
4. Cash Books	7 years
5. Construction Documents	Permanent
6. Contracts and Leases (current)	Permanent
7. Contracts and Leases (expired)	7 years
8. Corporate-Articles of Incorporation & By-Laws	Permanent
9. Corporate-Certificate of Incorporation and Related legal or government documents	Permanent
10. Corporate Minutes: Board/Committee meetings	Permanent
11. Correspondence (General)	3 years
12. Correspondence (Legal-important)	Permanent
13. Duplicate Bank deposit Slips	3 years
14. Email	5 years
15. Employee: employment records	7 years
16. Employee: Evaluations (current)	Permanent
17. Employee: Evaluations (after termination)	7 years
18. Employee: Payroll records	7 years
19. Employee: Payroll Reports (Fed./State)	7 years
20. Employee: Retirement records	Permanent
21. Employee: Workman's Comp. documents	11 years
21. Employment applications	1 years
22. Finance: Accounts payable-ledger/schedules	7 years
23. Finance: Accounts receivable-ledger/schedules	7 years
24. Finance: Audit reports of independent accountants	Permanent
25. Finance: General ledgers	Permanent
26. Finance: Tax returns—Federal 990's	Permanent
27. Finance: Tax returns—Federal (other)	Permanent
28. Finance: Tax returns---State/Local	Permanent
29. Finance: W-2, W-4,1099, etc.	7 years
30. Insurance: Policies (current)	Permanent
31. Insurance: Policies (expired)	Permanent

32. Invoices from vendors	7 years
33. Medical and Dental Claims	5 years
34. Paid Bills/Vouchers	7 years
35. Property documents-Deeds, appraisals, etc.	Permanent
36. Service provider contracts (current)	Permanent
37. Service provider contracts (expired)	7 years
38. Vendor payments	7 years
39. ERDF	25 years
40. Vouchers	7 years

B-Inspired Trading Ltd Records

Retention and Disposal Schedule

Scope

This Protocol sets out the procedures for managing the retention of documents within the organisation.

Introduction

The aim of this Retention Schedule is to provide a consistent approach to the way the organisation handles it records, and provide a clear set of guidelines to all staff, thereby supporting the organsiation's Record Retention and Disposal Policy.

What is a document Retention Schedule?

A Retention Schedule is a list of records that need to be kept by B-Inspired Trading Ltd for a specific length of time. This schedule contains recommended retention periods for records created and maintained by B-Inspired and refers to all information regardless of the media in which it is stored, i.e. manual files, photographs, computer files, etc.

- The Retention Schedule identity's records that need to be kept as a part of B-Inspired Trading Ltd funders requirements as well as preventing the premature destruction of records that need to be retained for a specific legal, financial or statutory period.

- It is important to remember that this Retention Schedule is a Corporate Document. This means that it could be used externally as a reference tool for members of the public when they wish to search for information under different legislative regimes.
- It is also a document that will require amending and updating as and when retention details change, new information is kept, or regulations and legislation that govern information and its use are introduced or altered.
- Alterations or temporary exceptions to the schedule may be appropriate in certain circumstances, provided consultation is undertaken with one of the Directors or Senior Managers prior to any adjustments being made.

- This Retention Schedule outlines the types of records that may fall within the document retention policy and the length of time the organisation should hold the record before taking disposal or archive action. Many retention periods are determined by law and contracts.

- Where available / appropriate the relevant legislation or statutory reason for keeping a record for a specific period of time has been included and the required disposal action once this document reaches the end of its 'retention lifecycle' has also been included. In conclusion good Records Management is not difficult; B-Inspired Trading Ltd needs to keep accurate and timely records for the appropriate period of time, making sure that obsolete records are securely disposed of in an appropriate manner.

Retention Schedules and the Data Protection Act (1998)

The Data Protection Act (1998) requires that personal data shall be:

- adequate, relevant and not excessive;
- accurate and where necessary kept up to date;
- not kept for longer than is necessary for its purpose.

This requires B-Inspired Trading Ltd and all organisations to have procedures in place, covering the review of information held on files. Such procedures include the establishment of a policy covering the retention and disposal of records.

- Unless otherwise stated, records containing personal data should not be held for longer than 6 years after the subject's last contact with the organisation. This period reflects the general time within which, under the Limitation Act (1980), a civil action could be brought before the Law Courts. It should also be noted that, under this Act, civil action could be taken up to 12 years following certain events. Examples of these can be seen in Appendix 1 .

- Exceptions to the six year period occur when records:
  - are held in legal documents 'under seal' where they may have to be retained for up to 12 years;
  - need to be retained because the information contained in them is relevant to legal action which has commenced or is due to commence;
  - are required to be kept for longer or shorter periods by statute;
  - are archived for historical purposes;
- - relate to individuals and providers of services who have, or whose staff have been judged unsatisfactory;
- - are held in order to provide for the Data Subject, aspects of his/her personal history.

The 'Record Status'

- 'C' (Current) - This document is for current use in the office only. Once the retention period for this record has been reached then the record should be disposed of securely either through confidential waste or by shredding.
- 'R' (Reviewable) - This document should be constantly reviewed for its relevance and disposed of after its business use or purpose no longer exists. The practitioner is given the option of disposal action or of retaining the record for a further period of time only if it is legitimately required.
- 'N' (Non-Reviewable) - Once the designated retention period has been decided the document should be destroyed and disposed of appropriately.
- 'P' (Permanent) - This document should be permanently preserved in an archive. Once this document's administrative use has ended it should be removed from the office and stored as a permanent record. Permanent files are normally kept for 100 years, after which time they are destroyed

Records that can be Destroyed after their Effective Use has Concluded

The types of records described below have no significant operational, informational or evidential value. They can therefore be destroyed as soon as they have served their primary purpose.

- Personal diaries, address books, etc.
- Requests for everyday information including general requests (e.g. when will my rubbish be collected).
- Requests for, and confirmations of, reservations for internal services (e.g. meeting rooms, car parking spaces, etc.) where no internal charges are made or required.
- Requests for, and confirmations of, reservations with third parties (e.g. travel, hotel accommodation,) after an invoice has been received.
- Fax Cover Sheets, E-mail messages (where they do not impact on a business decision or reflect the B-Inspired Trading Ltd's opinions).

- Compliment slips, message slips and similar items which accompany documents but do not add any value to them.
- Superseded address lists, distribution lists, etc.
- Duplicate documents for example drafts of documents, reports, emails etc.
- Working papers, where the results have been written into an official document and which are not required to support it.
- Announcements and notices of meetings and other events, and notifications of acceptance or apologies.
- Stocks of in-house publications which are obsolete superseded or otherwise not required e.g. magazines, marketing materials, directories, forms, and other material produced for wide distribution.
- Published or reference materials received from external organisations, which require no action and are not needed for record purposes, e.g. trade magazines, vendor catalogues, flyers, newsletters.

This is by no means an exhaustive list but is instead intended to provide an indication of the type of documents that are considered as having no significant operational, informational or evidential value and therefore can be destroyed immediately after their effective use has ended. If you are unsure please contact your manager for further advice.

This Retention Schedule has been developed to be used in the following ways:

When new records are created

The Retention Schedule should be used as a reference document for the day to day management of records. The most effective point is when the record is created. This moment should be used to decide how long it should be retained, and for what reason it should be stored.

When opening a new file, creating an electronic record or typing a letter, the Document Retention and Disposal Schedule is designed to act as a guide to the conditions under which that record should be managed, stored and ultimately disposed of.

When designing or implementing new paper filing systems

Any new office system intended to improve the efficiency of paper filing should be designed with; a clear understanding of the legal and business requirement for record keeping, when records should be transferred to an off-site location and when they should be permanently destroyed.

When transferring files to off-site or to an archive facility

Office space is at a premium and it is rarely possible to retain files on-site for the length of time for which they have to be retained. The Retention Schedule should always be consulted when considering the transfer of files to an off-site or archive location.

When destroying files

In order to protect the B-Inspired Trading Ltd and minimise risk, all service areas should not maintain records longer than they need to; nor should they destroy records prematurely.

In addition to a register of when documents are destroyed should also be maintained to evidence compliance with the stated retention guidelines.

Electronic Records Management System

Any Electronic Document & Record Management (EDRM) System should manage not only electronic records but also paper records, and ensure that all legal and business requirements are met in terms of the retention, security and disposal of all electronic records (including e-mail, electronic forms, website content and images).
The integration of EDRM into existing business systems must include proper guidance which is consistent with legal and operational requirements.

Responsibility for Implementing and Monitoring

When a record has reached the end of its specific retention period, the service manager needs to be responsible as the signatory for;

- the destruction process where destruction is the specified action
- transferring the record into a box for archiving within the organising
- The records should be regularly updated to account for any changes to business practice and reviewed regularly as a matter of best practice.