Data Protection Policy

Date	**24th January 2018**
Reviewed	**6th June 2018**
Date of next review	**5th June 2019**

Data Protection Policy

Introduction

Autism Bedfordshire holds personal data about our employees, service users, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. *Business purposes include the following:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* - *Ensuring business policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* - *Monitoring staff conduct, disciplinary matters* - *Marketing our business* - *Improving services*
Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.
Sensitive personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

As our Data Protection Officer, Sharon Sturge, has overall responsibility for the day-to-day implementation of this policy.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Data Protection Officer's responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by Autism Bedfordshire
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Approving data protection statements attached to emails and other marketing copy

- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the team to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Responsibilities of the IT Management Company

Our IT systems, services and software and equipment are managed by, Techies Computer Consultants, 7 St Johns Street, Bedford, Bedfordshire, MK42 0AH.

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly

- Researching third-party services, such as cloud services the company is considering using to store or process data

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that customers have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Data Protection Officer, Sharon Sturge.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Data Protection Officer will establish what, if any,

additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The Data Protection Officer must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Data Protection Officer.

Subject access requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the Data Protection Officer. We may ask you to help us comply with those requests.

Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Data Protection Officer about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the Data Protection Officer for advice on direct marketing before starting any new direct marketing activity.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

Data Breach Policy

Autism Bedfordshire holds and processes a large amount of personal data, which needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

This policy relates to all personal and sensitive data held by Autism Bedfordshire regardless of format.

This policy applies to all staff including temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of, Autism Bedfordshire.

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to Autism Bedfordshire's information assets and/or reputation.

An incident includes but is not restricted to, the following:

- Loss or theft of confidential or sentitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
- Equipment theft or failure (reported through regular equipment audits)
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack
- Unforseen circumstances such as a fire or flood
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

Any individual who accesses, uses or manages Autism Bedfordshire's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer and IT Management Company (Techies Computer Consultants, 7 St Johns Street, Bedford, Bedfordshire, MK42 0AH).

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The Data Protection Officer and senior staff have consented to be contacted out of hours to be notified of a breach.

The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. All staff should be aware that any breach of the Data Protection Act may result in Autism Bedfordshire's Disciplinary Procedures being instigated.

The Data Protection Officer will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach. An initial assessment will be made by the Data Protection Officer in liaison with relevant staff to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach in some cases it could be the Data Protection Officer).

The investigating officer will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause. They will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

The investigating officer, in liaison with the relevant members of staff will determine the suitable course of action to be taken to ensure a resolution to the incident.

An investigation will be undertaken immediately and wherever possible within 24 hours of the breach being discovered / reported. The investigating officer will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- the type of data involved
- its sensitivity
- the protections are in place (e.g. encryptions)
- what's happened to the data, has it been lost or stolen
- whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach

The investigating officer and / or the Data Protection Officer, in consultation with Techies, will determine who needs to be notified of the breach. Every incident will be assessed on a case by case basis. However, the following will need to be considered:

- Whether there are any legal/contractual notification requirements;
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- Would notification help Autism Bedfordshire to meet its obligations under the seventh data protection principle;
- If a breach is likely to result in a risk to the rights and freedoms of individuals then the breach must be reported to the relevant supervisory authority within 72 hours. In the UK this is the Information Commissioner's Office. If a breach is likely to result in a high risk (e.g. criminal activity such as fraud, or published in the public domain) to the rights and freedoms of individuals then those concerned must be notified without undue delay. Failure to notify a breach when there is a requirement to do so can result in a fine. You can report a breach at https://ico.org.uk/for-organisations/report-a-breach/

The GDPR requires all organisations to report certain types of data breach to the ICO and individuals in some cases. The ICO must be notified of a breach if it is likely to result in a risk to the rights and freedoms of individuals, i.e. a significant economic or social disadvantage; in most cases you will also need to inform the individual. As well as reporting to the ICO, it should be assessed what personal beneficiary data held would contravene the privacy risks to the individual and require the individual to be informed, as well as articulating what would be defined as "undue delay". As you may hold sensitive information about a beneficiary, for example, medical, criminal or other such information, it is very important to put in place clear procedures for contacting beneficiaries. In general, unless the data has been subject to pseudonymisation, it may be a prudent view to take the perspective that all personal data would constitute a risk to the privacy rights of the individual.

The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work. The ICO will only be notified if personal data is involved.

Notification to the individuals whose personal data has been affected by the incident will include a description of the breach, the data involved and when it occurred. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact Autism Bedfordshire for further information or to ask questions on what has occurred.

The LIO and or the Data Protection Officer must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The LIO and or the Data Protection Officer will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

All actions will be recorded by the Data Protection Officer.

Once the initial incident is contained, the Data Protection Officer will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review will consider:

- Where and how personal data is held and where and how it is stored

- Where the biggest risks lie, and will identify any further potential weak points within its existing measures

- Whether methods of transmission are secure; sharing minimum amount of data necessary

• Identifying weak points within existing security measures

• Staff awareness

• Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by the Board of Trustees.

Along with reporting a data breach to the ICO, Autism Bedfordshire will also need to consider whether the data breach is a serious incident, and if so whether to report to the Charity Commission. The Commission lists the below as a data breach that should be reported:

• Charity's data has been accessed by an unknown person; this data was accessed and deleted, including the charity's email account, donor names and addresses;

• A charity laptop, containing personal details of beneficiaries or staff, has been stolen or gone missing and it's been reported to the police;

• Charity funds lost due to an online or telephone 'phishing scam', where trustees were conned into giving out bank account details;

• A Data Protection Act breach has occurred and been reported to the ICO.

GDPR provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?

Information given by service users

In order to provide our services we need to collect and use personal information regarding the following:

Opt in marketing communications (electronic newsletters, campaign sign ups)

Supporters including donors, fundraisers, digital supporters, shop customers.

We will obtain personal information through enquiries about our activities and services, registrations for events, emails, registrations for our newsletters and updates, purchases from our online shop, donations, applications for job vacancies, questions regarding our organisation or people providing personal information for other purposes.

Below are examples of personal data held by us:

Newsletter mailing lists and marketing updates o Fundraising or supporter data

Event administration or shop purchases

Information we may gather from our website

We will gather general information on how users interact with our website such as the number of pages visited. This information is collected to help measure how users interact with our website and content. This is done by using tracking software from our third party supplier Google Analytics. For further information on Google Analytics visit Google's information page. To opt out of google analytics visit: https://tools.google.com/dlpage/gaoptout

How we use information

Supporter Information

We will collect information from donors, purchases from our shop, new members and fundraisers.

The information collected will usually be one or more than one of the following:

- Name
- Contact details
- Bank or Credit Card details
- email address

We require this information for the following reasons:

- to provide the relevant information or service that has been requested.
- to administer donations or sales, including processing gift aid.
- to thank those who have made donations or supported Autism Bedfordshire.

Electronic communications

We will collect information from those who sign up to receive further communications from us electronically including general updates, service updates including family events, careers or fundraising.

The legal basis for us to process this information is that consent has been given. We use a third party provider, MailChimp, to deliver our e-newsletter, we store contact information in our MailChimp account, we will use our MailChimp account to send marketing updates and gather statistics around email opening and clicks to help us monitor and improve our e-newsletter.

For further information please see Mail Chimp's privacy policy.

The information collected will be the following:

- Name
- Address
- Interest
- Email address

We will only use this information for the purposes selected when opting in to receive electronic communication via MailChimp. Recipients can change their mind at any time by clicking the unsubscribe link in the footer of the email, or by contacting us at enquiries@autismbeds.org

Social media

Private or direct messages sent via social media will be stored on our social media account for three months. It will not be shared with any other organisations.

Who do we share information with?

We will never sell or rent information to another party or organisation. Information provided as part of a Gift Aid declaration may be disclosed to HMRC as part of the declaration to reclaim Gift Aid. We may share or disclose your personal information if we are required to do so by any law or court order.

How we use cookies on our website

Cookies are small text files that are automatically placed onto devices by some websites. They are widely used to improve the performance of a website, for saving different options and to provide website owners with information on how the site is being used. We do not use our own cookies but there will be a number of third party cookies from our trusted suppliers used on our websites. Each company is responsible for the cookies that they place onto your device and have separate policy documents to highlight their use. Our list of trusted third parties who may deploy cookies is below with a link to their cookie details:

Third Party	Policy Location
YouTube	https://www.google.com/policies/technologies/types/
MailChimp	https://mailchimp.com/legal/privacy/
Google	https://www.google.com/policies/technologies/types/
Google Analytics	https://www.google.com/policies/technologies/types/
Facebook	https://www.facebook.com/policies/cookies/
Twitter	https://support.twitter.com/articles/20170514
Linked In	https://www.linkedin.com/legal/cookie-policy
Shopify	https://www.paypal.com/uk/webapps/mpp/ua/cookie-full
Just Giving	https://www.justgiving.com/info/cookies
Paypal	https://www.paypal.com/uk/webapps/mpp/ua/cookie-full

The right to see information held by Autism Bedfordshire

Under the new EU General Data Protection Regulation (GDPR) individuals have the right to confirmation that their data is being processed and the right to access to their personal data. For further information visit: https://ico.org.uk/for-the-public/

They have the right to request:

- Access to the personal data we hold (free of charge in most cases).
- The correction of personal data when incorrect, out of date or incomplete.
- That we stop using personal data for direct marketing (either through specific channels, or all channels).
- That we stop any consent-based processing of personal data after withdrawal of that consent.

Requests to see personal information held by us should be sent to: Autism Bedfordshire, Suite B1, 1 Hammond Road, Elms Farm Industrial Estate, Bedford, Bedfordshire, MK41 0UD.

How long we keep information?

Whenever we collect or process personal data, we will only keep it for as long as is necessary for the purpose for which it was collected.

At the end of that retention period, data will either be deleted completely or anonymised, for example by aggregation with other data so that it can be used in a non-identifiable way for statistical analysis and planning.

Request to delete information?

Under the new EU General Data Protection Regulation (GDPR) that will be coming into effect across all member states from the 25th May 2018, individuals will have the right to request deletion of personal information if the following applies:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- Where consent is withdrawn.
- Where the subject objects to the processing and there is no overriding legitimate interest for continuing the processing.
- Where personal data has been unlawfully processed (i.e. otherwise in breach of the GDPR).
- Where personal data has to be erased in order to comply with a legal obligation.
- Where personal data is processed in relation to the offer of information society services to a child.

How we protect personal data

We know how much data security matters and will treat data with the utmost care and take all appropriate steps to protect it. We secure access to all transactional areas of our websites and apps using 'https' technology. Access to personal data is password-protected, and sensitive data (such as payment card information) is secured by SSL encryption.

We regularly monitor our system for possible vulnerabilities and attacks, and we carry out penetration testing to identify ways to further strengthen security.

Contacting the Regulator

If an individual feels that their data has not been handled correctly, or if they are unhappy with our response to any requests they have made to us regarding the use of their personal data, they have the right to lodge a complaint with the Information Commissioner's Office.

You can contact the Information Commissioner's Office on 0303 123 1113.

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Data Protection Officer will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA without first discussing it with the Data Protection Officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Monitoring

Everyone must observe this policy. The Data Protection Officer has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Officer.