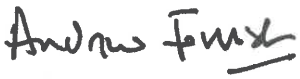
Data Protection Policy

PRIORY
GREAT YARMOUTH COMMUNITY TRUST

Date policy approved by Trustees	**17 May 2018**
This Data Protection Policy replaces all previous Data Protection Policies and references to the Data Protection Policies in other policies and documents from the implementation date set out below.	
Date policy to be implemented	**22 May 2018**
Manager/s responsible for policy review	Director of Business Support
Date of next review This policy is subject to annual review	May 2019
	
John Holmes – Chair of Board	**Andrew Forrest – Executive Director**

1. Introduction

1.1. As part of its day to day operations Great Yarmouth Community Trust (GYCT) needs to gather and uses information about individuals who: access its services; and work or volunteer for it.

1.2. This policy describes how this personal data must be collected, handled and stored to meet the company data protection standards and to comply with the law.

1.3. This Data Protection Policy ensures GYCT –

- Complies with data protection law and follow good practice
- Protects the rights of staff, service users and partners
- Is transparent about how it stores and processes individual data
- Protects itself from the risk of a data breach

1.4. This policy should be read in conjunction with the Managing Data Breaches Policy

2. Data Protection Law

2.1. This Policy complies with the Data Protection Act 1998 updated by the General Data Protection Regulation (GDPR) 2018. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

2.2. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

2.3. The new legislation is underpinned by the following 8 important principles - that in every case data should:

(1) Be processed fairly and lawfully
(2) Be obtained only for specific, lawful purposes
(3) Be adequate, relevant and not excessive
(4) Be accurate and up to date
(5) Not be held for any longer than necessary
(6) Be processed in accordance with the right of data subjects
(7) Be protected in appropriate ways
(8) Not be transferred outside Europe unless that country ensures adequate levels of protection

3. Scope of the policy

3.1. This policy applies to:

- All staff and volunteers of GYCT
- All contractors, suppliers and other people working on behalf of GYCT
- All data that GYCT holds relating to identifiable individuals, even if that information technically falls outside of GDPR 2018.

3.2. This data can include –

- Names of individuals
- Postal addresses
- Email addresses
- Phone numbers

Plus any other information relating to individuals

4. Data Protection risks

4.1. This policy protects individuals and GYCT from data security risks, including:

- breaches of confidentiality, i.e., information given out inappropriately
- failing to offer a choice, eg., all individuals should be free to choose how the company uses data relating to them
- reputational damage, eg., GYCT could suffer if hackers successfully gained access to sensitive data

5. Consent

5.1. In order to comply with GDPR 2018 Great Yarmouth Community Trust must know why each data set is collected, processed and stored and identify the lawful basis under which the data is being held.

5.2. Data may only be collected, processed and stored under one or more of the following lawful basis: consent, contract, legal obligation, vital interest, public interest or legitimate interest

5.3. GYCT understands that it must define the lawful basis under which we collect each data set before it begins to collect that data.

5.4. Each year GYCT will produce a schedule of data sets collected and the lawful purpose under which they are held which will be published on the Trust's website.

6. Providing information: Privacy Notices

6.1. GYCT aims to ensure that individuals are aware that their data is being processed, and that they understand how the data is being used and how to exercise their rights

6.2. To these ends, GYCT has a Privacy statement, setting out how data relating to individuals is used by the company. This is available upon request and will also be available on GYCT website – www.priorycentre.co.uk

7. Responsibilities

7.1. Everyone who works for, or with, GYCT has some responsibility for ensuring data is collected, stored and handled appropriately. However, the following people have key areas of responsibility:

7.2. **Board of Trustees** supported by the Executive Director are ultimately accountable for ensuring GYCT meets its obligations.

7.3. The Executive Director shall ensure that a **Data Controller** is appointed to act for the Trust who will be responsible for:

7.3.1. overseeing the implementation of the Data Protection Policy;
7.3.2. arranging data protection training for staff, including as part of first day induction;
7.3.3. checking and approving any contracts or agreements with third parties that may handle the company sensitive data;
7.3.4. approving any data protection statements attached to communications such as emails and letters;
7.3.5. ensuring that the annual schedule of data sets being held by the Trust (3.2 above) is prepared and published.

7.4. **Data Protection Officer,** who will report to the Data Controller and is responsible for:

7.4.1. keeping the staff updated about data protection responsibilities, risks and issues;
7.4.2. reviewing all data protection procedures and related policies, in line with an agreed schedule and under supervision of Data Controller;
7.4.3. cascading updates or changes to Data Protection Regulations as soon as possible to allow individuals and teams prepare for any changes in procedures;
7.4.4. handling data protection questions from staff and anyone else covered by this policy;
7.4.5. dealing with requests from individuals to see the data GYCT holds about them (subject access).

7.5. **IT Support Services,** who are responsible for:

7.5.1. Ensuring all systems, services and equipment used for storing data meet acceptable security standards
7.5.2. Performing regular checks and scans to ensure security hardware and software is functioning properly
7.5.3. Ensuring GDPR compliance for any new company providing a service or software suggested or procured

7.6. **GYCT Communication Officer**, who is responsible for:

7.6.1. Receiving and passing on the Data Controller any data protection queries from journalists or other media outlets
7.6.2. When necessary, working with other staff to ensure marketing initiatives abide by data protection principles

8. Staff Access to Data

8.1. The only people able to access data covered by this policy will be those who need it for their day to day work.
8.2. Data may not be shared informally.
8.3. If in the course of their work staff require access to additional data to which they do not normally have access, this must be requested from their line manager. The line manager must agree to this additional access and report this change to the Data Protection Officer.

9. Maintaining the security and confidentiality of data held by GYCT

9.1. Data Storage

9.1.1. All employees have a responsibility for ensuring that data is stored securely. Questions about storing data safely should be directed their line manager or the Data Controller.

9.1.2. When **data is stored on paper** (including data that is normally held electronically but has been printed out for some reason) employees must ensure that:

9.1.2.1. It is kept in a locked drawer or filing cabinet, where unauthorised people cannot see or access it;

9.1.2.2. The key should be accessible only to those members of staff who need to access their data for their work;

9.1.2.3. Printouts are not left where unauthorised people could see them, like on a printer or on desks;

9.1.2.4. It is shredded and disposed of securely when no longer required;

9.1.2.5. Where data has to be shared with another agency or organisation this should be done by hand delivery.

9.1.3. When **data is stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. In order to achieve this:

9.1.3.1. Data should be protected by strong passwords (eg., a mixture of letters, numbers and symbols) that are changed regularly and never shared between employees;

9.1.3.2. Data should only be stored on designated drives and in folders with restricted access on the company server, which are securely backed up on a daily basis and protected by an approved security software and robust firewall;

9.1.3.3. When working with electronic data, employees should ensure the screens of their computers are always locked when left unattended;

9.1.3.4. Data should never be saved directly on laptops or other mobile devices like tablets or smart phones;

9.1.3.5. If data has to be moved to another site it should temporarily be stored on removable media (like hard drives, memory sticks etc) which should be kept securely when not being used;

9.1.3.6. If data has to be transferred to another agency or organisation this should only take place via encrypted email.

9.2. Data accuracy

9.2.1. The law requires GYCT to take reasonable steps to ensure data is kept accurate and up to date.

9.2.2. The more important it is that the personal data is accurate, the greater the effort GYCT will put into ensuring its accuracy. This will include information required by legal and statutory bodies, such as – the Department of Education, Ofsted and local authorities including the LADO, (Local Authority Designated Officer).

9.2.3. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible:

9.2.3.1. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets. Any new data sets that are created should be reported to the Data Protection Officer.

9.2.3.2. Staff should take every opportunities to ensure date is updated. For instance, by confirming a customer details when they call.

9.2.3.3. Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored phone number, it should be removed from the database.

9.3. **The unauthorised disclosure of data covered by this policy, or failure to apply the policy regarding the security and confidentiality of data, is a serious matter and may lead an employee to be subject to disciplinary action.**

10. Retention of records (see Appendix)

10.1. GYCT will retain personal data as part of its records where legal or contractual reasons require it to do so.
10.2. The Trust will publish record retention guidance as an appendix to this policy record.
10.3. The Trust will make such arrangements as necessary to store archived records in a place with high security and minimal access.
10.4. Once the length of time for which the Trust is required to retain records has passed, the records in whatever form will be disposed of securely.

11. Subject access requests

11.1. All individuals who are the subject of personal data held by GYCT are entitled to:
- **Ask what information the company holds about them and why**
- **Ask how to gain access to it**
- **Be informed how to keep it up to date**
- **Be informed how the company is meeting its data protection obligations**

11.2. If any individual contacts the company requesting this information, this is called a Subject Access Request.
11.3. Any requests from individuals to see or obtain their personal data, should be made in writing addressed to the Data Protection Officer, The Old Vicarage, 24 Church Plain, Great Yarmouth, NR30 1NE or by email data-protection@gyctrust.co.uk , who will supply them with a standard request form, although individuals do not have to use this.
11.4. If the amount of data requested is excessive (in excess of 20 printed pages), GYCT reserves the right to charge a fee of £10.
11.5. The Data Protection Officer will aim to provide the relevant data within 14 days.
11.6. They will always verify the identity of anyone making a Subject Access Request, using photo identity or a reference from a Professional person, before handing over any information.

12. Disclosing data for other reasons

12.1. In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Examples could be – safeguarding, suspected criminal activity, health concerns.
12.2. Under these circumstances, GYCT will disclose requested data. However, the Data Controller will ensure the request is legitimate, seeking assistance from the Executive Director and GYCT legal advisors where necessary.

13. Freedom of Information Requests

13.1. As a charity GYCT is not required by law to comply with the Freedom of Information Act 2000, however in line with best practice GYCT will respond openly and promptly to reasonable requests for the information we hold. However, the Personal data covered by this policy may never be disclosed unless it is required in categories covered by section 12 (above).

Appendix	Record keeping guidance
Employment/personnel records	**Length of time**
Accident reports	Indefinite
Staff personnel records	8 years after employment ceases For employees working with children and vulnerable adults 15years
Expense records/cash book/record of payments	8 years
Health declaration/questionnaires	30 years after employment ceases
Committee minutes	Lifetime of charity
Health and safety	**Length of time**
Risk assessments	5 years
PAT testing	6 years
Fire drills	5 years
Asbestos registers	Keep on premises for 3 years then move to property file for 40 yrs.
Legionella checks	6 years
Environmental health checks	6 years
Financial records	**Length of time**
Invoice — revenue	8 years
Invoice —capital	10 years
Petty cash records	8 years
Purchase ledger	8 years
Bank paying in book	8 years
Bank statements	8 years
Receipts cash book	8 years
Sales ledger	8 years
Remittance advice	8 years
Pay records	8 years
Service delivery/operational records	**Length of time**
Registration forms	5 years
Registers of attendance	3 years after the child leaves
Accident book/forms	To be held with the insurance certificate for an indefinite period
Medication records	To be held with the insurance certificate for an indefinite period
Records of individual nursery children	Reasonable period e.g. 3yrs after the child had left the provision (EYFS statutory framework 3.70)
Child/family case files including safeguarding concerns	25 years
Insurance certificates /insurance policies	Indefinitely
Complaint records	At least 3 yrs from resolution date of complaint
Children's learning and development records	To be given to the parents (Nursery)

Child protection records (nursery)	To follow the child to the next setting
Children centre records NCC	PLEASE REFER: to children's centre record retention schedule.
Priory centre/ learning/research/marketing	Length of time
Client activity records	3 yrs from the finish date of the project
Learner records	5 years
Research documents	7 years
Who keeps the records/documentation if the trust cease trading: Named person – a representative of the Trustees to be identified during winding up	