



Data Security Policy including Biometric Data

Reviewed: July 2023

To be reviewed: July 2024

Caring

Respect

Nurture

Encourage

Growth

Equality

Company Reg.No. 08812259

Registered Office: Brooke Road, Walthamstow, London E17 9HJ

Charity Reg. No:1157645

Contents:

Statement of intent

1. Legal framework
2. Types of security breach and causes
3. Roles and responsibilities
4. Secure configuration
5. Network security
6. Malware prevention
7. User privileges
8. Monitoring usage
9. Removable media controls and home working
10. Backing-up data
11. User training and awareness
12. Protection of Biometric information

Statement of intent

Little Learners Nursery is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the nursery are only accessible by the appropriate individuals. It is therefore important to uphold high standards of security, take suitable precautions, and to have systems and procedures in place that support this.

Little Learners Nursery recognises, however, that breaches in security can occur, particularly as the majority of information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan containing procedures to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

For the purposes of this policy, the title of 'data controller' will be used in reference to the person(s) primarily responsible for the handling and protection of information and data within a nursery.

1. Legal framework

1.1. This policy has due regard to statutory legislation and regulations including, but not limited to, the following:

- The General Data Protection Regulation 2018
- The Computer Misuse Act 1990

1.2. This policy has due regard to the nurseries policies and procedures including, but not limited to, the following:

- Online Safety Policy
- Data Protection Policy
- Acceptable Use Policy
- Cloud Computing Policy

2. Types of security breach and causes

2.1. Unauthorised use without damage to data – involves unauthorised persons accessing data on the nursery system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.

2.2. Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.

2.3. Damage to physical systems – involves damage to the hardware in the nurseries ICT system, which may result in data being inaccessible to the nursery and/or becoming accessible to unauthorised persons.

2.4. Unauthorised damage to data – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Caring

Respect

Nurture

Encourage

Growth

Equality

2.5. Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

- Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.
- Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the nursery through accessing and altering, sharing or removing data.
- Negligence, e.g. as a result of an employee that is aware of nursery policies and procedures, but disregards these.

2.6. Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the nursery software is more vulnerable to a virus
- Incorrect firewall settings are applied, e.g. access to the nursery network, meaning individuals other than those required could access the system
- Confusion between backup copies of data, meaning the most recent data could be overwritten

3. Roles and responsibilities

3.1. The principal is responsible for implementing effective strategies for the management of risks posed by internet use, and to keep its network services, data and users secure.

3.2. The data controller is responsible for the overall monitoring and management of data security.

3.3. The principal is responsible for establishing a procedure for managing and logging incidents.

Caring

Respect

Nurture

Encourage

Growth

Equality

3.4. The director is responsible for holding regular meetings with the principal and data controller to discuss the effectiveness of data security, and to review incident logs.

3.5. All members of staff and pupils are responsible for adhering to the processes outlined in this policy, alongside the nurseries E-Safety Policy and Acceptable Use Policy.

4. Secure configuration

4.1. An inventory will be kept of all IT hardware and software currently in use at the nursery, including mobile phones and other personal devices provided by the nursery. This will be stored in the nursery office and will be audited on a termly basis to ensure it is up-to-date.

4.2. Any changes to the IT hardware or software will be documented using the inventory, and will be authorised by the data controller before use.

4.3. All systems will be audited on a termly basis to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded on the inventory.

4.4. Any software that is out-of-date or reaches its 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products such that any security issues will not be rectified.

4.5. All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed on a termly basis to prevent access to facilities which could compromise network security.

4.6. The nursery believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users.

5. Network security

5.1. The nursery will employ firewalls in order to prevent unauthorised access to the systems.

5.2. The nurseries firewall will be deployed as a:

- Localised deployment: the broadband service connects to a firewall that is located on an appliance or system on the nursery premises, as either discrete technology or a component of another system.

5.3. As the nursery's firewall is managed on the premises, it is the responsibility of the data controller to effectively manage the firewall. The data controller will ensure that:

- The firewall is automatically updated.
- Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.
- Any compromise of security through the firewall is reported to the principal. The data controller will react to security threats to find new ways of managing the firewall.

6. Malware prevention

6.1. Little Learners Nursery understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

6.2. The data controller will ensure that all nursery devices have secure malware protection and undergo regular malware scans.

6.3. The data controller will update malware protection on a termly basis to ensure it is up-to-date and can react to changing threats.

6.4. Malware protection will also be updated in the event of any attacks to the nursery's hardware and software.

6.5. Filtering of websites, as detailed in section 7 of this policy, will ensure that access to websites with known malware is blocked immediately and reported to the data controller.

6.6. The nursery will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users.

6.7. The data controller will review the mail security technology on a termly basis to ensure it is kept up-to-date and effective.

7. User privileges

7.1. Little Learners Nursery understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.

7.2. The principal will clearly define what users have access to and will communicate this to the data controller, ensuring that a written record is kept.

7.3. The data controller will ensure that user accounts are set up to allow users access to the facilities required, in line with the principal's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

7.4. The data controller will ensure that websites are filtered for inappropriate and malicious content. Any member of staff that has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process in section 12 of this policy.

7.5. All users will be required to change their passwords regularly and must use upper and lowercase letters, as well as numbers, to ensure that passwords are strong. Users will also be required to change their password if they become known to other individuals.

7.6. Staff are responsible for remembering their passwords; however, the data controller will have an up-to-date record of all usernames and passwords, and will be able to reset them if necessary.

7.7. Children do not have access to the network

7.8. The 'master user' password used by the data controller will be made available to the principal, or any other nominated senior leader, and will be kept in the nursery office.

7.9. A multi-user account will be created for visitors to the nursery, such as volunteers and students, and access will be filtered as per the principal's instructions. Usernames and passwords for this account will be changed on a termly basis, and will be provided as required.

7.10. Automated user provisioning systems will be employed in order to automatically delete inactive users or users who have left the nursery. The data controller will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

7.11. The data controller will review the system on a termly basis to ensure the system is working at the required level.

8. Monitoring usage

8.1. Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.

8.2. The nursery will inform all staff that their usage will be monitored, in accordance with the nurseries Acceptable Use Policy and Online Safety Policy.

8.3. If a user accesses inappropriate content or a threat is detected, an alert will be sent to the data controller. Alerts will also be sent for unauthorised and accidental usage.

8.4. Alerts will identify: the user, the activity that prompted the alert and the information or service the user was attempting to access.

8.5. The data controller will record any alerts using an incident log and will report this to the principal. All incidents will be responded to in accordance with section 12 of this policy, and as outlined in the Online Safety Policy.

8.6. All data gathered by monitoring usage will be kept in a filing cabinet in the nursery office for easy access when required. This data may be used as a method of evidence for supporting a not yet discovered breach of network security. In addition, the data may be used to ensure the nursery is protected and all software is up-to-date.

9. Removable media controls and home working

9.1. Little Learners Nursery understands that staff may need to access the nursery network from areas other than on the premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

9.2. The data controller will encrypt all nursery-owned devices for personal use, such as laptops, USB sticks, mobile phones and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

9.3. Staff are not permitted to use their personal devices where the nursery shall provide alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the principal.

9.4. If staff are instructed that they are able to use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the nursery's network security. This will be checked by the data controller.

9.5. When using laptops, tablets and other portable devices, the principal will determine the limitations for access to the network, as described in section 5 of this policy.

9.6. Staff who use nursery-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off nursery premises.

9.7. The data controller will use encryption to filter the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises.

9.8. The nursery uses tracking technology where possible to ensure that lost or stolen devices can be retrieved.

9.9. All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

9.10. The Wi-Fi network at the nursery will be password protected and will only be given out as required. Staff are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise by the principal.

9.11. A separate Wi-Fi network will be established for visitors at the nursery to limit their access to printers, shared storage areas and any other applications which are not necessary.

10. Backing-up data

10.1. The data controller performs a back-up of all electronic data held by the nursery on a regular basis, and the date of the back-up is recorded using a log. Each back-up is retained for three months before being deleted.

10.2. The data controller performs an incremental back-up on a monthly basis of any data that has changed since the previous back-up. The data controller will record the date of any incremental back-up, alongside a list of the files that have been included in the back-up.

10.3. Where possible, back-ups are run overnight and are completed before the beginning of the next nursery day.

10.4. Upon completion of back-ups, data is stored on the nursery's hardware which is password protected.

10.5. Data is also replicated and stored in accordance with the nursery's Cloud Computing Policy.

10.6. Only authorised personnel are able to access the nursery's data.

11. User training and awareness

11.1. The principal will arrange training for pupils and staff to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Use Policy and Online Safety Policy.

11.2. Training for all staff members will be arranged by the data controller following an attack or significant update.

11.3. Through training, all pupils and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords.

11.4. All staff will receive training as part of their induction programme.

11.5. All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Online Safety Policy.

12. Protection of Biometric information for children at Little Learners Nursery

12.1 Legal Framework - Protection of Freedoms Act 2012 – Data Protection Act 2018 – GDPR - DfE guidance Protection of biometric information of children in nurseries and colleges

12.2 At Little Learners Nursery the written consent of at least one parent must be obtained before the biometric data is taken from the child and used. This applies to all children in nurseries.

12.3 In no circumstances can a child's biometric data be processed without written consent.

12.4 Little Learners Nursery will not process the biometric data of child where:

- a) the child (whether verbally or nonverbally) objects or refuses to participate in the processing of their biometric data;
- b) no parent has consented in writing to the processing; or
- c) a parent has objected in writing to such processing, even if another parent has given written consent.

12.5 Little Learners Nursery will, where possible, provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

12.6 Little Learners Nursery refers to the latest guidance published by the DfE for the implementation of policy

<https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-nursery>