Data Protection Policy

Contents

1. Scope

This policy applies to all Northridge Care Group employees. The policy does not apply to sub-contractors, external consultants, agency workers or anyone working for a third-party supplier.

This policy does not form part of your Contract of Employment.

2. Legislative Framework and Guidance

In order to operate effectively and fulfil our legal obligations, Northridge Care Group Ltd must collect, maintain and use certain personal information about current, past and prospective employees, young people, their families, suppliers and other individuals with whom we deal. All such personal information, whether held on computer, paper or other media, will be obtained, handled, processed, transported and stored lawfully and correctly, in accordance with the safeguards contained in the General Data Protection Regulations and Data Protection Act 2018.

Other Relevant Policies and Procedures

Employment Handbook
Employee Privacy Notice
Job Applicant Privacy Notice
Children and Young Persons Data Protection Policy
Children and Young People Privacy Notice
Internet, Email and IT usage policy
Equality and Diversity Policy
Safer Caring, Privacy and Confidentiality Policy
Safer Recruitment Policy
Safeguarding Policy
Social Media Policy

3. Definitions

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier.
"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership.
"Criminal offence data" is data which relates to an individual's criminal convictions and offences.
"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration,

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4. Principles

Northridge Care Group Ltd makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related policies.
Where third parties process data on behalf of the business, the business will ensure that the third party takes such measures in order to maintain the business' commitment to protecting data.
In line with GDPR, Northridge Care Group Ltd understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.
All personal data obtained and held by the business will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- kept accurate and up to date and every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant GDPR procedures for international transferring of personal data.

Northridge Care Group Ltd has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access.

- it appoints staff with specific responsibilities for:
    - the processing and controlling of data
    - the review and auditing of its data protection systems and procedures
    - the review of the effectiveness and integrity of data

- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way.

- it provides its employees with information and guidelines to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially.

- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with.

- it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the business.

- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. Northridge Care Group Ltd understands that consent must be freely given, specific, informed, and unambiguous. We will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time.

- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences.

In addition personal data will be processed in recognition of data protection rights as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

Types of data held

Personal data is kept in personnel files or within the business' HR system. The following types of data may be held by the business, as appropriate, on relevant individuals:

- name, address, phone numbers - for individual and next of kin
- CVs, Application Forms and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- Right to work documents which may include passports and/or birth certificates
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings.

- holiday records
- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details.

The business may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.
Relevant individuals should refer to Northridge Care Group Ltd's Employee Privacy Notice for more information on the reasons for our processing activities and the lawful bases we rely on for the processing and data retention periods.

5. Rights

The Right to be Informed

To keep you informed about how we use your data, we have a privacy notice for employees. The privacy notice is held in the 'document's section of the personnel management system.
A separate privacy notice is applicable to job applicants this is available from Human Resources.
Our privacy notices set out:

a) the types of data we hold and the reason for processing the data;
b) our legitimate interest for processing it;
c) details of who your data is disclosed to and why, including transfers to other countries. Where data is transferred to other counties, the safeguards used to keep your data secure are explained;
d) how long we keep your data for, or how we determine how long to keep your data for;
e) where your data comes from;
f) your rights as a data subject;

g) your absolute right to withdraw consent for processing data where consent has been provided and no other lawful reason for processing your data applies;
h) your right to make a complaint to the Information Commissioner if you think your rights have been breached;
i) whether we use automated decision making and if so, how the decisions are made, what this means for you and what could happen as a result of the process.
j) the name and contact details of our data protection officer.

The Right of Access

Relevant individuals have a right to be informed if the business processes personal data relating to them and to access the data that the business holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- requests for a subject access request should be made to the Data Protection Officer.
- the business will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- the business will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform the business immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The business will take immediate steps to rectify the information.
For further information on making a subject access request, employees should refer to the Data Protection Officer.

The Right to Correction

If you discover that the data we hold about you is incorrect or incomplete, you have the right to have the data corrected. If you wish to have your data corrected, you should complete the Data Correction Form.
Usually, we will comply with a request to rectify data within one month unless the request is particularly complex in which case we may write to you to inform you we require an extension to the normal timescale. The maximum extension period is two months.
You will be informed if we decide not to take any action because of the request. In these circumstances, you can complain to the Information Commissioner and have access to a judicial remedy.
Third parties to whom the data was disclosed will be informed of the rectification.

The Right of Rectification

In certain circumstances, we are required to delete the data we hold on you. Those circumstances are:

a) where it is no longer necessary for us to keep the data;
b) where we relied on your consent to process the data and you subsequently withdraw that consent. Where this happens, we will consider whether another legal basis applies to our continued use of your data;
c) where you object to the processing (see below) and the business has no overriding legitimate interest to continue the processing;
d) where we have unlawfully processed your data;
e) where we are required by law to erase the data.

If you wish to make a request for data deletion, you should complete the Data Erasure form.
We will consider each request individually, however, you must be aware that processing may continue under one of the permissible reasons. Where this happens, you will be informed of the continued use of your data and the reason for this.
Third parties to whom the data was disclosed will be informed of the erasure where possible unless to do so will cause a disproportionate effect on us.

The Right of Restriction

You have the right to restrict the processing of your data in certain circumstances.
We will be required to restrict the processing of your personal data in the following circumstances:

a) where you tell us that the data we hold on you is not accurate. Where this is the case, we will stop processing the data until we have taken steps to ensure that the data is accurate;
b) where the data is processed for the performance of a public interest task or because of our legitimate interests and you have objected to the processing of data. In these circumstances, the processing may be restricted whilst we consider whether our legitimate interests mean it is appropriate to continue to process it;
c) when the data has been processed unlawfully;
d) where we no longer need to process the data but you need the data in relation to a legal claim.

If you wish to make a request for data restriction, you should complete the Data Restriction form.
Where data processing is restricted, we will continue to hold the data but will not process it unless you consent to the processing or processing is required in relation to a legal claim.
Where the data to be restricted has been shared with third parties, we will inform those third parties of the restriction where possible unless to do so will cause a disproportionate effect on us.
You will be informed before any restriction is lifted.

The Right to Data Portability

You have the right to obtain the data that we process on you and transfer it to another party. Where our technology permits, we will transfer the data directly to the other party.
Data which may be transferred is data which:

a) you have provided to us; and
b) is processed because you have provided your consent or because it is needed to perform the employment contract between us; and
c) is processed by automated means.

If you wish to exercise this right, please speak to your manager.
We will respond to a portability request without undue delay, and within one month at the latest unless the request is complex, or we receive a number of requests in which case we may write to you to inform you that we require an extension and reasons for this. The maximum extension period is two months.
We will not charge you for access to your data for this purpose.
You will be informed if we decide not to take any action because of the request, for example, because the data you wish to transfer does not meet the above criteria. In these circumstances, you can complain to the Information Commissioner and have access to a judicial remedy.
The right to data portability relates only to data defined as above. You should be aware that this differs from the data which is accessible via a Subject Access Request.

The Right to Object

You have a right to require us to stop processing your data; this is known as data objection.
You may object to processing where it is carried out:

a) in relation to the business' legitimate interests;
b) for the performance of a task in the public interest;
c) in the exercise of official authority; or
d) for profiling purposes.

If you wish to object, you should do so by completing the Data Objection Form.
In some circumstances we will continue to process the data you have objected to. This may occur when:

a) we can demonstrate compelling legitimate reasons for the processing which are believed to be more important than your rights; or
b) the processing is required in relation to legal claims made by, or against, us.
c) If the response to your request is that we will take no action, you will be informed of the reasons.

6. International Data Transfers

Northridge Care Group Ltd does not transfer personal data to any recipients outside of the EEA except in occasional and limited circumstances when employees whose data is transferred will be informed. Where this occurs, the business will

make every effort to ensure data is processed according to the business' own standards.

7. Breach notification

All staff must report any suspected or actual data breach immediately to the Registered Manager and Data Protection Lead. A breach includes unauthorised access, accidental disclosure, loss, or destruction of personal data.

The Data Protection Lead will:

1. Contain and assess the breach.
2. Determine the risk to the child's rights and freedoms.
3. Report the breach to the Information Commissioner's Office (ICO) within 72 hours if necessary.
4. Notify the affected individual(s), local authority, and Ofsted where required.
5. Record all incidents and outcomes in the data breach log.

If the breach is sufficient to warrant notification to the public, the business will do so without undue delay.

8. Data Processing Records

Northridge Care Group Ltd keeps records of its processing activities including the purpose for the processing and retention periods. These records will be kept up to date so that they reflect current processing activities.

9. Employees' Responsibility

Northridge Care Group Ltd adopts procedures designed to maintain the security of data when it is stored and transported.
Whenever and wherever you are processing personal data for the business you must keep this secret, confidential and secure, and you must take particular care not to disclose such data to any other person (whether inside or outside the business) unless authorised to do so. Do not use any such personal data except as authorised by us for the purposes of your job. If in doubt, ask a member of management.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by a senior manager. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system – a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

You must ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people. You must use computer screen blanking to ensure that personal data is not left on screen when not in use.

You must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

The Act gives every individual the right to see all the information which any data controller holds about them. Bear this in mind when recording personal opinions about someone, whether in an e-mail or otherwise. It is another reason why personal remarks and opinions made should be given responsibly, must be relevant and appropriate as well as accurate and justifiable.

For your information, the Act provides that it is a criminal offence to obtain or disclose personal data without the consent of the data controller. "Obtaining" here includes the gathering of personal data by employees at work without the authorisation of the employer. You may be committing this offence if without authority of the business: you exceed your authority in collecting personal data; you access personal data held by us; or you pass them on to someone else (whether inside or outside the business).

Failure to follow Northridge Care Group Ltd's rules on data security may be dealt with via the disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

10. Communication Monitoring

Northridge Care Group Ltd is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy. The Company may monitor your business communications for reasons which include:

- providing evidence of business transactions;
- ensuring that our business procedures, policies and contracts with staff are adhered to;
- complying with any legal obligations;
- monitoring standards of service, staff performance, and for staff training;
- preventing or detecting unauthorised use of our communications systems or criminal activities; and
- maintaining the effective operation of business communication systems.

From time to time the business may monitor telephone, e-mail and internet traffic data (i.e. sender, receiver, subject; non-business attachments to e-mail,

numbers called and duration of calls; domain names of web sites visited, duration of visits, and non-business files downloaded from the internet) at a network level (but covering both personal and business communications). This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

Sometimes it is necessary for us to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday.

11. Equality and Diversity

This Policy will always be carried out in accordance with our Policy on Equality & Diversity.

12. Monitoring and Reporting

This policy will be reviewed regularly to ensure compliance with applicable legislative changes, changes within the organisation and best practice.

13. Revision History

Version	Date	By whom
Version 1.0	July 2020	Vicky Wilden
Version 1.1	July 2021	Vicky Wilden
Version 1.2	October 2022	Vicky Wilden
Version 1.3	23rd August 2023	Vicky Wilden
Version 1.4	September 2024	Kerry McKevitt
Version 1.5	November 2025	Kendal Hulme