Information and Data Protection Policy

Introduction

1. Grimsby and Cleethorpes Area Doorstep (Doorstep), needs to keep certain information about its employees, trustees, volunteers, members, clients and other members of the public to enable it to monitor performance and achievements. It is also necessary to process information so that staff can be recruited and paid, activities organised and legal obligations to funding bodies and government fulfilled.

2. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Organisation must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the Act) and General Data Protection Regulation 2018. In summary these state that personal and sensitive data must be:

    i. obtained and processed fairly and lawfully;
    ii. obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose;
    iii. adequate, relevant and not excessive for that purpose;
    iv. accurate and kept up to date;
    v. not be kept for longer than is necessary;
    vi. processed in accordance with the data subject's rights;
    vii. kept safe from unauthorised access, accidental loss or destruction;
    viii. not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

3. Staff and volunteers who process or use any personal and sensitive Information must ensure that they follow these principles at all times. In order to ensure that this happens, the organisation has adopted this Data Protection Policy.

4. Any member of staff, trustee or volunteer, who considers that this policy has not been followed in respect of personal data about him/herself, should raise the matter with the Designated Data Protection Officer initially. If the matter is not resolved it should be raised as a formal grievance.

Notification of Data Held and Processed

5. All employees, trustees, volunteers, members, clients and other members of the public have the right to:

    - know what information the Organisation holds and processes about them and why;
    - know how to gain access to it;
    - know how to keep it up to date;
    - know what the Organisation is doing to comply with its obligations under the Act.

Information and Data Protection Policy

The Data Controller and the Designated Data Controllers

6. The organisation as a corporate body is the Data Controller under the Act, and the organisation is therefore ultimately responsible for implementation. However, Designated Data Controllers will deal with day to day matters.

7. Doorstep has one Designated Data Protection Officer who is the Senior Manager

Information Held

8. Personal Information is defined as any details relating to a living, identifiable individual. Within the Organisation this applies to employees, trustees, volunteers, members, clients and other members of the public such as job applicants and visitors. We need to ensure that information relating to all these people is treated correctly and with the appropriate degree of confidentiality.

9. Doorstep holds personal and sensitive information in respect of its employees, trustees, volunteers, members, clients and other members of the public. The information held may include an individual's name, postal, e-mail and other addresses, telephone and mobile number, subscription details, organisational roles and membership status.

10. Personal information is kept in order to enable the Organisation to understand the history and activities of individuals or organisations within the voluntary and community sector and to effectively deliver services to its members and clients.

11. Some personal information is defined as sensitive data and needs to be handled with special care (see paragraph 20 below).

Processing of Personal Information

12. All staff and volunteers who process or use any personal or sensitive Information are responsible for ensuring that:

    - Any personal and sensitive information which they hold is kept securely; and
    - Personal and sensitive information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

13. Staff and volunteers should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

14. Personal and sensitive information should be:

    - kept in a locked filing cabinet; or
    - in a locked drawer; or
    - if it is computerised, be password protected; or

Telephone Conversations and Meetings

15. If personal information is collected by telephone, callers should be advised what that information will be used for and what their rights are according to the Act.

16. Personal or confidential information should preferably not be discussed in public areas of the Organisation's work premises or within open-plan office areas. Wherever possible, visitors should be escorted to a private interview room or office and not be permitted to wander about the premises on their own. If possible, visitors should subsequently be escorted out of the premises when the meeting is over.

    All staff should be aware of the difficulties of ensuring confidentiality in an open plan area and respect the confidential nature of any information inadvertently overheard. Any notes taken during or after an interview should be of relevance and appropriate. It is recommended that such notes are subsequently filed in a legible and coherent manner and that informal notes are retained for a short period (1 year), in a secure place, before being shredded.

Collecting Information

17. Whenever information is collected about people, they should be informed why the information is being collected, who will be able to access it and to what purposes it will be put. The individual concerned must agree that he or she understands and gives permission for the declared processing to take place, or it must be necessary for the legitimate business of the Organisation.

Publication and Use of the Doorstep's Information

18. Doorstep aims to make as much information public as is legally possible. In particular information about the staff, trustees and members will be used in the following circumstances:

    - Doorstep may obtain, hold, process, use and disclose information in connection with the administration, management and business activities of the Organisation, including making and keeping lists of members and other relevant organisations.
    - We may publish information about Doorstep and its members including lists of members, by means of newsletters or other publications.
    - We may confirm to any third party whether or not any person is a member of the Organisation.
    - We may provide approved organisations with lists of names and contact details of members or other relevant organisations only where the members or other relevant organisations have given their consent.
    - We may use information for anything ancillary or incidental to any of the foregoing.
    - Names of, and a means of contacting, staff and trustees will be published within publicity leaflets and on the website.

- Photographs of key staff may be displayed at the Organisation or placed on the website with their consent.
- Internal staff contact list will not be a public document and information such as mobile telephone numbers or home contact details will not be given out, unless prior agreement has been secured with the staff member in question.

19. Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Designated Data Protection Officer.

Sensitive Information

20. Sensitive information is defined by the Act as that relating to ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. The person about whom this data is being kept must give express consent to the processing of such data, except where the data processing is required by law for employment purposes or to protect the vital interests of the person or a third party.

Disposal of Confidential Material

21. Sensitive material should be shredded. Particular care should be taken to delete information from computer hard drives if a machine is to be disposed of or passed on to another member of staff.

Staff Responsibilities

22. All staff are responsible for checking that any information that they provide to the Organisation in connection with their employment is accurate and up to date. Staff have the right to access any personal data that is being kept about them either on computer or in manual filing systems.

23. Staff should be aware of and follow this policy when handling data, and seek further guidance where necessary. Breaches of this policy may result in disciplinary action.

Retention of Data

24. The Organisation will keep some forms of information for longer than others. Because of storage problems, information about clients cannot be kept indefinitely, unless there are specific requests to do so. In general information about clients will be kept for a minimum of 6 years after they use the services. Please see **Appendix B** for a full description of how long we keep different forms of personal and Information for.

25. The Organisation will also need to retain information about staff. In general, all information will be kept for 3 years after a member of staff leaves the Organisation. Some information however will be kept for much longer, for example, if required by funders. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. A full list of information with retention times is available from the Designated Data Protection Officer.

26. A statement about Data Protection will be displayed clearly within public spaces within the Organisation's premises and on the website. A copy of the Data Protection Statement is contained in **Appendix A**.

Duty to Disclose Information

We will only ever share personal and sensitive information with the individual's consent. However there are some circumstances that we will share personal and sensitive information without the individual's consent and this is when we are required to do so by law. Examples of these situations are described below:

- Suspected/actual illegal activity will be reported to the Police;
- Suspected/actual abuse may need to be reported to the Police and/or Social Services/Safeguarding Adults;
- If an individual or others are at risk of harm we may need to refer this to an appropriate professional;
- In an emergency situation we may contact an individual's next of kin – for example in a medical emergency.

Data Breach

The Organisation has taken every care to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Types of breach 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;
- system failure;
- 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.

Information and Data Protection Policy

Any individual who accesses, uses or manages the Organistion's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The Date Protection Officer, will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Amended May 2018

Appendix A

Privacy Policy Statement

Sharing information with others

- Sometimes we have to confirm or share information with other organisations. If we need to do this, we will make it clear to you on the forms you complete giving us the information.
- We will draw up an agreement with the organisation that we need to share the information with as appropriate. This is so that both sides understand why the information is being passed on, and what use can be made of it. In some cases, a third party organisation, such as a funding body, may draw up the agreement.

Information quality

- We will make sure that the information about you is accurate and up to date when we collect or use it. You can help us with this by keeping us informed of any changes to the information we hold about you.

Information security

- We will keep information about you secure.
- We will protect your information against unauthorised change, damage, loss or theft.

Keeping information

- We will hold information about you only for as long as the law says. After this, we will dispose of it securely and properly.

Openness

- We will tell you what kinds of information we hold and what we do with it.

Access and correctness

- Whenever possible, we will let you see the information we hold about you and correct it if it is wrong.

In general

- We will comply with the Data Protection Act 1998, General Data Protection Regulation 2018, and any subsequent legislation on information handling and privacy.
- We will do this through the Organisation's Data Protection Policy.
- We will help you with any questions or problems that you may have with the Data Protection Act 1998, Human Rights Act 1998, Freedom of Information Act 2000 or General Data Protection Regulation 2018.
- If we cannot help you, we will give you advice on where to write to get the information you may need. Pinilised

Our Commitment

- We will only collect information that is necessary for what we do.
- We will be fair in the way we collect information about you.
- We will tell you who we are and what we intend to do with the information about you.
- Where practicable, we will collect information directly from you.
- If we collect information about you from someone else, we will make sure you know that we have done this whenever possible.

Appendix B

Process for Storing Personal and Confidential Data at 115 Pasture Street

Areas that we collect data from:	What personal and sensitive data do we collect?	How do we protect the data we have?	Do we share this information with any third party organisation?	How long do we keep the personal and sensitive information for?	Action Points
Young people accessing the Drop-in	Name and gender.	Data is on shared folder, computers all are password protected and only staff members have log-in details.	No information is purely collected for monitoring and statistical purposes, to monitor trends in services and for future funding. No actual names are shared will be shared outside the organisation.	Information is kept on the shared folder for 12 months, then placed in an archiving folder.	**1.** Staff should be aware when taking notes from a telephone call names of individuals should not be wrote on Desk Pads where other young people/members of the public could see. **2.** Answer machine messages are monitored daily and deleted once they have been listened to. **3.** Notices are on display in the Drop-in about what information is kept and how to have personal information removed. **4.** Any pending client assessments should be kept confidential, ensure other service users or members of the public do not see the forms and at the end of the day they are locked away. **5.** Client information is shredded/placed in confidential waste if no longer needed**.** **6.** Clients that do not go onto having a support service from Doorstep, their information is to be placed in the archiving box which will be destroyed after 12 months. **7.** Clients are given information on what our organisational process is for collecting personal and sensitive data**.** **8.** Removing names after 12 months on any data-bases/spreadsheet and just keep statistical information. **9.** Also ensure we do not collect any other information other than name and gender. **10**. Staff working in the Drop-in should be aware what information they are saying on the telephone and not disclose people's name or other personal information if there are other people in the Drop-in.

Process for Storing Personal and Confidential Data at 115 Pasture Street

Areas that we collect data from:	What personal and sensitive data do we collect?	How do we protect the data we have?	Do we share this information with any third party organisation?	How long do we keep the personal and sensitive information for?	Action Points
Young people that apply for housing/support service from Doorstep but do not become clients	Names, address, date of birth, gender, national insurance number, previous addresses, copy of ID documents, telephone number, previous convictions and email addresses.	Client Assessments are kept locked away in an archiving box, information on Harmonia is password protected and only Support staff have access to this database.	We share information on the outcome of assessment with The Gateway, which is an online database maintained by the Housing Team at NELC. All our referrals for housing must come through the Gateway, it is an essential part of assessing and housing people. All young people are made aware of this at assessment.	This information is kept for 12 months then it is shredded.	**1.** Make young people aware that their details are maintained for 12 months after they have applied for a service. Notices created and displayed in Drop-in. **2.** To make young people aware that can request for Doorstep to remove their personal information from our records before the 12 month destroy date. Notices created with the information and displayed in Drop-in.

Process for Storing Personal and Confidential Data at 115 Pasture Street

Areas that we collect data from:	What personal and sensitive data do we collect?	How do we protect the data we have?	Do we share this information with any third party organisation?	How long do we keep the personal and sensitive information for?	Action Points
Clients that have received support service from Doorstep (Floating Support or Housing Support)	Names, address, date of birth, gender, national insurance number, previous addresses, telephone number, copies of personal identification, bank details, previous convictions, next of kin details, telephone numbers and email addresses.	Client details in Harmonia is password protected, individual support staff have their own personal log-on details. Paper files are kept in Support Workers office and are in locked filing cabinet, access to the office is only by other staff members (not members of public), key is hidden at the end of the day, once the client is no longer a client, it is placed in archiving which is locked. Paper files are kept in the Housing Office, locked filing cabinet, key is only accessible by Housing Officers. Information is shredded if no longer needed or placed in the archiving system.	We share information on the outcome of assessment with The Gateway, this is an online database maintained by the Housing Team at NELC. Young people are made aware of our use of Gateway throughout their service with Doorstep. Once a young person is receiving a support service from Doorstep, we update Gateway on a monthly basis with their support areas and what work has been completed this month. Updating Gateway is part of our funding requirements and we would be unable to support any young person without updating this Database. We also share information with our Contractors this would be name, address and telephone number - this is to enable them to carry out repairs/maintenance in the property.	Any paper details relating to the client are placed in the locked archiving system after they have left service, this information is kept for 6 years after the support has ended and then it is securely destroyed.	**1.** Amended Client Consent Form which is completed at Assessment, to make sure it conforms with GDPR. **2.** Created Third Party Sharing Information, to be completed at the beginning of their support service. **3.** Notices created for all supported young people to make them aware that we store personal data for 6 years after they have left Doorstep. **4.** Due Diligence Questionnaire sent to Paloma to check they are storing our information correctly **5.** An agreement has been created with the Contractors to ensure they are holding the clients information correctly and what we expect from them. **6.** At the end of a Support Service all paper files relating to the client are placed in the secure archiving system, with a destroy date of 6 years.

Process for Storing Personal and Confidential Data at 115 Pasture Street

Areas that we collect data from:	What personal and sensitive data do we collect?	How do we protect the data we have?	Do we share this information with any third party organisation?	How long do we keep the personal and sensitive information for?	Action Points
General Needs Tenants	Names, address, date of birth, gender, copies of ID documents, national insurance number, previous addresses, telephone number, bank details and email addresses.	Paper files are locked in Housing Managers Office, only Housing Officer's has access.	The only third party organisation we would share information about General Needs Tenants would be Housing Benefit/Universal Credit, we are unable to process rents without sharing this information to HB.	Information is kept for 12 months after they have left our accommodation, this information will be kept for longer if there are arrears on the account after they have left.	**1.** Notices created and sent to general needs tenants to make them aware that their information is stored for 12 months after they have left Doorstep property. **2.** Notices also let general needs tenants know how they can go about their information removed after they have left Doorstep property, as long as they have no rent arrears. **3.** Once General Needs Tenants have left Doorstep property, all their personal details and client files to be placed in secure archiving system with a destroy date of 12 months.
Supported Lodgings Providers (including Nightstop Hosts)	Name, address, date of birth, national insurance number, telephone number, email addresses and copies of identityocuments.	Only workers directly working on this service have access to this data, currently this is two workers, Supported Lodgings Co-ordinator and Operations Service Manager.	The only third party organisation we share host information is Housing Benefit/Universal Credit, this is to process rent benefit payments. The personal information that is shared is name and address.	We keep personal information on providers for as long as they are providing a service to Doorstep, if they are no longer a provider, this information will be shredded after 3 years.	**1.** Data Protection Statement created and sent out to all Supported Lodgings Providers, with details of how we store their personal information, how their personal information is used and how long we store it for after they leave. **2.** Once they are no longer a Provider all personal information to be placed in secure archiving system with a destroy date of 3 years later.

Process for Storing Personal and Confidential Data at 115 Pasture Street

Areas that we collect data from:	What personal and sensitive data do we collect?	How do we protect the data we have?	Do we share this information with any third party organisation?	How long do we keep the personal and sensitive information for?	Action Points
Employee Details/Temp Staff	Name, address, date of birth, national insurance number, mobile telephone number, DBS checks, copies of ID, previous convictions and bank details.	Staff details are kept in a filing cabinet in the Senior Manager's office, the cabinet is locked and only the Senior Manager has access to the cabinet and the key. On People HR individual staff can only see their personal information and have no access to other employee's information. Unless they are a Line Manager's/Supervisors they will then have access to online records for the individuals they manage. There are 3 administrators who have access to all information on the online hr system. Finance and Business Support Officer keeps all personal staff information in a locked filing cabinet which is only accessible by staff in the Finance Team.	We share information regarding employees with Data Plan who process our wages, we also share information with People's Pension who process our employer's pension and we use an online database called People Hr for all our HR info on annual leave, sickness absence, toil and this contacts staff personal information.	Staff details are kept on file whilst they are employed by Doorstep, once they are no longer employed their details are kept for 3 years and will then be confidentially shredded.	**1.** Staff are securely archived once they are no longer employed by Doorstep and destroyed 3 years later. **2.** Third party organisations are contacted and ask them to complete Due Diligence Questionnaire to ensure they are using our data correctly. **3.** Once third parties have completed their DD Questionnaire, we will then ask them to sign a Data Protection Agreement which will be redone every 3 years.

Process for Storing Personal and Confidential Data at 115 Pasture Street

Areas that we collect data from:	What personal and sensitive data do we collect?	How do we protect the data we have?	Do we share this information with any third party organisation?	How long do we keep the personal and sensitive information for?	Action Points
Unsuccessful Employee Applicants	Name, addresses, date of birth, telephone number, email addresses, previous convictions and national insurance numbers.	Only Senior Manager stores these applications, the filing cabinet is locked with only the Senior Manager having access to the filing cabinet.	No information is not shared with any third party organisation/agency.	We will hold unsuccessful employment applications for 6 months, then they will be securely destroyed.	**1**. All un-successful applicants are placed in secure archiving with a destroy date of 6 months post interview.
Trustee Details	Name, addresses, date of birth, telephone number, email addresses and national insurance numbers.	Trustee details is kept in locked filing cabinet only key members of staff have access to this information.	We share Trustee personal details with Charity Commission, Accountants, Funding Applications and our Bank has a record of our Trustees. This is part of governance and must be done to comply with various laws.	Trustee details are kept on file whilst they are an active member on the Board, once they are no longer a Trustee their details are kept for 3 years and will then be shredded.	**1**. Ex-trustee personal details are to be placed in the secure archiving system with a destroy date of 3 years.