Bewbush Community Nursery CIC

Data Protection Policy

Author: Bewbush Community Nursery CIC,
Commencement: June 2019
Review Due: June 2022

Table of Contents

Version Control

Version	Amendment	Date	Author
1.0	First Issue	June 2019	CaPS Ltd

Introduction

Organisation

In order for Bewbush Community Nursery CIC (the Company) to provide commercial services, it needs to gather and use personally identifiable information (PII) about individuals. These can include parents, children, suppliers, business contacts, employees, job applicants and other people the organisation has a relationship with or may need to contact. The Company has determined that it is a Data Controller as defined under the General Data Protection Regulations. Additionally, the Company processes personal data provided by its clients in relation to servicing those contracts.

The Company has produced this Data Protection Policy to ensure that the organisation:

- Complies to all applicable laws and regulations and contractual obligations.
- Adheres to any and all Data Processing Agreements required to be put in place
- Implements organisational and technical data protection practices that considers information security requirements following the results of applicable risk assessments.
- Instruct all employees and associates in the needs and responsibilities of Data Protection.
- Implement continual improvement initiatives, including risk assessment and risk treatment strategies, while making best use of its management resources to better meet Information Security requirements.

Policy scope

This policy applies to:

- The corporate functions of Bewbush Community Nursery CIC
- All staff of Bewbush Community Nursery CIC
- All contractors, suppliers and other people working on behalf of Bewbush Community Nursery CIC

It applies to all data that the company holds relating to natural living persons. The definition of PII is:

"Any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person." Note, this is not an exhaustive list.

Policy Operational Date and Review

This policy is effective from 20th June 2019 and remains in force until revoked. It will be reviewed every 3 years but may be amended before should a need be identified.

Policy Preparation

This policy has been prepared with support from the Company's Data Protection advisor.

Policy Approval

This policy has the authority and approval at Board level.

Purpose of Policy

The purpose of this policy is to ensure that the Company complies with UK Data Protection law (GDPR/ Data Protection Act 2018), upholds the principles of the GDPR, honours Data Subject Rights and is transparent about how it processes individuals' data. In addition, it will ensure the Company follows good practice, protects the data of clients, the data it processes on behalf of its clients, customers, staff, contractors of the company as well as protecting its reputation, particularly in relation to data breaches.

The Company recognises that as far as possible, personal data needs to be shared across the organisation so that the business can operate in the most efficient and effective way. In establishing this 'need to share' position, it is extremely important that data sharing is conducted in accordance with the Regulations.

Data Types

Data processed by the Company comprises, but is not limited to, data relating to personal identity, contact details, employment requirements, training, the delivery of contracted services and marketing. The Company does process some special category data, namely health, religion and ethnicity. We do not protectively mark documents and systems. Therefore, you should assume information is confidential unless you are sure it is not and act accordingly.

Policy Statement

The General Data Protection Regulations (GDR) (EU directive 2016/679) describes how organisations — including Bewbush Community Nursery CIC can lawfully collect, process and store personally Identifiable information (PII). These rules apply regardless of whether data is stored electronically, on paper or on other materials.

The GDPR is underpinned by six important principles. These say that PII must be:

1. Processed lawfully, fairly, and in a transparent way in relation to individuals
2. Collected for specific, explicit, and authentic purposes
3. Adequate, relevant, and limited to what is needed
4. Accurate and kept up to date
5. Retained only for as long as necessary
6. Processed in an appropriate way to maintain security

In addition, the law states that the Data Controller (Bewbush Community Nursery CIC) shall be responsible for, and be able to demonstrate, compliance with the principles.

The Company is committed to comply with both the law and good practice. The Company will be open and honest with individuals whose data it processes and will provide training and support to staff so that they can act confidently and consistently. The company will honour data subjects' rights and support those organisations we undertake data processing for, to do the same.

The Company has developed a data breach procedure which is designed to facilitate a fast response to data security incidents as well as developing an ability to learn from such occurrences in order to mitigate the potential for a repeat occurrence.

Data protection risks

This policy mitigates the risk to Bewbush Community Nursery CIC from data security risks, including:

- Data Breaches; for instance, PII being given out inappropriately, loss of data, not having data backup.
- Failing to uphold the rights of data subjects and not responding appropriately to lawful requests.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data or if the company were publicly sanctioned by the Information Commissioners Office.

Responsibilities

The Board/ Company Directors

Everyone who works for or with Bewbush Community Nursery CIC has responsibility for ensuring data is collected, stored and handled appropriately in accordance with the data protection law. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:

The board of directors is ultimately responsible for ensuring that the Company meets its legal obligations.

The Board is responsible for:

- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Handling data protection questions received from external sources.
- Monitoring requests from individuals in relation to subject access rights
- Monitoring Data Breach reporting and remediation.

The HR Manager is responsible for:

- Background verification checks on all candidates for employment in accordance with relevant laws regulations and ethics. These checks will be proportionate to the business requirements
- Arranging data protection training and advice for the people covered by this policy.
- The security of data
- The accuracy of personnel records
- Reviewing retention periods
- Creating and maintaining data disposal policies
- Ensuring accessibility of data
- Receiving, acknowledging and coordinating the response to data protection questions from staff covered by this policy
- Receiving, acknowledging and coordinating the responses to Subject Rights requests from any source
- Maintaining records of processing and data maps

The Finance Manager is responsible for:

- Supplier compliance
- The security of data
- The accuracy of financial records containing personal data
- Reviewing retention periods
- Creating and maintaining data disposal policies
- Ensuring accessibility of data

The Head of IT is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services that the company is considering using to store or process data. For instance, cloud computing services.
- Providing sufficient redundancy of systems to enable disaster recovery and business continuity
- Ensuring the backup of data occurs and testing of restore protocols
- Ensuring appropriate authorisations are in place in relation to the access of personal data
- Establishing and maintaining authentication onto the Company's systems
- Physical security in relation to servers, CCTV recording equipment and infrastructure.
- The serviceability of electronic access controls and the availability of entry/ exit records

- The encryption of CCTV image transmission
- Appropriate security in the transmission of sensitive or high risk personal data.

General staff guidelines

The only people able to access data covered by this policy, should be those who need it for their work, data should not be shared informally without reason.

The following things (among others) are, in general, prohibited on company systems and while carrying out your duties for the company and may result in disciplinary action:

- Anything that contradicts our equality and diversity policy, including harassment.
- Circumventing user authentication or security of any system, network or account.
- Downloading or installing pirated software.
- Disclosure of confidential information at any time.

Bewbush Community Nursery CIC will provide awareness training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below. In particular, strong passwords must be used and they must never be shared.

Personal data must not be disclosed to unauthorised people, either within the company or externally. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of. Employees should request help from their line manager if they are unsure about any aspect of data protection.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

When not required, the paper or files should be kept in a locked drawer or filing cabinet. Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer. Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. This includes ensuring that access control is in place at an administrative level to ensure access to personally identifiable information is restricted to those authorised to access it. In addition, authentication onto the various hosted systems will be organised and administered at the enterprise level by use of controls such as Active Directory.

Social Media and Blogging Policies

The use of apps such as LinkedIn, Facebook, Twitter and Instagram, are permitted for marketing and business development purposes but should only be used to promote business information, news and tips. When using social media, employees and associates should make it clear that any views being expressed are their own and not on behalf of the company.

Users also have a responsibility to ensure Bewbush Community Nursery CIC's data is securely maintained and is available for backup. Users will ensure documents and files are saved to the appropriate area of the company's servers. These shared drives will have access controls, governed by permissions to ensure against unauthorised disclosure. This procedure allows for the backup of data at the system level.

Users must not use personal / local drives to store data except in the circumstances set out below. If the Bewbush Community Nursery CIC network becomes unavailable for whatever reason and data or work is at risk of being lost, users will have no option but to save the data (files) locally (i.e. on the computer being used) or on approved and encrypted media storage such as a data stick (USB storage). Once the Corporate Network becomes available again, data (files) should be immediately transferred to the Corporate network in order for it to be backed up safely and local copies of data on the computer or portable storage media should be deleted. This will help to ensure the availability and integrity of data and to avoid duplicate copies of data being stored.

Policy Breaches

Breaches of this policy and/ or security incidents can be defined as events which could have, or have resulted in, loss or damage to Bewbush Community Nursery CIC's assets, or an event which is in breach of Bewbush Community Nursery CIC's security procedures and policies. All employees, associates, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible to the Compliance department. This obligation also extends to any external organisation contracted to support or access the Information Systems of Bewbush Community Nursery CIC. Bewbush Community Nursery CIC will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place.

Security

Security Measures

All data requires protection from accidental or unauthorised disclosure. Bewbush Community Nursery CIC processes data of parents, children and staff, some of which is special category (sensitive). Any breach has the potential to cause reputational damage both to the data subjects and the company. It is for this reason that security of data is considered extremely important to the company.

Passwords

Bewbush Community Nursery CIC controls logical access to its technology infrastructure through password based authentication. Bewbush Community Nursery CIC shall ensure development and implementation of appropriate password controls to protect all business data, related application systems and operating systems software from unauthorized or illegal access. The password controls shall be automated using system features and parameters wherever feasible.

- The minimum length of the password shall be 8.
- Password shall be combination of alpha, numeric and special characters.
- Password shall not be the same as the user name or user id.
- Users shall be forced to change the initial password set by System Administrator on the first successful logon into the system.
- Every employee of Bewbush Community Nursery CIC. shall follow the best practices and guidelines with respect to password security.

Passwords should never be shared among employees. If data is stored on removable media these should be kept locked away securely when not being used.

Clear Desks and Screens

Personally Identifiable Information is of no value to Bewbush Community Nursery CIC unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. When working with personal data, employees should ensure the screens of their computers are always locked when left unattended. Desks and working surfaces should be left clear of personal data when left unattended. These measures are particularly important to peripatetic workers when using communal spaces or working from home.

Malicious Code (Ransomware)

Bewbush Community Nursery CIC will provide a number of security layers to prevent malicious code entering the company network. This includes the application of firewalls, antivirus, email security, back up and disaster recovery. However, all users of internet enabled computing equipment must be aware of malicious attempts to bypass the company's security regime by using tactics such as Phishing (email) or Vishing (phone) in order to obtain personal data or covert access to computer systems. All suspicious emails must not be opened but reported to the IT Department.

Additionally, users shall not be allowed to:

- Download executable and media files.
- Access restricted sites (Profane/ Obscene sites).

Removable Media

Personal data should only be copied to removable media if data sticks and other portable devices have been encrypted.

Data Sharing

Personal data should not be shared informally as all records of personal data are disclosable to the data subject. Personal data which is highly sensitive or presents a risk to the data subject if disclosed, should be sent by encrypted email.

Personal data should never be transferred outside of the European Economic Area or EU approved third countries without the appropriate consents, lawful basis or approved controls in place.

Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Recording and Storage

Data Accuracy

The law requires the Company to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Bewbush Community Nursery CIC should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data will be held in a few places as necessary. Staff should not create any unnecessary additional data sets. Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

Updating

Bewbush Community Nursery CIC will make every effort to ensure data subjects personal information is up to date. Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database. Data subjects will be asked to confirm their details during routine interactions with members of the team.

A full data refresh exercise will be undertaken on a 12-month basis.

Storage

Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services. Servers containing personal data should be sited in a secure location, away from general office space.

Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures. Data should only be downloaded to laptops or other mobile devices if those devices have sufficient end point security applied and data

accuracy is ensured by uploading updated personally identifiable data to organisations physical servers or appropriate cloud host, from which, data backups are made.

Retention Periods

Data be retained in accordance with either a legal obligation or company policy. PII collected for the purpose of employing staff will be held for a maximum of 6 years. PII required for the purposes of administrating payroll or financial transactions will be retained for 7 years. Client contact data will be held during the contracted period and further in order to pursue the legitimate interests of the organisation. All data will be deleted once the legitimate purpose has been fulfilled. The Company has developed and continues to monitor a detailed data retention policy which provides greater detailed information.

Archiving

Data will be destroyed after the retention period has been reached. Computer files will be deleted from all directories and backup files and hard copy material will be securely shredded.

Right of Access

Subject Access Requests

Individuals whose Personally Identifiable Information the Company process and is the Data Controller for, will have the right to obtain:

- Confirmation that their data is being processed
- Access to their Personal Data
- Other supplementary information - this largely corresponds to the information that is provided in our privacy notice (see Article 15 GDPR)

This information must be provided within one month, unless the request is unusually complex or there are multiple requests, in which case, the time limit can be extended to two months. There is no fee chargeable for exercising this right.

It is important that the identity of the person requesting the data is verified before responding in full to the request. All data contain that subject's personal data must be made available to the Compliance department who will decide what needs redaction or can be lawfully withheld. Data should be made available in a commonly used format if requested electronically.

Bewbush Community Nursery CIC has produced a Subject Access Request procedure to facilitate data subject rights.

Transparency

Commitment

Bewbush Community Nursery CIC. commits to ensuring that data subjects are aware that their data is being processed, who it is being shared with, how long it will retain it and how we will keep it secure. In addition, we will ensure that data subjects know how to exercise

their rights. The prime vehicle for ensuring our commitment is the publication of a privacy notice on the company web site. This privacy notice will be reviewed annually but may be amended sooner should a need be identified.

Procedure

Members of staff will be made aware of our commitment through the onboarding process.

Disclosing data for other reasons

In certain circumstances, Personally Identifiable Information can to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Bewbush Community Nursery CIC will disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Lawful Basis

Underlying Principles

The GDPR requires that all data processing is conducted within a lawful basis. There are six lawful basis, they are:

- Consent of the data subject
- In pursuance of a contract
- Legal obligation
- In the vital interest of the data subject
- In the public interest, or
- In the legitimate interest of the organisation.

Bewbush Community Nursery CIC has identified its lawful basis for processing and recorded that within its record of processing.

International Transfers

Bewbush Community Nursery CIC does not transfer data internationally.

Opting out

Bewbush Community Nursery CIC does not offer an opt out opt in relation to data processing unless it is being processed on a consent basis.

Withdrawing Consent

Each data subject category and data type have a lawful purpose identified within the company Data Inventory. Wherever consent is used as a lawful basis, we acknowledge that consent can be withdrawn and that all processing of that data must cease.

Employee Training and Acceptance of Responsibilities

Induction

All employees who have access to any kind of personal data will have basic data protection awareness training delivered to them during their induction into the organisation.

Continued Training

Refresher training will be made compulsory and delivered annually.

Staff Acceptance

Staff members will be required to read this policy upon receipt and will be deemed as having accepted their responsibilities in relation to Data Privacy.