Data Protection Policy and Procedures

The purpose of this policy is to set out the Little Hiccups commitment and procedures for protecting personal data. Little Hiccups is committed to a policy of protecting the rights and privacy of individuals, Little Hiccups needs to collect and use certain types of Data in order to carry on our work. This personal information must be collected and dealt with appropriately.

The Data Protection Act 2018 (UK GDPR) (DPA) and the General Data Protection Regulation 2018 (GDPR) governs the use of information about people (personal data). Personal data will only be held in secure, encrypted cloud based applications and includes email, minutes of meetings, membership forms and photographs. Little Hiccups will remain the data controller for the information held. Little Hiccups and volunteers will be personally responsible for processing and using personal information in accordance with the Data Protection Act and General Data Protection Regulation.

Trustees and volunteers running Little Hiccups who have access to personal information, will be expected to read and comply with this policy.

Little Hiccups has appointed a Data Protection Controller (DPC) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 2018 (UK GDPR). The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy.

The Data Protection Officer (DPO) on the Trustees is:

Name: Miriam Watson-Pratt

Contact Details: miriam@littlehiccups.co.uk

The Queen's Award for Voluntary Service

The Data Protection Act Legislation

This contains 8 principles for processing personal data with which Little Hiccups will comply.

Personal data covers both facts and opinions about an individual where that data identifies an individual. For example, it includes information necessary for volunteering such as a volunteer's name and address. Personal data may also include sensitive personal data as defined in the Act.

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s)
4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

Applying the Data Protection Act within Little Hiccups

Whilst access to personal information is limited to the Trustees and volunteers at Little Hiccups, volunteers at Little Hiccups may undertake additional tasks which involve the collection of personal details from members of the public.

In such circumstances we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

Accuracy

Little Hiccups will endeavour to ensure that all personal data held in relation to all data subjects is accurate. Data subjects must notify the data processor of any changes to information held about them. Data subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.

Enforcement

If an individual believes that Little Hiccups has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, the Trustees should utilise the Little Hiccups grievance procedure and should also notify the DPC.

Responsibilities

Little Hiccups is the Data Controller under the Act, and is legally responsible for complying with the Act, which means that it determines what purposes personal information held will be used for.

The Trustees will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information,
- Meet its legal obligations to specify the purposes for which information is used,
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- Ensure the quality of information used,
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information
- Take appropriate technical and organisational security measures to safeguard personal information,
- Ensure that personal information is not transferred abroad without suitable safeguards,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- Set out clear procedures for responding to requests for information

The Trustee responsible for records management responsibilities is:

Name: Miriam Watson-Pratt

Contact Details: miriam@littlehiccups.co.uk

The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so

- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- Dealing promptly and courteously with any enquiries about handling personal information
- Describe clearly how it handles personal information
- Will regularly review and audit the ways it hold, manage and use personal information
- Will regularly assess and evaluate its methods and performance in relation to handling personal information
- All staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018 (UK GDPR).

In case of any queries or questions in relation to this policy please contact Little Hiccups Data Protection Officer.

Data collection

Processing of Personal Data

Consent may be required for the processing of personal data unless processing is necessary. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with appropriate consent.

Little Hiccups processes some personal data for direct marketing and fund-raising purposes, data subjects have the right to request an opt-out to these activities at any point, which must be respected.

Sensitive Personal Data

Little Hiccups may, from time to time, be required to process sensitive personal data. Sensitive personal data includes data relating to medical information, gender, religion, race, sexual orientation, trade union membership and criminal records and proceedings.

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPC.

Informed consent

Informed consent is when

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- and then gives their consent.

Little Hiccups will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, Little Hiccups will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

When personal details are collected, Little Hiccups will ensure that they are only obtained through an 'opt in' option rather than 'opt-out'.

Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised volunteers.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

It is Little Hiccups' responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Little Hiccups and therefore all staff are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.

In most cases, personal data must be stored in appropriate systems and be encrypted when transported offsite.

External Processors

Little Hiccups must ensure that data processed by external processors, for example, service providers, Cloud services including storage, web sites etc. are compliant with this policy and the relevant legislation.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018 (UK GDPR) and the General Data Protection Regulation 2018.

Data Subject Access Requests

Data subjects have the right of access to information held by Little Hiccups, subject to the provisions of the Data Protection Act 2018 (UK GDPR) and the Freedom of Information Act 2000. Any data subject wishing to access their personal data should put their request in writing to the DPC. Little Hiccups will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 40 days for access to records and 21 days to provide a reply to an access to information request. The information will be imparted to the data subject as soon as is reasonably possible after it has come to Little Hiccups' attention and in compliance with the relevant Acts.

Exemptions

Certain data is exempted from the provisions of the Data Protection Act which includes the following:-

- National security and the prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Little Hiccups, including Safeguarding and prevention of terrorism and radicalisation

Disclosure

Little Hiccups may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Little Hiccups to disclose data (including sensitive data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting vital interests of a Data Subject or other person
- The Data Subject has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion
- Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

Little Hiccups regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Little Hiccups intends to ensure that personal information is treated lawfully and correctly.

Befriending and Personal Contact Outside of Little Hiccups

Little Hiccups recognises that friendships and supportive relationships may naturally develop between families, volunteers, and individuals involved in our activities. While we encourage community and connection, it is important to distinguish between interactions that are part of official Little Hiccups activities and those that occur independently.

Sharing of personal contact details (such as phone numbers or social media accounts) is a personal choice and is not facilitated or endorsed by Little Hiccups. Once contact is made outside of our organised activities, these interactions are considered personal and fall outside the scope of Little Hiccups' responsibility and safeguarding framework.

We ask all participants to respect privacy, maintain appropriate boundaries, and ensure that any sharing of information is consensual and in line with our safeguarding and data protection policies.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of Little Hiccups is not damaged through inappropriate or unauthorised access and sharing.

Destroying personal data.

Personal data should only be kept for as long as it is needed i.e. only keep that data for the duration of administering the campaign/project and securely dispose of once the promotion and monitoring period is complete. If a customer is housebound and receives regular visits from a volunteer – ensure the list is securely stored and remove customer details when they change or the customer no longer receives the service. Review the list annually. We will ensure that this information is confidentially destroyed at the end of the relevant retention period.

Further information

If members of the public/or stakeholders have specific questions about information security and data protection in relation to Little Hiccups please contact the Data Protection Officer:

The Information Commissioner's website (www.ico.gov.uk) is another source of useful information.

Policy agreed by Trustees on:

Signed by Chairperson:

To be reviewed:

The Queen's Award for Voluntary Service

Little Hiccups, The Barrowbys, Barrowby Lane, Garforth, Leeds LS25 1NG
07831 230741 **info@littlehiccups.co.uk** **www.littlehiccups.co.uk**
Registered Charity No: 1170147 Company Limited by Guarantee No: 9692276

APPENDIX 1: Technical Terms

The following list contains definitions of the technical terms we have used and is intended to aid understanding of this policy:

Data Controller – The person who (either alone or with others) decides what personal information Little Hiccups will hold and how it will be held or used.

Data Protection Act 2018 (UK GDPR) – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person on the Trustees who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 2018 (UK GDPR)

Data Subject/Service User – The individual whose personal information is being held or processed by Little Hiccups (for example: a service user or a supporter)

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him.

Explicit consent is needed for processing sensitive data this includes the following:

(a) racial or ethnic origin of the data subject
(b) political opinions
(c) religious beliefs or other beliefs of a similar nature
(d) trade union membership
(e) physical or mental health or condition
(f) sexual orientation
(g) criminal record
(h) proceedings for any offence committed or alleged to have been committed

Notification – Notifying the Information Commissioner's Office (ICO) about the data processing activities of Little Hiccups. *Note: Not-for-profit organisations are exempt from notification.*

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018 (UK GDPR).

Processing – means collecting, amending, handling, storing or disclosing personal information

Personal Information – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers of the Group.

APPENDIX 2: Privacy Notice

This privacy notice explains how Little Hiccups looks after personal information you give us or that we learn by having you as a client and the choices you make about marketing communications you agree we may send you. This notice explains how we do this and tells you about your privacy rights and how the law protects you.

Topics:

- What information we collect about you
- How information about you will be used
- Marketing
- Employment
- How long your information will be kept for
- Where your information is kept
- Access to your information and correction
- Cookies
- Other websites
- Changes to our privacy notice
- How to contact us

What Information We Collect About You

We collect information about you when you register with Little Hiccups or sign up to use one of our services whether contact is online, on paper, by email or over the phone.

The information you give us may include your name, address, email address, phone number, relevant history to check your eligibility for Little Hiccups payment and transaction information, IP address and CVs.

Details on Little Hiccups children under the age of 16 are only kept with the consent of a parent, carer or guardian.

How Information About You Will Be Used

In law, we are allowed to use personal information, including sharing it outside Little Hiccups, only if we have a proper reason to do so, for example:

- To fulfil a contract with you ie to provide the service you have requested and to communicate with you about details
- When it is in our legitimate interest ie to apply for a grant, unless this is outweighed by your rights or interests
- When you consent to it: we will always ask for your consent to hold and use health and medical information.

We have rigorous data protection and security policies in place with all our third party software.

We will not share your information with any other third party without your consent except to help prevent fraud, or if required to do so by law.

Marketing

We would like to send you information about Little Hiccups and other relevant information which may be of interest to you. We will ask for your consent to receive marketing information.

If you have consented to receiving marketing, you may opt out at a later date.

You have the right at any time to stop us from contacting you for marketing purposes or giving your information to third party suppliers of products or services. If you no longer wish to be contacted for marketing purposes, please contact Little Hiccups at info@littlehiccups.co.uk.

Employment / Volunteers / Trustees

The information we collect about employees (including contractors), volunteers and Trustees the purposes it is used for and who it will be shared with is set out in our employment contracts and employee handbook.

How Long Your Information Will Be Kept For

Unless you request otherwise, we will keep your information for a maximum of 5 years from your last visit to a Little Hiccups service.

After 5 year we will delete all your personal information, except for financial transactions (which we are obliged to keep for 6 years).

Information about unsuccessful job applicants will be deleted after four months.

See our data retention policy for further information, including employee data.

Where Your Information Is Kept

Your information is stored within the European Economic Area on secure servers provided by 123-reg, Paypal, Yapsody and MailChimp. Any payment transactions are encrypted. Sending information via the internet is not completely secure, although we will do our best to protect your information and prevent unauthorised access.

Access to Your Information and Correction

You have the right to request a copy of the personal information that we hold about you. This will normally be free, unless we consider the request to be unfounded or excessive, in which case we may charge a fee to cover our administration costs.

If you would like a copy of some or all of your personal information, please contact Little Hiccups on info@littlehiccups.co.uk

We want to make sure that your personal information is accurate and up-to-date. You may ask us to correct or remove information you think is inaccurate.

You have the right to ask us to object to our use of your personal information, or to ask us to delete, remove or stop using your personal information if there is no need for us to keep it.

E-Newsletters

We email e-newsletters to inform you about events and services provided by Little Hiccups and other relevant information. You have the opportunity to unsubscribe from e-newsletters at any time.

E-newsletters may contain subscriber tracking facilities within the actual email, for example, whether emails were opened or forwarded, which links were clicked on within the email content, the times, dates and frequency of activity. We use this information to refine future email campaigns and provide you with more relevant content based around your activity.

Cookies

Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. This is used to track visitor use of the website and to compile statistical reports on website activity. For further information visit www.aboutcookies.org or www.allaboutcookies.org

You can set your browser not to accept cookies and the above websites tell you how to remove cookies from your browser. However, in a few cases some of our website features may not function as a result.

The Queen's Award for Voluntary Service

Other Websites

Our website includes links to other websites. This privacy notice only applies to this website so when you link to other websites you should read their own privacy notices.

Changes to Our Privacy Notice

We keep our privacy notice under regular review and we will place any updates on this webpage. This privacy notice was last updated on 9th July 2020.

How To Contact Us

Please contact us if you have any questions about our privacy notice or information we hold about you:

- By email - info@littlehiccups.co.uk

You also have the right to complain to the Information Commissioner's Office. Find out on their website how to report a concern:
www.ico.org.uk/concerns/handling

APPENDIX 3: Information Audit for Little Hiccups

What Personal Data Do We Hold and Where?

Type of personal data held	Where held eg software, paper	What you use the data for	Where you got the data from	Do you have consent?	Who you share it with (if anyone)
PERSONAL DATA:					

Name of adult Name of child DOB of child Contact details (address, phone number, email) Details about the child's additional needs and medication Emergency contact information Details of any allergies	Collected on Registration forms via the website and stored on Wordpress/Go Daddy server. Backup is kept on Google Drive. Mailchimp / Yapsody / Paypal / Wordpress website	To ensure eligibility to Little Hiccups (disability / under 16) Emergency contact for events in case of illness. etc For event organisation. Email out details. Occasionally text. To post out Max Cards / e-commerce goods	Families fill out registration forms. Online forms on Yapsody / Mailchimp /Paypal/website	Yes	No specific details shared. Statistics and percentages may be shared with grants.
EMPLOYEE / CONTRACTOR / VOLUNTEER DATA:					

Contact details (address, phone number, email) Emergency contacts/next of kin Job applications and references Training records Disciplinary records Appraisals / performance reviews DBS Check	Collected on application forms which are then uploaded to Google cloud. Paper copies are then destroyed or returned.	To comply with Safeguarding and Child Protection Guidelines. To ensure that our employees/contractors/volunteers have good feedback and continuing professional development. Contacts for emergencies.	Application form DBS office References	Yes	Trustees (including Child Protection Officer) have access
TRUSTEE DATA:					
Contact details (address, phone number, email) Training records Disciplinary records	Google Cloud Charity Commission / Company House / Co-Operative Bank	Charity Commission / Company House / Co-Operative Banking Requirements	Requested from the Trustees	Yes	Charity Commission / Company House / The Co-Operative Bank

Appraisals / performance reviews DBS Check					
MARKETING DATA:					
Mailing lists (email, text, post) Online booking	Mailchimp (mailing list) Website	Mailing lists Booking on events	Mailchimp: sign up through the website or from registration form Website: Details inputted by user	Yes - Opt in	Not shared
FINANCIAL DATA:					

Events Attendees Max Card Requests E-commerce on website	PayPal Website	Post out Max Cards/ Event Booking E-commerce on website	Users register to Paypal	Yes	Not shared
Suppliers Receipts Invoices Bank account details Credit/debit card details Payment history Fundraisers Sponsor Forms	Held on electronic file and paper hard copy	Accounts evidence	Supplied or created via online banking as evidence /receipt	Yes	Accountant Charity Commission Bank Companies House

Date completed ……..

Appendix 4: Procedure for personal data breaches

This procedure is to be followed if there is a breach of personal data. The person responsible for managing the process is initially the Data Protection Officer. If the DPO is not available then it is the Marketing and Compliance Coordinator.

All decisions on whether or not to notify the Information Commissioner's Office (ICO) or individuals affected will be countersigned by the Chairperson.

This procedure covers:

- What is a personal data breach?
- What must be recorded?
- Assessing the likelihood and severity of the adverse consequences of the breach

- When do breaches have to be reported to the ICO?
- What must be reported to the ICO?
- How to report a breach to the ICO
- Telling individuals affected about a breach
- What are the consequences of failing to notify the ICO?

What is a Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data.

Examples include:

- access by an unauthorised third party
- deliberate or accidental action by a Little Hiccups data controller or a data processor (third party supplier, who must inform you without undue delay as soon as they become aware of it)
- sending personal data to an incorrect recipient
- computer or data storage devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data (ie data is made unavailable and this unavailability has a significant negative effect on individuals)

What must be recorded?

All breaches must be recorded, whether or not they need to be reported to the ICO. If you decide not to report a breach, you must be able to justify this decision and it must therefore be documented.

Record:

- The facts relating to the breach
- Its effects
- Remedial actions taken
- What caused the breach and how a recurrence could be prevented

Assessing the Likelihood and Severity of the Negative Consequences of the Breach

Use the template in Appendix 4A to help answer the following questions

- What is the likelihood and severity of the resulting risk to people's rights and freedoms?
- What are the potential negative consequences to the individuals concerned?
- How serious and substantial are the consequences? Don't forget this can include emotional distress, as well as financial, physical or material damage.

If there is a high risk of negatively affecting individuals' rights and freedoms (scoring 6 or more points on the risk assessment template at Appendix 4A), then it must be reported to the ICO. This includes personal data breaches notified to you by third party data processors.

You may also need to notify third parties such as the police, insurers, banks or credit card companies who could help to reduce the risk of financial loss to individuals.

When Do Breaches Have To Be Reported To The ICO?
Breaches which are likely to result in a high risk of negatively affecting individuals' rights and freedoms must be reported no later than 72 hours after you first become aware of it. If you take longer than this, the reasons for delay must be documented.

What Must Be Reported To The ICO?
A description of the nature of the personal data breach including:

- The categories and approximate number of individuals concerned and the categories and approximate numbers of personal data records concerned (which may be the same number)
- The name and contact details of the person who can provide more information if required
- The likely consequences of the personal data brea
- The measures taken, or proposed to be taken, to deal with the personal data breach including measures taken to mitigate any possible negative effects

The information can be provided in phases if it is not all available within 72 hours, as long as this is still done without undue further delay and you tell the ICO when to expect further information from you.

You must prioritise the investigation, give it adequate resources and deal with it urgently.

How To Report A Breach To The ICO

The section of the ICO website on reporting breaches has not yet been updated for GDPR. However, the following contact details are provided:

Data breaches : Call 0303 123 1113
Open Monday to Friday between 9am and 5pm, closed after 1pm on Wednesdays for staff training.

Telling Individuals Affected About A Breach

If the breach is likely to result in a high risk to the rights and freedoms of individuals (scoring 6 or more on the more points on the risk assessment template at Appendix 4B), you must inform the individuals affected as soon as possible.

One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

You need to tell individuals:

- The nature of the personal data breach
- The name and contact details of the person who can provide them with more information
- The measures taken or proposed to be taken to deal with the personal data breach and the measures taken to mitigate any possible adverse effects

If you decide not to notify individuals, you still need to notify the ICO unless you can show that the breach is unlikely to result in risks to rights and freedoms. The ICO has the power to make you inform individuals if they consider there is a high risk. The decision-making process must be documented.

What Are The Consequences Of Failing To Notify The ICO?

A fine of up to 10 million euros or 2% of your turnover or a fine of up to 20 million euros or 4% of your turnover in the most severe cases.

Appendix 4A – risk assessment template for personal data breaches

COMPLETING THE RISK ASSESSMENT TEMPLATE

Step 1
Provide brief details of the personal data breach, when it happened, how it happened and who has been affected.

Step 2
List all the possible adverse consequences of the data which has been lost, altered or access by an unauthorised person.

Step 3
How likely are those adverse consequences to occur?

Low likelihood	- 1 point
Medium likelihood	- 2 points
High likelihood	- 3 points

Step 4
How serious would those adverse consequences be if they did occur?

Low likelihood	- 1 point
Medium likelihood	- 2 points
High likelihood	- 3 points

Step 5
Produce an overall score by multiplying the points in columns 2 and 3 eg if a negative consequence is unlikely (1 point) but if it happened the impact would be high (3 points), the overall score will be 3.

Anything scoring 6 points or more must be reported to the ICO and to the individuals concerned.

What happened? When did it happen? How did it happen? Who has been affected?

List all the possible consequences of the data being lost, altered or accessed by an unauthorised person	**How likely is it there will be negative consequences? 1, 2, 3 points**	**How severe would negative consequences be? 1, 2, 3 points**	**Combined**
1.			

2.			
3.			
4.			
5.			

Continue on another sheet if necessary

Form Completed by : .....

Date: : .....

The Queen's Award for Voluntary Service

Little Hiccups, The Barrowbys, Barrowby Lane, Garforth, Leeds LS25 1NG
07831 230741 **info@littlehiccups.co.uk** **www.littlehiccups.co.uk**
Registered Charity No: 1170147 Company Limited by Guarantee No: 9692276

Appendix 5: Top five tips

Here are our top five of data protection tips for small and medium sized charities and third sector organisations:

1. **Tell people what you are doing with their data**
   People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.

2. **Make sure your staff are adequately trained**
   New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.

3. **Use strong passwords**
   There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves.

4. **Encrypt all portable devices**
   Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted

5. **Only keep people's information for as long as necessary**
   Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

Amendments

Date	Amendment Made	By whom
15/09/2023	3 year review - updated storage locations. Moved from Yapsody to website and away from paper versions	MWP
23/07/2025	Data Protection 1998 updated to Data Protection 2018 New section added: Befriending and Personal Contact Outside of Little Hiccups	MWP