The Green House Data Protection Policy

Date of last review: June 2023 Date of next review: March 2024

Staff Name	Title	Date Reviewed
Gemma Halliwell	CEO	March 2023
Josh Taylor	DPO	June 2023
Gemma Halliwell	CEO	June 2023

Roles & Responsibilities

- Data Protection Officer (DPO): Josh Taylor
- SIRO: Gemma Halliwell
- Caldicott Guardian: Natalie King
- HR Officer: Tara Krgo

This Data Protection Policy is the overarching policy for data security and protection, and should be read in conjunction with other relevant policies, including:

- Data Security Policy - outlines procedures for ensuring the security of data including the reporting of any data security breach
- Record Keeping Policy - details transparency procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures), information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share
- Safeguarding Policy
- Whistleblowing Policy
- Employee Handbook
- Contract of Employment
- Remote Working Policy
- Client and Donor Privacy Policies

Contents

1 Introduction

We want everyone who comes to The Green House for support, who works for our organisation, or supports our work to feel confident and comfortable with how any personal information will be securely looked after or used.

The Green House holds and manages a lot of personal data about individuals such as (but not limited to): services users (including children, young people, parents and carers, and professionals working with the child and/or family); employees and associates; donors; and suppliers.

Data protection legislation requires us to collect control and process data in ways which both protect the rights of the individual, and also gives us powers to do our jobs.

The law tries to strike a fine balance between the rights of the individual, and needs of organisations like The Green House to have access to and be able to process data.

Data can be held on individuals in a variety of ways – in paper form, in creative materials, on The Green House network, our case management system OASIS, and The Green House IT applications and databases.

Ensuring the integrity and security of the data we hold on individuals is important both in terms of (a) our responsibilities to our clients, (b) legal compliance, (c) safeguarding the rights of individuals, and (d) our reputation in the sector.

2 Definitions & Legal Background

The Data Protection Act 1998 (“DPA”) codified the eight data protection principles, and brought in rules as to how data controllers and data processors should obtain, use, store, share, alter & update and erase personal data.

The 8 Data Protection Principles are:

1. Personal data should be processed fairly and lawfully.
2. Personal data should be obtained and processed only for specified lawful purposes.
3. Personal data should be adequate, relevant and not excessive in relation to the purposes for which it is obtained.
4. Personal data should be accurate, and kept up to date.
5. Personal data should not be kept for any longer than is necessary for the purpose it was collected for.
6. Personal data should be processed in accordance with the rights of the data subject.
7. Appropriate technical and organisational measures should be taken against. unauthorised or unlawful processing, loss or destruction of data.
8. Personal data should not be transferred to a territory outside the EEC unless there is an adequate level of protection for the rights and freedoms of data subjects in that territory.

The DPA brought in the following key definitions, which are used in this Policy:
Personal data - Data relating to a living individual. (This can be facts and opinions.)
Data subject - The individual who is the subject of the personal data. The individual owns his/her personal data. The data subject cannot be a dead person, or someone who cannot be identified from grouped or anonymised data.
Data controller - The person/organisation who determines the purposes for which and the manner in which data is collected, stored, processed, shared, updated/altered and ultimately deleted/destroyed.
Data processor - A person/organisation outside of the data controller who processes the data on behalf of the data controller.

The General Data Protection Regulations ("GDPR") were published in May 2016, and came into force on 25 May 2018 by the Information Commissioner's Office ("ICO"). GDPR keeps the same core 8 principles as DPA, and uses the same key definitions above.

GDPR brings in the following additional requirements to the DPA:

- A greater requirement for consent to be freely given, informed and for specific purposes. Consent is temporary and should be regularly refreshed.
- Data subjects have more rights – the right to object to processing; the right to be forgotten; and the right of data portability.
- Data processors must fully comply with GDPR.
- Subject access request will be free of charge (previously £10 fee) and must be complied with within 30 days (previously 40 days).
- Data controllers must fully document processes and rationale for how they store and manage data.
- All data breaches must be reported to the ICO.
- New role of Data protection Officer ("DPO") created.
- ICO gains new powers, including significant fines and penalties.

The 2018 Data Protection Act ensures that the provisions of GDPR will continue post Brexit, and also consolidates other related legislation. The Act also clarifies and confirms the powers that criminal justice agencies have in relation to data processing, as well as the rights of data subjects within the criminal justice system.

3 Purpose and aim of the policy

The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

This policy aims to clarify roles and responsibilities of all staff, Trustees and volunteers of the need to collect and handle personal data in line with data protection legislation, and in ways which minimise risks to (a) the data subject; (b) the integrity and security of the data, and (c) The Green House's reputation. This includes data which is processed either in hardcopy or digital copy, including special categories of data.

All of The Green House's procedures and projects should incorporate data protection principles and safeguards "by design", rather than data protection being an afterthought. This policy applies to all staff, including temporary staff and contractors.

The Green House expects our partners to uphold our commitment to achieve and maintain "best practice" in relation to data protection. Data protection will, therefore, always be a core component of all of our contracts, agreements and ways of working with our partners, and we will ask partners for copies of their data protection policies and procedures.

The principles of data protection and data protection "best practice" should also be applied when working with anonymised or pseudo-anonymised data. All staff, associates, Trustees and volunteers working on behalf of The Green House have a duty to understand and work according to this policy, and to 8 the data protection principles.

4 Statement of Policy

The Green House will:

- Through the establishment and maintenance of policies we will at all times ensure the capture, management, processing, updating, sharing and archiving/deleting of personal data is done in accordance with prevailing legislation and current best practice. This includes the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.
- We will ensure all staff (including associates), Trustees and volunteers understand their roles and responsibilities with respect to data protection.
- Provide training to all staff (and associates), Trustees and volunteers on the principles of data protection and this policy.
- Promote data protection by design on all its activities and projects from the beginning of any data processing and during the planning and implementation of any new data process, including completion of a Data protection Impact Assessment (DPIA) where appropriate. We'll provide clear procedures for staff to follow which enable compliant processing and management of data. Data protection by design will include (but is not limited to) performing privacy impact assessments on new activities and projects, and validating and documenting the legal basis on which we capture, manage and potentially share personal data.
- Appoint a Data Protection Officer, and will promote internally the responsibilities and duties of the DPO. The Green House will support the DPO in the performance of their duties, in accordance with ICO guidance. We guarantee that the DPO will not be pressured on how to carry out their tasks, and that they are protected from disciplinary action when carrying out the tasks associated with their role.
- We will undertake annual audits of our compliance with legal requirements.
- Ensure that all relationships with 3rd parties (e.g. partners, suppliers, other agencies) take due account of data protection issues, with data protection being a key component of all external contracts and arrangements

- Respond to subject access requests in accordance with prevailing legislation and best practice.
- Respond to requests from the ICO in a prompt and compliant manner.
- Maintain a log of data breaches, and report data breaches to the ICO in accordance with prevailing legislation and associated guidance.
- Maintain and develop IT systems and controls which incorporate best practice data security and data protection.
- Ensure all staff and trustees are trained on the IT and internet usage policy, as outlined in the Employee Handbook.
- We acknowledge our accountability in ensuring that personal data shall be:
    - Processed lawfully, fairly and in a transparent manner.
    - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
    - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
    - Accurate and kept up to date.
    - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation').
    - Processed in a manner that ensures appropriate security of the personal data.
- We uphold the personal data rights outlined in the GDPR:
    - 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.

This policy will be widely promoted and is mandatory for everyone involved in The Green House. Failure to comply with the policy and procedures will be addressed without delay and may ultimately result in disciplinary action or dismissal from the organisation.

5 Responsibilities

5.1 All staff (including associates), Trustees & volunteers

Everyone working at The Green House must:

- Ensure they are familiar with this policy and understand it, and how it relates to their job in their team/project.
- Undergo regular GDPR training, including as part of induction and refresher courses at least every 12 months.
- Ensure that, at all times, they are capturing, amending, updating, processing and deleting/archiving data in accordance with the data protection principles and this policy.
- Ensure data is as accurate and as complete as possible. This responsibility extends to any system the staff member has access to in both hardcopy and digital records by making sure all data has the following characteristics:

    - Authentic – i.e. the data is what it claims to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed
    - Reliable – i.e. the data is complete, accurate, has been created close to the time of the activity it records, and has been created by individuals with direct knowledge of the event it records
    - Integrity – i.e. the data is complete and unaltered, it is also protected from being changed or altered by unauthorised persons, any alterations are clearly marked and the person who made them can be identified
    - Useable – i.e. the data can be located when it is required for use and its context is clear in a contemporaneous record
- Understand the data protection risks associated with their job, and how to mitigate against them.
- Understand the role of the Data Protection Officer (DPO), and discuss or report any data protection issues to them.
- Understand what a subject access request is and refer any subject access request immediately to the DPO and their line manager for triage and advice on how to deal with, before taking any action themselves.
- Understand what a data breach is and report any suspected breach immediately to the DPO and their line manager to assess, before taking action themselves.
- Make appropriate checks and take any necessary action before sharing any personal data outside of The Green House (always check first with line manager and/or DPO).
- Make the DPO aware if they have grounds for believing there is deliberate non-compliance with data protection policy and procedures by colleague(s) within The Green House, or by other agencies we work with (see also Whistleblowing Policy).
- Comply with The Green House IT and internet usage policy, as set out in the Employee Handbook.

5.2 Staff directly working with clients must:

- Follow specific role guidance as set out in staff handbooks and OASIS manual to ensure that best practice policies are followed in all activities that involve personal data.
- Where consent is required for the processing of personal data ensure that informed and explicit consent is obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in our Record Keeping Policy: Withdrawal of Consent procedures. Ensure that it is as easy to withdraw as to give consent.
- Upload client information onto OASIS as soon as possible. Working documents may be temporarily stored on work devices with password protection, or in paper form in a locked cabinet. Once client documents are finalised these must be uploaded to Oasis and securely destroyed.
- Ensure that records on OASIS are accurate and kept up to date.
- Ensure that only initials or case reference numbers are used in staff notebooks. Notebooks need to be securely stored when not in use, such as in a locked cabinet, and securely shredded when no longer in use.

- Regularly audit their work laptop and phone devices to ensure that no identifiable client data is stored on their device or on The Green House network (SharePoint/One Drive)
- When storing client's phone numbers on a mobile phone, their details should be recorded using their initials and OASIS number. Client details should never be stored on a personal device.
- For emails where confidential information about a client is being disclosed internally, use client initials and OASIS reference number wherever possible.
- Staff must consider risk when sending emails externally that contain personal data. Both the recipient and sender must have access to secure email.
- Staff must consider risk when sending letters to clients. It may be appropriate to have documents signed for. All post should have a clear return address on the outside.

5.3 Line Managers

Additionally, Line managers must:

- Ensure they and their team's receive regular data protection training, and understand data protection risks in relation to their team's work.
- Ensure their teams understand and know what do in the event of a subject access request or suspected data breach.
- Ensure that data protection by design is built into their team activities/projects, together with changes to projects/activities, and also in respect of new projects/activities.
- Ensure that their teams have, and adhere to, clear team specific rules/requirements on data protection, including (but not limited to); data capture, data processing, data sharing, and data and document retention/anonymising and ultimate destruction.

5.4 The Data Protection Officer (DPO)

The DPO will:

• Be the contact link with the ICO on all data protection issues.
• Act as the contact for data subjects regarding all issues related to processing of their personal data and to the exercise of their rights under Data Protection Legislation.
• Keep abreast of changes to data protection legislation and will update the Board, SLT and teams on upcoming changes and their implications to The Green House and our operating model.
• Advise the Board, SLT, line managers and staff on data protection issues, including updates and amendments to this policy.
• Oversee any changes to systems and processes
• Working with the SIRO, understand the risks associated with the nature, scope, context and purposes of processing for the organisation.
• Monitor compliance with the GDPR and the Data Protection Act 2018
• work with the SIRO to complete Data Protection Impact Assessments (DPIAs).
• Assess all subject access requests and data breaches and advise on the most appropriate course of action.
• Engage the support of suitably qualified data protection professionals to advise on any data protection issues which are too complex or technical for the DPO to advise.

• Work with IT providers to ensure we have up to date and effective IT and cyber security, including data back up. This will include maintaining appropriate IT security accreditations, such as Cyber Essentials.
• Define our data protection policy and procedures and all related policies, procedures and processes and to ensure that sufficient resources are provided to support the policy requirements.

5.5 The Senior Information Risk Owner (SIRO)

The SIRO will:

• Approve the data protection policy and any subsequent changes to it.
• Designate a DPO, and ensure the DPO has sufficient training and support to discharge their responsibilities.
• Ensure the Board of Trustees is briefed on data protection issues.
• Update the risk register with respect to data protection risks.
• Ensure the long term IT strategy takes full account of data protection issues and risks Links to other Policies/documents.
• Ensure that all contracts/arrangements their teams have with external agencies (including data sharing agreements with data processors) incorporate best practice data protection principles and clauses; and that these contractual provisions are adhered to, and are updated in accordance with prevailing legislation/best practice.
• Act as an IRM focal point dealing with risk resolution across the organisation and with other escalated risk issues raised.
• Ensure that data protection impact assessments (DPIA's) are carried out on all new projects in accordance with the UK General Data Protection Regulation (UK GDPR)/Data Protection Act 2018 (DPA 2018) utilising any guidance provided by the Information Commissioner.
• Develop and implement an information risk policy that is appropriate to all departments of the organisation and their uses of information, setting out how compliance will be monitored.
• Ensure that information risk management methods and standards are documented, applied and maintained consistently throughout the organisation's information risk assessment process and management framework.
• Review all key information risks faced by the organisation and its partners, on a regular basis, ensuring that mitigation plans are robust. These risk assessments and mitigation actions will need to benefit from appropriate independent scrutiny so that the identified risks can inform investment decisions including outsourcing.
• Initiate and oversee a comprehensive programme of work that identifies, prioritises and addresses IG risk and systems' accreditation for all parts of the organisation, with particular regard to information systems that process personal data.
• Ensure information risk assessments are completed on a quarterly basis, taking account of all available Information Governance and data security guidance.

5.6 Caldicott Guardian

The Caldicott Guardian will:

- Ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles
- Play a key role in ensuring that The Green House satisfies the highest practical standards for handling person-identifiable information.
- Represent and champion confidentiality issues at Board/senior management team level
- Main concern is information relating to clients and their care, but the need for confidentiality extends to other individuals, including their relatives, staff and others.

5.7 The HR Officer

The HR officer is responsible for staff induction and ongoing L&D, and in that capacity (and with support of the DPO) will ensure that:

- Data protection is included in all new members of staff's induction
- Data protection update/refresher training is regularly delivered across The Green House, and particularly in advance of any regulatory changes.