**POLICIES & PROCEDURES –** **DATA PROTECTION AND INFORMATION GOVERNANCE**

**PURPOSE:**

To set out the approach of GNFC with regard to Data Protection and Information Governance

**RELATED POLICIES & PROCEDURES:**

* Privacy, Confidentiality & Access to Information
* Protection from Abuse & Discrimination (Adult and Children)
* Informing Service Users
* Management of Information Technology
* Partnership working
* Record keeping
* Privacy
* Risk Assessment and Risk Management
* Health and Safety
* Management of Incidents, High risk Incidents and Emergencies

**INTRODUCTION**

This document contains a policy statement (Part One) and procedural guidance (Part Two). The functions of each are set out briefly below.

**Part One – Policy Statement.** The policy statement sets out the broad framework of principles within which the particular area of work will be carried out. It sets out the organisation’s broad style and approach to the issue, including any aims and guiding principles.

**Part Two – Procedural Guidance.** The procedural guidance sets out the details that staff will require to carry out their duties in this particular area of work. It also sets out the specific tasks involved in undertaking this area of work and identifies who is responsible for carrying them out.

**PART ONE: POLICY STATEMENT: AIMS AND PRINCIPLES**

1. Good News Family Care’s Policy is to comply with the requirements of the Data Protection Act 1998 and General Data Protection Regulations 2018. This statement relates to information held by Good News Family Care (Homes) Ltd. on personal and sensitive personal data about service users, employees, and other individuals connected with the organisation, for example job applicants, volunteers, members and other contacts.
2. We employ different measures to keep your data safe, and to prevent any unauthorised access to, or disclosure of information. This includes ensuring that written personal data is locked in a secure filing cabinet and room not accessible to unauthorised people. Electronic data is held on secure devices or our secure server which is accessible by authorised staff, and with different access levels based on job roles and responsibility.
3. Staff have a legal and professional responsibility to:
* Provide a confidential service to clients, sharing information lawfully and appropriately.
* Process information regarding service users in accordance with data protection regulations, information sharing guidelines and ensuring respect of the rights of individuals.
* Comply with Freedom of Information requirements.
* Record information accurately and ensure it is accessible needed.
* Ensure information is held securely.
1. Personal Data refers to information which can identify someone, or that which on or has the potential to impact an individual for example their name, date of birth, medical details. The Data Protection Act sets out 8 principles of how to handle personal data:
* Fairly and lawfully processed
* Processed for limited purposes and not in a manner incompatible with those purposes
* Adequate, relevant and not excessive
* Accurate
* Not kept for longer than is necessary
* Processed in accordance with an individual’s rights
* Secure
* Not transferred to other countries without adequate protection
1. Personal information may be shared with other people or professionals if:
* the service user has given consent and/or
* there is a legal base permitting it and/or
* there are exceptional circumstances in the overriding public interest.

**PART TWO: PROCEDURAL GUIDANCE**

GNFC appoints a lead person for with responsibility for overseeing, co-ordinating, publicising and monitoring standards of information handling within the organisation and for developing and implementing an Information Governance (IG) improvement plan.

The named lead is: Johanna Collier.

1. **General Data Protection Regulation**

The ‘General Data Protection Regulation’ (GDPR) introduced by the European Parliament, the Council of the European Union and the European Commission strengthens and unifies data protection for all individuals within the European Union (EU). The legislation promotes accountability, governance and transparency.

The GDPR provides the following rights for individuals:

* The right to be informed
* The right of access
* The right to rectification
* The right to erasure
* The right to restrict processing
* The right to data portability
* The right to object
* Rights in relation to automated decision making and profiling.
1. Every organisation or sole trader who processes personal information is required to register with the Information Commissioner’s Office (ICO). GNFC are registered with the ICO, the registration number is: Z8278134. Information regarding data breaches is reported to the ICO.
2. **Data Collection
Types of information GNFC collects**
* Personal data: provided by service users, employees, supporters or other individuals connected to GNFC according to the nature of the relationship and information required.
* Information we generate: additional information will be generated such as key work session notes, disciplinary records, sickness records and referrals to other agencies.
* Information from third parties: Information may be sought/received from third parties. This includes but is not limited to information from the probation service, or in relation to housing benefit and/or unemployment benefits.
* Sensitive personal data: We collect and store sensitive personal information (this includes racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, health information concerning our residents and employees (as appropriate). We will take extra care with this information, to ensure that everybody’s privacy rights are protected.
* Accidents and incidents: If an accident or incident occurs on our property, we will keep a record of the incident (which may include both personal and sensitive personal data). We will also share this information with statutory bodies as required.
	+ - 1. Information is only collected and used when necessary to fulfil a contract or agreement; comply with a legal duty and to protect an individual’s personal and lawful interests.

Good News Family Care (Homes) Ltd.collects and processes data for:

* **Standard Business Purposes**
This includes staff administration, advertising, marketing and public relations, accounts and records, service user records and plans, recruitment, appraisals, performance review, training, pay and remuneration, pension and insurance, payroll, tax, national insurance, health and safety, disciplinary and grievance (this list is not exhaustive).
* **Processing Not for Profit Organisation**
This includes records of GNFC supporters, providing or administering activities for individuals who are either supporters of the organisation or have regular contact with it.
* **Realising the Objectives of the organisation**
This includes records relating to services provided by GNFC, fundraising and administration associated with funding bodies
* **Data audit**
Data audits are completed periodically to collect outcomes, monitor service delivery and review record keeping.
* **Retention of Data Periods**
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose that it is required. This applies to both paper and electronic records.

|  |  |
| --- | --- |
| **Related to Service Users** | **Minimum time of retention** |
| Service User Records/Risk Management/Support Plan | 50 years (paper/electronic) |
| Refused/Declined Referral Forms | 1 year |
| Communication Book | 2 years after year end |
| Work Diary | 2 years after year end |

|  |  |
| --- | --- |
| **Related to Service Provision** | **Minimum time of retention** |
| Minutes of meetings | 2 years |
| Accident Register | 10 years |
| Incident Forms | 10 years |
| Audits | 2 years |
| Health and Safety documentation | 2 years |
| Complaints | 8 years following completion of action |
| Flexible working hours for staff | 6 months |

|  |  |
| --- | --- |
| **Related to Recruitment & Employees** | **Minimum time of retention** |
| Application forms of successful applicant | Duration of employment |
| References received | 1 year |
| Payroll & tax information | 7 years |
| Sickness records | 3 years |
| Annual leave records | 2 years |
| Unpaid leave/special leave records | 3 years |
| Appraisal and performance review | 5 years |
| Promotion/transfer/training | Through duration of employment and 1 year after |
| Disciplinary matters | According to Disciplinary policy |
| References given/information to enable references to be given | 5 years from end of employment |
| Summary of record of service: Name, positions held, dates of employment, records relating to accident or injury at work | 12 years |

1. **Disposal of Confidential waste**

A cross-cut shredder is used to destroy confidential waste.

1. **Information Sharing**

Poor or non-existent information sharing is a factor repeatedly identified as an issue in Serious Case Reviews. Effective information-sharing underpins integrated working and is a vital element of both early intervention and safeguarding. As stated in government guidance for Information Sharing (2018), the 7 Golden rules for sharing information are:

* Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure personal information about living individuals is shared appropriately.
* Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
* Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
* Share information, where possible with consent and respect for the wishes of those who do not consent to their information being shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.
* Consider safety and well-being: base information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
* Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
* Keep a record of your decision and the reasons for it – whether to share information or not. If you decide to share, record what you have shared, with whom and for what purpose.

Information shared with professionals must be:

* Necessary and proportionate, considering the right amount/type of information proportionate to the level of risk.
* Relevant for the purpose of being shared, with those who need the information.
* Adequate and sufficient quality to ensure it can be relied upon.
* Accurate, factual and up-to-date.
* Shared in a timely way, to reduce the risk of missed opportunities to offer support and protection.
* Shared in a secure and appropriate way.
* Recorded.

There may be situations where progress of service-users is shared with partner agencies. Whenever possible consent will always be obtained prior to sharing information unless there is a safeguarding risk when it may be necessary to share without their prior knowledge. In all other instances, consent will always be obtained prior to sharing of information, such as with supporters of the charity for promotional purposes. In these cases, information will normally be anonymised, other than when a personal testimony.

1. **Disclosure to third parties**

Data may be transferred to third parties where the data is required to transact GNFC business, such as insurers, bankers, legal & other professional advisors, pension schemes and funders.

Information is never sold. Data will not be disclosed to other third parties by GNFC without the data subjects consent, for example:

* Mortgage company requesting employment period and pay details.
* Third parties requesting personal telephone numbers (excluding mobile phones solely for work use), or home addresses.

Access to personal files is restricted for all personnel to ensure security and confidentiality. Personal files can only be accessed where there is a specific need such as:

* Line managers updating personnel records
* Next of kin details needed for emergency contact.
* Service User records/support plans being updated by Support Workers.
* Line Manager supervision/quality assurance regarding service user records.

Service Users’ permission will be obtained before disclosing personal data to a third party. The only time this will be overridden is if:

* There is a Child Protection issue
* There is a need to protect the interests of the service user (ie it is a dangerous situation)
* GNFC is required by law to do so
* GNFC is assisting in the prevention or detection of a crime.
1. **Data Protection – Service User Records**

When staff are recording information and sharing information, they must do so using the Caldicott principles which are quoted as follows:

* Justify the purpose(s): Every single proposed use or transfer of patient identifiable information within GNFC or from another organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate individual.
* Don't use patient identifiable information unless it is necessary: Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
* Use the minimum necessary patient-identifiable information: Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
* Access to patient identifiable information should be on a strict need-to-know basis: Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
* Everyone with access to patient identifiable information should be aware of their responsibilities: Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
* Understand and comply with the law: Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.
* The duty to share information can be as important as the duty to protect patient confidentiality: Professionals should in the patient's interest share information within this framework. Official policies should support them doing so.

Client records should be adequate, relevant and not excessive in relation to the purposes for which they were processed, the organisation will only retain information necessary information.

Each service user’s details are kept in a personal file, contained in a secure, locked cabinet. Any confidential information regarding clients stored electronically is password protected on a computer only accessible by appropriate staff members. The information contained in the file might include: Initial referral information, licence agreements, support plans (action plans and reviews), minutes of meetings, copies of correspondence.

Under the provision of the Data Protection Act clients can access their records on request. To do this, the service user should discuss their request to do so with a manager or their key-worker. To avoid parts of the record being changed or removed, a member of staff should be present while the service user reviews their records.

Information regarding service users will be shared between staff, volunteers and the management committee **only on a need to know basis**. Personal details disclosed by an individual on a one to one basis will remain confidential unless the following circumstances prevail:

* There is a direct effect on the safety of GNFC premises and individuals within it
* There is a Safeguarding/Child Protection/Adult Protection issue
* A service user is threatening to harm themselves

Where external agencies have ongoing relationships with residents, all parties concerned will agree boundaries of confidentiality. In some circumstances, it will be necessary to share some information with professionals or/and partner agencies working with a service user. Consent to share this information with relevant professionals/agencies is obtained from service user wherever possible.

1. **Data Protection – Employee Records**

Each employee’s details are kept in a personnel file, contained in a secure cabinet in a locked room. The information contained in a personnel file might include: Application Form, Curriculum Vitae, salary details, holiday request forms, sickness record and medical certificates, appraisal forms, disciplinary records and copies of correspondence between the parties.

The organisation undertakes not to compile an excessive amount of information and seek and retain only that information which is adequate and relevant.

All employees and volunteers who have unsupervised contact with service users have Enhanced DBS checks for which the certificate must be shown to the recruiter. Details of the DBS certificate will be saved on a confidential file. The DBS certificate is the property of the individual it concerns; therefore, they must keep the certificate. No copies of DBS certificates are kept by GNFC.

The information is only available to the Management Committee for the purpose of carrying out their function within the organisation. Information will not be disclosed to a 3rd party, unless there is a legal duty to do so.

In order to ensure that employment records are up to date, we will from time to time inform each employee of the basic personal details that are on file. It is necessary to advise us if this information is inaccurate and of the relevant amendments.

Employees are entitled to view their personnel file, and if you wish to do so, an appointment should be made with your department manager. Employees cannot remove the file from the organisation’s offices.

1. **The Freedom of Information Act 2000**

All recorded information is covered by the Freedom of Information Act 2000, there are specific exemptions that stipulate how certain types of information must be protected or released. Generally, if there is no harm to be caused by disclosing the information, there is no reason to withhold the information, although special care and consideration needs to be taken when releasing personal information about an individual.

The Freedom of Information Act came fully into force on 1st January 2005. It is the implementation of freedom of information legislation in the United Kingdom on a national level. It introduces a public “right to know” in relation to public bodies. It covers:

* Central Government
* Local Government
* National Health Service including voluntary hospitals
* Maintained schools, universities, institutes of technology, colleges of education and other educational institutions
* Police

Good News Family Care has an obligation to provide information regarding the governance and management of its services. The annual report is available via the Charity Commission website, and certain other information can be available on request according to need.

Requests for information should be made in writing using the form in Appendix 1. Management will respond to requests for information within 1 month, according to the stipulated timescale in the General Data Protection Regulation. If necessary GNFC can request further clarification on what information is required. If the application for information is refused, the individual will be informed why and that they have the right to complain or appeal the decision.

Information regarding service users is confidential and must not be shared with people who do not have a need to know the information. Where residents request to view their records, they should do so in writing. When viewing records, a member of the management team will be present and respond to questions.

1. **CCTV**
GNFC premises have CCTV, therefore service users and visitors may be recorded. CCTV is used to aid security and to protect staff, residents and their possessions. CCTV will only be viewed when necessary (eg for reasons for security, or to detect or prevent unauthorised activity).
2. **Breach of Personal Data**
* A personal data breach means a security breach leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data, it is more than losing personal data.
* A breach of data is reportable to regulatory bodies when it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental effect – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. The service manager/co-ordinator will discuss the breach with senior management and report the breach to regulatory bodies where applicable.
* GNFC will notify both the individual/s which the breach affects and the Information Commissioners Office (ICO) without delay and within a maximum of 72 hours from when the breach is identified.
* If a staff member breaches data protection guidelines, this may lead to disciplinary action within GNFC.
1. **Organisation management**

Where there are changes to how services or systems are managed, the management team will ensure that the rights of service users are not affected and that there are no breaches of data protection.

**Appendix 1: Information Request Form**

This form should be used to request access to information under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004.

Your name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Your address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Contact number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Description of the information you require**

Please describe as fully as you can the information you are seeking. If your description is not clear or is ambiguous we will ask for clarification.

|  |
| --- |
|  |