DATA PROTECTION POLICY

Data Protection Act 2018

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. It also considers the provisions of the General Data Protection Act that became enforceable 25 May 2018 and has subsequently been updated to the UK GDPR, effective January 31, 2021.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection- regulation-UK GDPR/principles/

Naomi's Garden (NG) collects and uses personal information about staff, clients, students, parents, and other individuals who come into contact with the organisation. This information is gathered to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the charity complies with its statutory obligations.

This policy statement applies to all Trustees, employees, other staff, and individuals about whom NG processes personal information, as well as other partners and companies with which the organisation undertakes it business. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Data Controllers

Naomi's Garden are 'Data Controllers' under the Data Protection Act 2018 and must 'Notify' (register with), the Information Commissioner's Office on the following website, unless exempt:

https://ico.org.uk/for-organisations/register/

Review frequency: At least every two years (Registration is annual).

Approval: The Governing body is free to determine how to implement. Further information is on the Information Commissioner's Office website:

https://ico.org.uk/

The Registration/Self-Assessment (to find out if we are exempt can be found at:

https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/

Legislation: The Data Protection Act 2018 (with consideration to the six data protection principles appearing in Chapter 2):

https://www.legislation.gov.uk/ukpga/2018/12/part/4/chapter/2/enacted

We at Naomi's Garden are the Data Controller for the purposes of the Data Protection Act.

NG is required under Data Protection legislation to comply with essential good practice in respect of the information collected here and to manage it securely. All records will be kept confidential. We will not pass on information to any third parties unless we have received permission to do so. The individuals who are the subject of the information or who have parental/ guardian responsibility are generally entitled to see the information and are encouraged to help keep the information up to date. This information will be used for educational, planning, or managerial purposes and to keep parents, clients and staff informed of NG events and dates.

The charity also has a duty to issue a Fair Processing Notice to all clients and parents; this summarises the information held on clients, why it is held and the other parties to whom it may be passed on.

Under Article 6 of the UK GDPR, the lawful basis for processing the workforce, parents and trustees information is to fulfil legal, contractual obligations and other legitimate interests. Consent will be requested for specific activities (at the time of activity) where activities require processing of data if deemed suitable.

Data Protection Officer / Lead

The Data Protection Lead in Naomi's Garden is Amanda Franklin

Personal Information

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. The UK GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria.

We need to collect and use certain types of personal information about people with whom we deal in order to operate. These include current, past, and prospective employees, children, suppliers, clients, and others with whom we communicate. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments.

This personal information must be dealt with properly however it is collected, recorded, and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the Data Protection Act 2018. We regard the lawful and correct treatment of personal information by the organisation as very important in order to secure the successful carrying out of operations and the delivery of our services, and to maintaining confidence with those whom we deal. NG wishes to ensure that it treats personal information lawfully, correctly and in compliance with the 2018 Act.

To this end we fully endorse the obligations of the Act and adhere to the Principles of Data Protection, as enumerated in the 2018 Act.

We collect information from parents/carers and clients and may receive information about them from their school other therapists and professionals. We hold this personal data and use it to:

- Support teaching, learning and therapy;

- Monitor and report on progress;
- Provide appropriate pastoral care,
- Assess how well our organisation is doing.

This information includes contact details, attendance information, characteristics such as ethnic group, special educational needs, and any relevant medical information.

We will not give information to anyone outside the organisation without consent unless the law and our rules permit it.

We are required to pass some information to the Local Authority (LA)

If anyone would like to see a copy of the information we hold and share about them personally, then please contact the Data Protection Lead.

Data Protection Principles

Specifically, the Principles require that personal information shall:

- be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions as set out in the 2018 Act are met;
- be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed;
- be accurate and, where necessary, kept up to date;
- not be kept for longer than is necessary for that purpose or those purposes;
- be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

Our Commitment

NG will, through appropriate management and application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used, including its accuracy and relevancy for the purpose(s) specified;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the 2018 Act. These include:

- the right to be informed that processing is being undertaken;
- the right of access to one's personal information;
- the right to prevent processing in certain circumstances;
- the right to correct, block or erase information which is regarded as erroneous;

- take appropriate technical and organisational security measures to safeguard personal information;

and

- ensure that personal information is not transferred abroad without suitable safeguards.

Compliance

In addition, NG will take steps to ensure that:

- there is an understanding that everyone is personally responsible for Data Protection within the organisation
- everyone managing and handling personal information understands that they are responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately supervised;
- anybody wanting to make enquiries about handling personal information knows what to do;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are clearly described;
- methods of handling personal information are regularly assessed and evaluated;

and

- it disseminates to employees, information on good practice in respect of handling, using, and storing personal information.

Procedures/Methods

- All staff (employed and voluntary) must take appropriate technical and organisational security measures to safeguard personal information.
- Personal information must be protected from unauthorised or accidental disclosure.
- Staff are responsible for ensuring that the personal information which they use during their role is appropriately secured and any concerns regarding its security are brought to the attention of The Data Protection Lead. This includes ensuring that personal information is removed from desks out of hours and sensitive personal information is locked in filing cabinets or desks when not in use.
- The Data Protection Lead is responsible for ensuring that personal information when in use is only accessible by those with a need and right to access it to perform their function or role.
- Staff must respect the privacy of the subject of the personal information they are handling by treating personal information about others as we would expect information about ourselves to be treated.

- Careful consideration must be given to the transmitting of Personal Data. Personal data must not normally be transmitted **externally** via email. **Although it is acceptable to transmit personal data internally, you should consider choosing another method if possible.**
- Personal information must be disposed of safely and securely.
- Documents and any storage media containing input to and output from systems (paper or electronic) detailing personal information must be held, transported, and disposed of with due regard to its sensitivity.
- Where information is particularly sensitive it may be appropriate to ensure that the information is shredded on site.
- Publishing personal information on the Internet would make it available internationally therefore personal information must not be published on the internet, other than the names and work contact details of some employees and members if appropriate to their role.

Use of Images

An 'image' is personal data if the subject can be identified and therefore the Data Protection Act 2018 principles apply. Photographs, videos, and webcams of *clearly identifiable people* must not be processed for any other purpose other than that it was originally collected for. NG will get the permission for all use of photographic images and video footage by ensuring parents sign a consent form when a child or client is enrolled.

Images taken (including video) at an event attended by others, such as a sports event or assemblies are only to be used for personal viewing (or if taken by NG the purpose for which it is being collected) and the person in charge should address everyone to alert them to this and give them the opportunity to move away.

In the case of children, the purpose for which the images are to be used should be covered by a consent form, but if not a separate, signed parental consent form for each child will be obtained for that specific project.

Photographic/Video images used on a website will not include the child's first name in the accompanying text or photo caption. If a child is named in the text, a photograph will not be included unless specific parental consent has been given.

Photographs may be taken for security reasons to enable access to buildings for example and this is a legitimate business purpose for processing personal data.

Inappropriate and Unacceptable Use

Unacceptable use includes:

- unauthorised access of personal information
- unauthorised disclosure of personal information
- unauthorised use of personal information (e.g., not for reason given to access personal information)
- non-adherence to the organisation's information-sharing protocol
- unauthorised deletion

Naomi's Garden

Employee or customer personal information must not be used for:

- any illegal purpose;
- any purpose which is inappropriate in the workplace by virtue of the fact that it may cause embarrassment or distress to another person or may bring the organisation into disrepute;
- any purpose which is not in accordance with the staff member's role or job description.

This is not an exhaustive list. Cases where staff do not comply with this Policy or legislation will be dealt with under the Disciplinary Procedure and, depending on the circumstances; non-compliance may be deemed an act of gross misconduct.

Staff are required to notify an appropriate person, if they become aware, or suspect that personal information is being misused or handled inappropriately.

Subject Access

Staff have a right to access their own personal information. Requests by individuals for copies of their own information must be made in writing and supported by original proof of identity – copies are not acceptable (Passport, Driving Licence, Birth or Marriage certificate). Parents may request their child's information by giving proof of their own identity, and proof of parental responsibility e.g. birth certificate naming them as the parent. The decision on whether to release information in the event of a request will be that of The Data Protection Lead. Subject Access requests will be supplied within 15 days for children/clients and 30 days for staff. Where an investigation of a member of staff has commenced and Subject Access has been requested by them, the processing should be done as quickly as possible.

Complaints

In the event that a complaint is received regarding Subject Access complaints will be dealt with in accordance with the organisation's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Training

All staff will be trained on Data Protection on induction by using this policy and online training, and the Data Protection Lead will ensure staff are kept up to date with any changes in legislation.

General Statement

Naomi's Garden is committed to maintaining the above principles always. Therefore, will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely

- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft, and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

Data Breach Procedure

Important Note

This procedure has been produced based on current UK General Data Protection Regulations (UK GDPR) information. As further updates are released this procedure may be updated to reflect the changes.

Policy Statement

Naomi's Garden holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Naomi's Garden and all staff, trustees, volunteers, and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Naomi's Garden if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the Commissioner

1. In the case of a personal data breach, the Data Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The Data Controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Commissioner to verify compliance with this Article.

Types of Breach

Data protection breaches could be caused by several factors. Several examples are shown below:

- Loss or theft of client, child, staff, or governing body data and/ or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment Failure.
- Poor data destruction procedures.
- Human Error.
- Cyber-attack.
- Hacking.

Managing a Data Breach

In the event that NG identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform The Data Protection Lead or, in their absence, the administrator. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Data Protection Lead or nominated person must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The Data Protection Lead or nominated person must inform the Chair of Trustees as soon as possible. As a registered Data Controller, it is NG's responsibility to take the appropriate action and conduct any investigation.

4. The Data Protection Lead or nominated person must also consider whether the Police need to be informed. 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. In such instances, advice from the organisation's legal support should be obtained.

5. The Data Protection Lead or nominated person must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the relevant County Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately by The Data Protection Lead .

c. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately, and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Data Protection Lead to fully investigate the breach. The Data Protection Lead should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g., encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Data Protection Lead should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case-by-case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what NG is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see NG Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Data Protection Lead should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Trustees meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put correct these. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Data Protection Lead should ensure that staff are aware of NG Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision, and ongoing training. If staff have any queries in relation to the Data Protection policy and associated procedures, they should discuss this with the Data Protection Lead or the nominated person.

Review

This policy will be updated as necessary (at least once every two years) to reflect best practice in data management, security, and control to ensure compliance with any changes or amendments made to the Data Protection Act 2018.

Policy Adopted by Trustees on: 24.01.2022

Policy Last Reviewed on: 01.06.2023

Policy Due for Review on: 31.05.2024

Policy Review frequency: At least every two years

Information Commissioner's Office Registration/Notification/Renewal

Date of Registration/Notification with the Information Commissioner's Office: July 2020

Registration/Notification to be renewed annually:

Renewal dates:

08.07.2022 08.07.2023

Appendix I

ACTIONING A SUBJECT ACCESS REQUEST

1. Data subjects will be clearly informed of their right to access their personal data and to request that any errors or omissions be corrected swiftly.

   Such access shall be given and the correction of errors or omissions shall be made free of charge provided that such requests are reasonable and not trivial or vexatious.

   There is no prescribed format for making such requests provided that:

   the request is made in writing, signed & dated by the data subject (or their legal representative) to the chair of trustees.

   the data claimed to be in error or missing are clearly and unambiguously identified;

   the corrected or added data are clear and declared by the subject to be complete and accurate.

2. It will be explained to subjects who make a request to access their data and/or to have errors or omissions corrected, or that their data be erased, that, while their requests will be actioned as soon as is practical there may be delays where the appropriate volunteers or staff to deal with the request do not work on every normal weekday.

3. Where a data subject requests that their data be rectified or erased the Data Protection Lead will ensure that the rectifications or erasure will be applied to all copies of the subject's personal data including those copies which are in the hands of a Third Party for authorised data processing.

4. NG may make a charge for the provision of information, dependent upon the amount of pages being requested.

5. The Data Protection Act 2018 allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.

6. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or a school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40-day statutory timescale.

7. Any information which may cause serious harm to the physical or mental health or emotional condition of a child or client, or another should not be disclosed, nor should information that would reveal that the child/client is at risk of abuse, or information relating to court proceedings.

8. If there are concerns over the disclosure of information then additional advice should be sought.

9. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

Appendix I

10. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

Complaints

Complaints about the above procedures should be made to the Chair of Trustees who will decide whether it is appropriate for the complaint to be dealt with in accordance with the charity's complaint procedure.

Complaints which are not appropriate to be dealt with through the complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies /procedures, then please contact the Chair of Trustees.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.