GDPR Policy

We at HEY Kids have built our success on striving for excellence in all our activities.

The charity has and will sustain an effective data management system that will satisfy the General Data Protection Regulation (known as the "GDPR") that comes into effect on 25 May 2018.

The charity recognises that sustained commitment by decision makers and key people in our organisation will ensure commitment to protecting privacy. As part of that commitment provision will be made to train our trustees who need access to personal information to perform their duties, have a good understanding of their duties and responsibilities for security (including cyber security) and only holding data under a lawful basis.

We understand that no other person or corporation own the rights to an individual's personal information. Any information we collect is used for our own processing purposes and meets a lawful basis. The information is only shared when required to meet a lawful basis, further details of when data is shared are shown in our process document. Our data audit details the data we hold and why we hold it.

For any information relating to our GDPR policy please contact the data protection lead for HEY Kids Caroline Wilson, email contact@HEYKids.org.uk

Individuals have the right to check any information that is held about them, to do this you should contact the data protection lead. If you find any inaccuracies in the information we hold about you, we will update our records and delete incorrect information.

The issues addressed by the policy and resultant required working practices will be fully communicated to all our trustees who use data to carry out their duties and anyone else it affects.

The GDPR Policy will be reviewed at intervals to ensure that is remains valid and reflects the charity's activities.

…….. Date 11 May 2018

Helen Crawforth
Chair of Trustees
HEY Kids

Scope of the GDPR Policy

1. The address for registration of the charity at:
   Hey Kids Type 1 Diabetes Children And Family Support Group
   % Mrs Helen Crawforth
   2 St Peters Walk
   Wawne
   East Yorshire
   HU7 5FB

2. Home or work address of Trustees who carry out administration duties for the charity.

3. Work carried out whilst at charity events, meetings and activities.

Aims

1. Ensure compliance with all relevant legislation, with training, communication and documentation.

2. Keep an accurate record of Data held and the lawful basis for holding the information.

3. Document how personal data flows through our charity or if it is sent to other organisations, the lawful basis for sharing the information.

4. Document what the charity will do in the event of a data breach.

5. Document a privacy policy that is an easy to understand summary of our GDPR policy.

RESPONSIBILITIES

1. **Data Protection Lead**

The Data Protection Lead is responsible for:

1. Implementing the GDPR Policy.
2. Reporting data breach to ICO.
3. Ensuring that adequate and appropriate organisation and resources are available for the effective implementation of the policy.
4. The provision of appropriate advice and assistance.
5. Monitoring that the security practices are actively and effectively been used, implementing refresher training if trustees fail to comply with security practices.
6. Ensuring all trustees have a full understanding of the Charity and legal requirements.
7. The provision of appropriate GDPR information, instruction and training.
8. The detailed implementation of the policy.
9. Identifying needs and allocating the necessary resources.
10. Ensuring appropriate and informed supervision.
11. Ensuring the provision of appropriate GDPR advice and assistance.
12. Implementation of effective data protection practices.
13. Ensuring all appropriate personnel are aware and conform to the Charity and Legal requirements, using a documented monitoring system.
14. Developing all appropriate documentation required for use to implement the GDPR.
15. Liaising with all levels of internal personnel and any appropriate external body to ensure that any subsequent procedure document can be used effectively.
16. Ensuring compatibility with existing recording systems.
17. Continuously review and improve systems following guidance and ensure proportionate and reasonable steps are taken to ensure security (including cyber security).

RESPONSIBILITIES

2. **Chair and Vice Chair of Trustees**

Are responsible for:

1. Contributing and fully supporting the GDPR Policy.
2. Implementing and monitoring the charity's GDPR arrangements.
3. Reporting data breach to Data Protection Lead [or in the case of absence report directly to the ICO].
4. Ensuring they and all trustees are aware and conform to the Charity and legal requirements and has suitable and sufficient experience, information, instruction and training.
5. Leading by good example.
6. Continuously monitoring performance of other trustees.
7. Actively seeking co-operation from trustees and members in maintaining and improving Data Management Systems.

RESPONSIBILITIES

3. **Trustees**

Are responsible for:

1. Fully co-operating with the charity in fulfilling its legal obligations and implementing the GDPR Policy and procedures.

2. Implementing the charity's GDPR arrangements.

3. Not misusing or interfering with anything provided by the charity in the interest of data control and security.

4. Reporting data breach to the data protection lead, chair of trustees and vice chair.

5. Reporting incorrect data to data protection lead.

6. Reporting any shortcomings in the Charity's arrangements, to the data protection lead.

RESPONSIBILITIES

4. **All Members**

Are responsible for:

1. Fully co-operating with the charity in fulfilling its legal obligations and implementing the GDPR Policy and procedures.

2. Not misusing or interfering with anything provided by the charity in the interest of data control and security.

3. Reporting data breach to trustees.

4. Reporting incorrect data to trustees.

5. Reporting any shortcomings in the Charity's arrangements, to the trustees.

ARRANGEMENTS

DATA AUDIT (Overview of the data held by the charity)

1. Suppliers:

    - Information is kept after being provided by the supplier in order to fulfil the requirements of the contract, or in the case of a new supplier in order for them to provide us a quotation.

    - Records will be kept for seven years, so that we can provide information for legal reasons for the reporting of the charities accounts for the previous six years and the information may be shared with our accountants who check our records are sufficient and correct to meet legal requirements.

    - Disclosure requests should be addressed to the data protection lead.

2. Supporters:

    - The Name, Address and reason for donation will be kept of supporters of the charity.

    - Records will be kept for seven years, so that we can provide information for legal reasons for the reporting of the charities accounts for the previous six years and the information may be shared with our accountants who check our records are sufficient and correct to meet legal requirements.

    - Disclosure requests should be addressed to the data protection lead.

3. Trustees:

    - Information is kept after being provided by an trustee in order to fulfil the requirements of records required to be kept by the charity commision and the bank, or in the case of a new trustee in order to evaluate if you are suitable for a trustee role.

    - Our accountants keep Trustee records as they update our details with the Charity commision as is legally required.

    - Upon application to become a trustee we will ask you for your name, contact details and proof of identity, the proof of identity will be stored by the accountants. A DBS check will be carried out to ensure safeguarding as the charity supports children. You will be asked to complete a trustee information form for the bank the charity uses, so that the bank can comply with it’s legal requirements, this information will be stored by the bank as is required by their regulations requirements.

- As the charity is specifically set-up to support children and their families we do not intend to destroy trustee records, so that they can remain accessible for reference if there was to be a claim relating to a historic offence, so that we can trace the individuals involved. A trustee record will be kept as a dormant record once a trustee resigns.

- Disclosure requests should be addressed to the data protection lead.

4. Members:

    - Information is kept after being provided by an adult with parental responsibility in order to fulfil the requirements of safeguarding for us to keep a record of who is involved with the charity and so that we have contact details and medical details to ensure safety in an emergency.

    - We will ask you for your name, contact details, the names of family members, children's dates of birth and medical treatment details.

    - We will only share your information if legally required to do so or with the Charity's trustees to ensure safety at events.

    - Your contact information may be used so that we can inform you of vital information, but most information is provided via our website and facebook group to ensure speedy communication.

    - Whilst you are using the services we will ask for your consent to take and use photographs on our web-site and facebook group. You do not need to given consent to photographs to participate in the charity's activities and you can withdraw consent at any time.

    - As the charity is specifically set-up to support children and their families we do not intend to destroy member records, so that they can remain accessible for reference if there was to be a claim relating to a historic offence, so that we can trace the individuals involved. A member record will be kept as a dormant record once the child with Type 1 diabetes reaches 26 years old.

    - Disclosure requests should be addressed to the data protection lead.

PROCESS DOCUMENT

STORAGE ARRANGEMENTS

1. Locked cabinets for currently used documents containing personal information, archive personal files and accounts information.

SECURITY ARRANGEMENTS

1. Storage to be kept locked and access limited to trustees.

2. Keeping documents locked away when not attended ('clear desk system' treat documents showing personal data the same as cash).

3. Always use a shredder to dispose of confidential waste.

CYBER SECURITY ARRANGEMENTS

1. Password protect all phones, laptops, tablets, computers and any other device containing personal information. Only use genuine devices and install the developers updates, do not use 'jailbroken' devices as these will not have security protection. Keep passwords secure.

2. Keep member records on a google cloud drive accessible by three trustees so that in an emergency records are easily accessible. Passwords changed regularly and if who has access changes. Back up of data to be stored in a locked cabinet.

3. Cyber security, general IT, legal seminars and courses for Data Protection Lead

4. Cyber security online course for all trustees needing to improve their skills, implement the good working practices to reduce risk of attack, be particularly cautious with emails and internet use.

5. Log out of the google drive when not in use and do not allow shared computers to store the password.

6. Lock computers when leaving them unattended or to protect privacy if other people can see the screen (windows + L)

7. Store phones, laptops, tablets or any other portable devices securely when unattended. Don't print documents unnecessarily.

8. Ensure privacy of personal email addresses by using 'bcc' when sending to multiple recipients.

9. Facebook group is a closed group, four trustees have admin rights.

SHARING ARRANGEMENTS

1. 360 Chartered Accountants are the appointed accountants for the charity, they keep trustee records for the charity and may need to review accounts records to ensure compliance with legal requirements.

2. Barclays Bank are the charity's bankers and need to keep records relating to transactions and trustees to meet legal requirements.

3. We can be asked for information relating to investigations. Requests should be made to the Data Protection Lead or a Trustee and they must check the legal basis for sharing the information.

4. If the trustees have a safeguarding concern reported to them, once they are satisfied that the report is genuine they may share information with the relevant authority to investigate.

ARRANGEMENTS

PRIVACY POLICY

We at HEY Kids have built our success on striving for excellence in all our activities.

The charity has and will sustain an effective data management system that will satisfy the General Data Protection Regulation (known as the "GDPR") that comes into effect on 25 May 2018.

We understand that no other person or corporation own the rights to an individual's personal information. Any information we collect is used for our own processing purposes and meets a lawful basis. The information is only shared when required to meet a lawful basis, further details of when data is shared are shown in our process document. Our data audit details the data we hold and why we hold it.

For any information relating to our GDPR policy please contact the data protection lead for HEY Kids Caroline Wilson, email contact@HEYKids.org.uk

Individuals have the right to check any information that is held about them, to do this you should contact the data protection lead. If you find any inaccuracies in the information we hold about you, we will update our records and delete incorrect information.

…….. Date 11 May 2018
Helen Crawforth
Chair of Trustees
HEY Kids

ARRANGEMENTS

BREACH POLICY

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation or if the data is made unavailable, for example, when is has been encrypted by ransomware, or accidentally lost or destroyed.

We have a duty to report certain types of personal data breaches to the ICO, within 72 hours of becoming aware of a breach, where feasible, if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.

If a personal data breach has occurred, we first must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then the Data Protection Lead should contact the ICO to report a breach using the online 'report a breach portal' https://ico.org.uk/for-organisations/report-a-breach/ (If the Data Protection Lead is absent another Trustee will report the breach).

Reportable personal breaches can include (but are not limited to):

- access by an unauthorised third party
- deliberate or accidental action or in-action by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

If the breach does not pose a risk to people's rights and freedoms, action may still need to be taken. Below is an example of a breach, that requires action with the individual, Probably, mostly things you would do as a matter of courtesy. This should all be recorded, but the incident would not need to be reported to the ICO:

If you send an email to an intended recipient, you should not include personal email addresses, as opposed to business email addresses, in the to or cc section if others are also receiving the email. Given they are visable to all this would be deemed a data breach. Against the above test, the appropriate action would probably be to inform the person whose data has been breached, ask the recipients to delete or ignore the email address and issue an apology.