Data Protection Policy (including Data Breach Procedure and Data Retention Checklist)

Data Protection Officer (DPO): Briony Sedgeman, Senior Deputy Manager

General Data Protection Regulation GDPR

The General Data Protection Regulation (GDPR) came into effect on 25 May 2018, it replaced the Data Protection Act 1998. The GDPR is designed to strengthen and unify the safety and security of all data held on individuals.

Data Protection Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals.
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.
e) Kept in a clear, easily understood format which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data is processed.
f) 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.

Article 5(2) requires that: "the controller (Oasis Childcare Centres) shall be responsible for, and be able to demonstrate, compliance with the principles". (Please see Data Protection File).

Purpose of Policy

To implement procedures to ensure that information is stored or processed in accordance with the General Data Protection Regulation (GDPR). Oasis Childcare Centres are committed to following the data protection principles to ensure that personal information about children, parents/carers, staff, committee, students, volunteers and other relevant

professionals/contractors are as secure as possible at all times. This means that Oasis Childcare Centres will:

- Only collect personal information that is relevant to/required for the effective running of the settings. We will inform you of how we intend to use the information when we collect it.
- Inform you when information needs to be shared with third parties, explaining why, with whom and under what circumstance. The only exception would be in the event of a safeguarding concern or lawful obligation.
- Regularly check the quality and accuracy of the information we hold.
- Ensure that information is not held longer than necessary. Please see Data Retention Policy.
- Ensure that when information is authorised for disposal it is disposed of appropriately.
- Ensure appropriate security measures to safeguard personal information, both in paper form and electronically stored on the settings computers/cloud storage.
- Share personal information with others when it is necessary and legally appropriate to do so.
- Set out clear procedures for responding to requests for access to personal information known as 'subject access'.
- Regularly review policies and procedures with staff to support their knowledge and understanding.

We will always follow the guidance of the Information Commissioner's Office (ICO) to ensure our procedures comply with the requirements of the GDPR.

Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on GDPR and the ICO's Code of Practice for Subject Access Requests. It also reflects the ICO's code of practice for the use of CCTV surveillance cameras and personal information.

Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Date of Birth • Address • Telephone number • Bank details • Identification number

	It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and, therefore, requires higher levels of protection. This includes information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingertips, retina and iris patterns), where used for identification purposes • Health - physical or mental • Sexual orientation
Processing	Anything done with personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The Data Controller

Oasis Childcare Centres process personal data relating to children, parents, staff, committee members, students, volunteers, visitors and other relevant professionals, and therefore is a data controller. The setting is registered as a data controller with the ICO and will renew this registration annually or as otherwise required by law.

Roles and Responsibilities

Data Protection Officer (DPO): Briony Sedgeman, Senior Deputy Manager

All staff members are responsible for ensuring that personal information about children, parents/carers, colleagues, committee members and other relevant professionals is not shared with individuals outside the setting (please also see Confidentiality Policy). The DPO is responsible for ensuring that all personal information is kept safe and secure and in compliance with the GDPR. The DPO is also responsible for responding to any suspected and/or confirmed data breaches (please see Data Breach Procedure).

Collecting Personal Data

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to individuals when we first collect their data. If personal data is required for reasons other than those given when we first obtained the data, we will inform the individuals concerned prior to using their information and seek consent where necessary.

Lawful Bases for Processing

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply when processing personal information:

a) **Consent:** an individual has given clear consent for an organisation to process their personal data for a specific purpose.
b) **Contract:** the processing is necessary for a contract between an individual and an organisation, or because an organisation has asked an individual to take specific steps before entering into a contract.
c) **Legal Obligation:** the processing is necessary for an organisation to comply with the law (not including contractual obligations).
d) **Vital Interests:** the processing is necessary to protect someone's life.
e) **Public Task:** the processing is necessary for an organisation to perform a task in the public interest or for the organisations official functions, and the task or function has a clear basis in law.
f) **Legitimate Interests:** the processing is necessary for the organisations legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply to public authorities processing data to perform an official task).

Please see Data Inventory in Data Protection File, which is stored securely in the main office.

Data Storage and Access

At Oasis Childcare Centres we are committed to protecting personal data and keeping it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. We collect and process personal data on children, parents, staff, committee members, students, volunteers, visitors and other relevant professionals, which includes (but is not exclusive to):

- Children's details such as name, address, date of birth, birth certificate/passport reference number, medical/allergy information, name of health visitor and any other professionals involved with the child,
- Parents/carers details such as name, address, date of birth, telephone number, email address, national insurance number, bank details. We also include on registration forms the name of parent/parents with parental responsibility and name of person with whom the child resides.
- Emergency contact details – telephone numbers of children's family members or family friends to contact in the event of an emergency if unable to contact parents.
- Staff information such as name, date of birth, address, telephone numbers, email address, bank details, national insurance number, qualifications, medical/allergy information, emergency contact details, DBS information (please see Policy for Secure Storage, Handling, Use, Retention and Disposal of Disclosures and Disclosure Information).
- Committee members such as name, date of birth, address, telephone numbers, email address, DBS information (please see Policy for Secure Storage, Handling, Use, Retention and Disposal of Disclosures and Disclosure Information).
- Outside contractors such as name, address, date of birth, telephone number, email address, bank details, DBS information (please see Policy for Secure Storage, Handling, Use, Retention and Disposal of Disclosures and Disclosure Information).

Other information includes (but is not exclusive to):

- Accident forms
- Incident forms
- Medication records
- Signing in and out records
- Sleep charts
- Nappy change records
- Weekly attendance registers
- Learning Journals (including All About Me forms, Key Person Permission Forms, weekly observations and Development Matters tracking tool)
- Individual Educational Plans (IEP's)/Special Educational Needs (SEN) reports
- Absence/Sickness record for children
- Staff sickness records (including any doctors notes)
- Staff supervision records

Personal information may be stored in two forms:

1. Paper: Personal information about children, parents/carers, staff, committee and other relevant professionals is stored securely in the main office which is kept locked at all times when not in use. Individual staff/children/committee files, which contain confidential and sensitive information, are securely stored in lockable, non-portable filing cabinets and access is restricted to relevant members of staff.
2. Electronically: any information that is stored on the settings internet cloud storage/computers will be held in accordance with the GDPR. All staff have individual

logins for the main computers and cloud storage, with a hierarchy of access to the relevant information and data for their role. All documents that contain sensitive information are password protected and access to these files is restricted to the relevant members of staff. The settings internet access is password protected and the password is only shared with relevant staff and professionals. The setting's internet network is protected by firewall systems provided by IP Office Solutions (please see E-Safety Policy).

At Ludgvan Oasis Childcare Centre we have two main computer workstations which are located in the office. Screens are positioned away from the view of people accessing the setting (parents/carers, other professionals, visitors to the setting), and all staff members remain conscious of casual observers at all times when working at these stations. If staff members leave the workstations for any reason, they must ensure that they lock the computer to restrict other users accessing confidential/sensitive information. The setting also has three laptop computers; two that are accessed by all staff to use the interactive whiteboard and complete paperwork. Both laptops are password protected and remain on site at all times. All staff have individual logins with different levels of user access depending on their roles. The other laptop is used by the Centre Manager only and may, on occasions, be taken off site to complete necessary paperwork tasks. This laptop is encrypted and password protected. Access to sensitive and confidential information is also password protected.

We have 3 mobile tablet devices for staff to use; one in each of the learning rooms. Each of the tablets are password protected and have a designated safe storage place for when not in use. The mobile tablet devices must remain on site at all times.

Accuracy of Personal Data

Oasis Childcare Centre strives to ensure that the personal information we hold on site is accurate and up to date. Regular reminders are issued to parents via the monthly newsletters and new contact detail forms are given out every 12 months. Regular reminders are also given to staff via our staff meetings and all staff are required to complete a new contact details form every year as part of their Formal Supervision. The settings Administrator ensures that all personal information is updated when changes occur and ensures that any changes shared with necessary third parties where relevant (such as the Local Authority Funding team).

Data Disclosures

Personal information regarding children, parents, staff, committee members, students, volunteers, visitors and other relevant professionals will only be shared with third party individuals or organisations with prior consent. However, in exceptional circumstances personal information will be shared with third party organisations without prior consent when we are legally required to do so. This includes:

- In the event of a safeguarding concern (please see Child Protection Policy)
- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders

- The assessment of collection of tax owed to HMRC
- In connection with legal proceedings
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them respond to an emergency situation that affects any of our children, families or staff.

Any personal data that is required to be transferred to a country or territory outside of the European Economic Area (EEA), we will shared in accordance with data protection law.

Subject Access Requests

Under the new GDPR guidelines, individuals have the right to make a 'subject access request' to gain access to the personal information we hold on them. This enables individuals to be aware of and verify the lawfulness of the processing. We will not charge a fee to access your personal data or to exercise any of the other rights under data protection laws. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

All 'Subject Access Requests' must be made in writing addressed to Lorna Trudgeon, Senior Manager (please see Appendix A: Data subject access request form). Requests will be acknowledged in writing within five working days and the information must be provided within one month of receipt of the initial 'Subject Access Request'. In the event of receiving complex or numerous requests, the compliance period can be extended to three months. If this is the case, the individual must be informed within one month of the receipt of the request and explain why the extension is necessary.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee that takes into account administrative costs.

A request will be deemed unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and explain their right to complain to the ICO.

Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing

- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area (EEA)
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

All requests listed above should be submitted in writing to Lorna Trudgeon, Senior Manager.

Retention and Disposal of information

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. Please see Data Retention Policy for details.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Personal data that is no longer required will be disposed of securely; paper files will be shredded on site and electronic files will be permanently deleted. We will also securely dispose of any personal data that has become inaccurate or out of date, where we are unable to rectify or update it.

CCTV

We have 12 CCTV cameras installed in various locations around the setting. Lorna Trudgeon, Senior Manager, is responsible for the control of images and their purpose, and we adhere to the ICO's code of practice for the use of CCTV. The security cameras are clearly visible and prominent signs are displayed across the setting to explain that CCTV is in use.

The CCTV is used to safeguard the children as well as staff and other adults on the premises. The security of the premises is also recorded when the setting is closed, which includes the outdoor area.

Management may decide to use the CCTV as part of staff supervision and monitoring practices of staff throughout the setting. This will be discussed with individual staff members and a written supervision form will be kept on their employment records; this supports the quality and delivery of our service. All benefits from installing CCTV at the setting have been considered.

The CCTV footage is stored locally on the hard drive for 2-3 weeks, which is located in the staff room. In the event of footage being required to support a safeguarding concern, criminal offence or any other practices deemed inappropriate by management, individuals concerned will be informed. Images will be recorded onto a USB memory stick and securely stored in a locked cabinet, which is only accessible by Management. Images will be removed from the USB memory stick when they are no longer required.

During inductions, all new staff and potential parents are made aware of the CCTV system and its purpose. They are required to sign their induction form, which includes our privacy statement and consent for the Oasis Childcare Centres to record images of themselves and/or their child.

Photographs and Videos

The use of cameras and photographs within the settings is central to the implementation of the EYFS and the completion of learning journeys. Individual signed parent/carer permission to take photographs must be sought on admission details. This includes permission for child to be used in press releases. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the relevant photographs/videos and not distribute them any further.

Please see our 'Taking of Images Policy' for more information on our use of Photographs and videos.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a Data Protection Officer (DPO), and ensuring they have the necessary resources to fulfil their duties and maintain their knowledge and understanding.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles.
- Completing privacy impact assessments when the setting is required to process personal data which presents a high risk to the rights and freedoms of individuals, and when introducing new technologies.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Holding regular staff meetings/in-house staff training on data protection law, related policies and other relevant data protection matters. All staff meetings are minuted and staff attendance is recorded.

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
  >For the benefit of data subjects, making available the name and contact details of our settings and DPO, and all the information we are required to share about how we use and process personal data (please see Privacy Notices).
  >For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

Data Protection Breaches

Oasis Childcare Centres will endeavour to ensure that there are no personal date breaches. In the unlikely event of a suspected date breach, we will follow the procedures set out in our Data Breach Procedure.

Staff Training

All staff, committee, students and volunteers are provided with in-house data protection training as part of the induction process. Data protection also forms part of our continuous professional development, ensuring that changes to legislation, guidance, policy or procedures are shared with staff during staff meetings and/or individual staff supervision.

This policy applies to all staff employed by Oasis Childcare Centres, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action (please see Disciplinary Procedures).

All parents/carers, staff, committee, students, volunteers and other relevant professionals/contractors should note that in the event of a safeguarding concern being raised, information about children, families and/or professionals may be shared with the relevant agencies without prior consent.

Adopted by The Oasis Management Committee on: 31.08.2021
Representative of Management Committee Signature: Lorna Mudgeon
Review Date: August 2022

Please note that this is a working document and will be regularly updated. For updated list of third parties we work with, please see the Privacy Statements on our website.

Data Breach Procedure

What is a personal data breach?

'A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data'. (ICO, 2018)

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

The GDPR clearly specifies that if a security incident takes place, we should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including informing the ICO if required.

All data breaches will be investigated to find out whether the breach occurred as a result of human error or a systemic issue, and actions will be put in place to prevent future recurrence. This could be through staff training or making alterations to current procedures.

The following procedures are based on the document 'Guidance on personal data breaches' produced by the ICO.

Identifying a Data Breach

In the event of a potential data breach being identified, the DPO must be informed immediately. The DPO will alert the Senior Manager and together, they will investigate the report to determine whether a breach has occurred, taking into consideration whether personal data has been accidently or unlawfully:

- lost,
- stolen,
- destroyed,
- altered,
- disclosed or made available to unauthorised people and/or companies.

The DPO, assisted by the Senior Manager, will:

- make all reasonable efforts to contain and minimise the impact of the breach.
- assess the potential consequences, based on how serious they are, and how likely they are to happen.

- determine whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO and Senior Manager will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned.

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), which will be stored electronically on the setting's internet drive. A designated file called GDPR has been created in the Oasis Admin Shared Drive, and within this is a designated file called 'Data Breaches'. Any potential data breaches will be stored in this file to ensure we have access to the relevant information should a decision be challenged in the future by the ICO or an individual affected by the breach.

Reporting a Data Breach

Where the decision is made to notify the ICO, the DPO will complete this via the 'report a breach' page of the ICO website. This must be completed within 72 hours of becoming aware the breach. The individual(s) affected must also be informed as soon as possible. As required, the DPO will provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If all of the above details are not known, the DPO will report as much as they can within 72 hours. The report must explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

Informing Individuals

If a data breach is identified as being 'high risk' to people's rights and freedoms, the individual(s) must be informed as soon as possible. We are required to describe, in clear and plain language, the nature of the personal data breach and provide, at least:

- the name and contact details of our data protection officer
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

The DPO will also notify any relevant third parties who can help minimise the loss to individuals, such as the police, insurers, professional bodies, or bank or credit card companies.

Documenting Data Breaches

In all cases, the DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, the record will include the:

- facts and causes
- effects
- action taken to contain the breach and ensure is does not happen again (such as establishing more robust processes or providing further staff training for individuals).

Records of all breaches are stored electronically on the setting's internet drive. A designated file called GDPR has been created in the Oasis Admin Shared Drive, and within this is a designated file called 'Data Breaches'. Any potential data breaches will be stored in this file to ensure we have access to the relevant information should a decision be challenged in the future by the ICO or an individual affected by the breach.

Actions to minimise the impact of data breaches

Oasis Childcare Centre will take the actions set out below to minimise the impact of different types of data breach, focusing particularly on breaches that involve sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records):

- All sensitive information must be password protected when being shared with authorised third parties via email.
- If special category data (sensitive information) is accidently made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the Senior Manager or DPO will contact our ICT Support to recall the email.
- In the event of the recall being unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the email was sent in

error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

- The DPO will request a written response from all of the individuals who received the data, and ensure that they all reply to confirm that they have complied with this request.
- The DPO will complete an internet search to ensure that the information has not been made public; in the event of the information being published online, the DPO will contact the publisher/website administrator and request that the information is removed from their website and deleted.
- If a staff member receives personal data sent to them in error, they must alert the sender and inform the DPO as soon as possible.

Setting's computers and/or laptops containing non-encrypted sensitive personal data being lost, stolen or hacked:

- All laptop's and mobile tablet devices do not leave premises. The only exception is the Senior Manager's laptop, which is occasionally taken off-site to complete paperwork based tasks from home. The laptop is password protected and has the necessary encryption software installed.
- All documents containing sensitive information (including child protection documents) are password protected.
- Access to the internet is password protected. Its content is filtered using a Draytek router, which is set-up and configured by IP Office Solutions who provide our filtering and firewall service. Please see 'E-Safety Policy'.

Disciplinary procedures will be followed if staff do not adhere to the regulations set out in this policy (please see Disciplinary Procedures).

ICO Contact Details

Information Commissioner's Office (ICO)
Telephone: 0303 123 1113
Website: https://www.ico.org.uk/concerns

Adopted by The Oasis Management Committee on: 31.08.2021
Representative of Management Committee Signature: Lorna Trudgeon
Review Date: August 2022

Please note that this is a working document and will be regularly updated. For updated list of third parties we work with, please see the Privacy Statements on our website.

Data Retention Checklist

Basic file description	Data protection issue	Retention period	Action at the end of the administrative life of the record
Committee records			
Agenda's for committee meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff.	One copy should be retained with the master set of minutes. All other copies can be disposed.	SECURE DISPOSAL
Minutes of committee meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff.	Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.
AGM reports presented to the committee	There may be data protection issues if the report deals with confidential issues relating to staff.	Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently.	SECURE DISPOSAL
Recruitment/Employment Records			
Individual staff files	Yes - contains sensitive personal information.	6 years from the date of termination of employment	SECURE DISPOSAL
Job applications and interview records of unsuccessful candidates.	Yes - contains sensitive personal information.	Date of interview + 6 months	SECURE DISPOSAL
Job applications and interview	Yes - contains sensitive	All relevant information added to	SECURE DISPOSAL

records of successful candidates.	personal information.	individual staff file. Any other information will be retained for 6 months.	
Personnel and training records	Yes - contains sensitive personal information.	Duration of employment + 6 years	SECURE DISPOSAL
Job description, contract of employment and any changes to terms and conditions.	Yes - contains sensitive personal information.	Duration of employment + 6 years	SECURE DISPOSAL
Staff supervision records	Yes - contains sensitive personal information.	Current year + 5 years	SECURE DISPOSAL
Timesheets	Yes – contains sensitive personal information	Current year + 6 years	SECURE DISPOSAL
Annual leave records	No	6 years	SECURE DISPOSAL
Payroll and wage records	Yes – contains sensitive personal information.	6 years from the financial year-end in which payments were made.	SECURE DISPOSAL
PAYE records	Yes – contains sensitive personal information.	3 years after the end of the tax year to which they relate.	SECURE DISPOSAL
Maternity records	Yes – contains sensitive personal information.	3 years after the end of the tax year in which the maternity pay period ends.	SECURE DISPOSAL
Sickness records required for the purposes of Statutory Sick Pay	Yes – contains sensitive personal information.	3 years after the end of the tax year in which the payments period ends.	SECURE DISPOSAL
Records held under retirement benefits schemes (information powers) regulations 1995	Yes – contains sensitive personal information.	Current year + 6 years	SECURE DISPOSAL
Current bank details of employees	Yes – contains sensitive personal information.	Duration of employment until final payments are made.	SECURE DISPOSAL
Any reportable accident, death or injury in connection with work	Yes – contains sensitive personal information.	Date of incident + 12 years. In the case of serious accidents a further retention period will need to be applied.	SECURE DISPOSAL

Consents for the processing of personal and sensitive data	Yes – may contain sensitive personal information.	Duration of when the data is being processes + 6 years	SECURE DISPOSAL
Disclosure and Barring Service (DBS) checks and disclosures of criminal records forms	Yes – contains sensitive personal information.	The setting does not keep copies of DBS certificates. If they are copied for any reason, they are not retained for any period longer than 6 months.	SECURE DISPOSAL
Proofs of identity collected as part of the process of checking 'portable' enhanced DBS disclosures.	Yes – contains sensitive personal information.	Where possible these should be checked and a note kept of what evidence has been seen and checked. If it is felt necessary to keep a copy of the documentation provided, then this should be securely stored in individual staff files.	SECURE DISPOSAL
Immigration checks	Yes – contains sensitive personal information.	2 years after the termination of employment.	SECURE DISPOSAL
Staff Supervision Records/ Professional Development Plans	There may be data protection issues if the meeting is dealing with confidential issues relating to individual staff and/or children.	Date of meeting + 6 years	SECURE DISPOSAL
Disciplinary and Grievance Procedures			
Allegation of a child protection nature against a member of staff, including where the allegation is unfounded.	Yes – contains sensitive personal information.	Until the persons normal retirement age or 10 years from the date of the allegation, whichever is longer. Then review. *Note – allegations that are found to be malicious should be removed from	SECURE DISPOSAL (documents must be shredded)

		personnel files. If allegation is founded, they are to be kept on file and a copy provided to the individual concerned.	
Disciplinary proceedings: • Oral warning • Written warning – level 1 • Written warning – level 2 • Final warning • Case not found	Yes – contains sensitive personal information.	• Date of warning + 6 months • Date of warning + 6 months • Date of warning + 12 months • Date of warning + 18 months • If the incident is child protection related then see above, otherwise dispose of information at the end of the case.	SECURE DISPOSAL (if warnings are placed in individual staff file then they must be removed from the file)
Children's records			
Individual children's registration forms.	Yes - contains sensitive personal information.	Duration of attendance + 1 year	SECURE DISPOSAL
Child protection information held in individual files.	Yes – contains sensitive personal information.	DOB of the child + 25 years	SECURE DISPOSAL (These records MUST be shredded)
Special Educational Needs files, reviews and Individual Education Plans (IEPS) (includes records of Education, Health and Care (EHC) Plans, advice/information given to parents, reports from external professionals, any referrals made to external professionals and accessibility strategies where relevant)	Yes – contains sensitive personal information.	DOB of the child + 25 years.	SECURE DISPOSAL (unless the document is subject to a legal hold)
Individual children's educational	Yes – contains sensitive	Retain whilst the child attends the	This information should follow

records, (including baseline assessments, termly assessments and progress tracker)	personal information.	setting as a minimum. DOB of the child + 25 years	the child when he/she leaves the setting. This will include: • To another nursery setting • To primary school
Administration			
Complaints	Yes – may contain sensitive information.	Date of the resolution of complaint + a minimum of 6 years. Then review for further retention in case of contentious disputes.	SECURE DISPOSAL
Staff meeting minutes	There may be data protection issues if the meeting is dealing with confidential issues relating to individual staff and/or children.	Date of the meeting + 3 years	SECURE DISPOSAL
Signing in sheets (children)	Yes – contains personal information	Current year + 6 years	SECURE DISPOSAL
Signing in sheets (visitors)	Yes – contains personal information	Current year + 6 years	SECURE DISPOSAL
School meals register	Yes – personal information	Current year + 3 years	SECURE DISPOSAL
Attendance registers	Yes – contains personal information	Current academic year + 3 years	SECURE DISPOSAL
Parental declarations for Funding.	Yes – contains personal and sensitive information.	7 years	SECURE DISPOSAL
Record of sickness/absence	Yes – contains personal information	Current academic year + 2 years	SECURE DISPOSAL
Ofsted Report	No	Until new report is published	SECURE DISPOSAL

Educational trips/visits			
Parental consent forms for school trips where there has been no major incident	Yes - contains personal information	Conclusion of the trip	SECURE DISPOSAL
Parental consent forms for school trips where there has been a major incident	Yes - contains personal information	DOB of the child involved in the incident + 25 years. The permission slips for all children on the trip need to be retained to show the rules had been followed for all pupils.	SECURE DISPOSAL
Health and Safety			
Accident reporting: • Adults • Children	Yes - contains sensitive personal information.	• Date of the incident + 6 years • DOB of the child + 25 years	SECURE DISPOSAL
Control of Substances Hazardous to Health (COSHH)	No	Current year + 40 years	SECURE DISPOSAL
Fire precautions log book	No	Current year + 6 years	SECURE DISPOSAL
Financial Management			
Employer's liability insurance certificate	No	Closure of the school + 40 years	SECURE DISPOSAL
Annual accounts	No	Current year + 6 years	SECURE DISPOSAL
All records relating to the creation and management of budgets, including the annual budget statement and background papers.	No	Duration of the budget + 3 years	SECURE DISPOSAL
Invoices, receipts, order books and requisitions, delivery notices	No	Current financial year + 6 years	SECURE DISPOSAL
Records relating to the	No	Current financial year + 6 years	SECURE DISPOSAL

collection and banking of monies.			
Records relating to the identification and collect of debt.	Yes - may contain sensitive personal information of individual concerned.	Current financial year + 6 years	SECURE DISPOSAL
Property Management			
Title deeds of properties belonging to Oasis Childcare Centres	No	PERMANENT These should follow the property unless the property has been registered with the Land Registry.	
Plans of property belonging to Oasis Childcare Centres	No	These should be retained whilst the building belongs to the setting an should be passed on to any new owners if the building is leased or sold.	
Leases of property leased by or to the Oasis Childcare Centres	No	Expiry of lease + 6 years	SECURE DISPOSAL
Records relating to the letting of Oasis Childcare Centres premises	No	Current financial year + 6 years	SECURE DISPOSAL
All records of the maintenance of the setting carried out by contractors	No	Current year + 6 years	SECURE DISPOSAL
All records relating to the maintenance of the setting carried out by our Handyman, including maintenance log books	No	Current year + 6 years	SECURE DISPOSAL

Data Subject Access Request Form

The General Data Protection Regulation (Regulation (EU) 2016/679) **(GDPR)** gives you the right to access your personal data held by the Oasis, including the right to obtain confirmation that we process your personal data, receive certain information about what we do with such personal data, and obtain a copy of the personal data we hold about you. You must submit this request in writing, via post to: Lorna Trudgeon, Lower-Quarter Ludgvan, Penzance TR20 8EX or electronically via email to admin@oasischildcare.org.uk. Once you have submitted your request, we must confirm your identity through a form of ID, such as passport or photo card driver's licence.

We expect to respond to your request within one month of receipt of a fully completed form and proof of identity. If we are not able to respond to your request within such one month period, we will write to you within such one month period to let you know why we are not able to respond within the month. If this is the case, we will send you our substantive response within three months of your request.

In addition to exercising your access right, GDPR also grants you the right to:

- Request that your personal data is corrected or deleted.
- Restrict or object to certain types of data processing.
- Make a complaint with the Information Commissioner's Office, which is the UK's supervisory authority for data protection purposes.

For more information on your rights under the GDPR, see please our Privacy Policy at www.oasischildcare.org.uk/dataprotection or speak to Briony Sedgeman, Data Protection Officer.

1. Requester Name (Data Subject) and Contact Information

Please provide your information in the space provided below. [If you are making this request on an employee's/child's behalf, you should provide your name and contact information in Section 3].

We will only use the information you provide on this form to identify you and the personal data you are requesting access to, and to respond to your request.

Please complete as follows:

First and last name: _____

Any other names that you have been known by (including nicknames): _____

Home address: _____

Date of birth: _____

Telephone number: _____

E-mail address: _____

If you are a current or former employee of the Oasis, please provide us with your approximate dates of employment:

_____

Please provide other unique identifiers or related information to help us locate your personal data (for example, national insurance number):

_____

2. Proof of Data Subject's Identity

We will need proof of your identity before we can respond to your access request. To help us establish your identity, you must provide with this form identification that clearly shows your name, date of birth, and current address. We accept a photocopy or

a scanned image of one of the following as proof of identity: passport or photo card driver's license. If you have changed your name, please provide the relevant documents that show how your name has been changed e.g. marriage certificate.

If you do not have any of these forms of identification available, please contact Briony Sedgeman (DPO) or Lorna Trudgeon (Centre Manager) at 01736 741528 or admin@oasischildcare.org.uk for advice on other acceptable forms of identification.

We may request additional information from you to help confirm your identity and your right to access, and to provide you with the personal data we hold about you. We reserve the right to refuse to act on your request if we are unable to identify you.

3. Requests Made on a Data Subject's Behalf

Please complete this section of the form with your name and contact details if you are acting on an employee's behalf.

First and last name: _____

Home address: _____

Date of birth: _____

Telephone number: _____

E-mail address: _____

We will need proof of your identity and your legal authority to act on behalf of the employee before we can respond to your access request. We accept a photocopy or a scanned image of one of the following as proof of your identity: passport or photo card drivers licence. If you do not have any of these forms of identification available, please contact Briony Sedgeman (DPO) or Lorna Trudgeon (Centre Manager) at 01736 741528 or admin@oasischildcare.org.uk for advice on other acceptable forms of identification. We may request additional information from you to help confirm your identity if necessary.

We accept a copy of the following as proof of your legal authority to act on the employee's behalf: a written consent signed by the employee (the data subject), a certified copy of a Power of Attorney, or evidence of parental responsibility.

Please state below the evidence you are enclosing with this form to (a) verify your identity and (b) prove your legal authority to act on behalf of the above named employee:

(a) _____
(b) _____

4. Information Requested

To help us process your request quickly and efficiently, please provide as much detail as possible about the personal data you would like to have access to. Please include time frames, dates, names, types of documents, file numbers, or any other information to help us locate your personal data.

For example, you may specify that you are seeking:

- Employment records or personnel records.
- Personal data held by certain departments (please name the department).
- Medical records.
- E-mail or other electronic communications (specify the approximate dates and times).
- Billing information.
- Photographs.
- Video footage.
- User activity logs.

- Transaction histories
- Correspondence (please provide the dates between which you are requesting the data).

Please enter the details of the information requested here:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

We will contact you for additional information if the scope of your request is unclear or does not provide sufficient information for us to conduct a search (for example, if you request "all information about me"). We will begin processing your access request as soon as we have verified your identity and have all of the information we need to locate your personal data.

In response to your request, we will provide you with the information required by the GDPR, including information on:

- The purposes of processing.
- The types of personal data processed.
- Recipients or categories of recipients who receive personal data from us.
- How long we store the personal data, or the criteria we use to determine retention periods.
- Information on the personal data's source if we do not collect it directly from you.
- Whether we use automated decision-making, including profiling, the auto-decision logic used, and the consequences of this processing.
- Your right to:
- request correction or deletion of your personal data;
- restrict or object to certain types of processing with respect to your personal data; and
- make a complaint with the local data protection authority.

If the information you request reveals personal data about a third party, we will either seek that individual's consent before responding to your request, or we will take out such third parties' personal data before responding. If we are unable to provide you with access to your personal data for certain reasons such as disclosure adversely affecting the rights and freedoms of third parties, we will notify you of this decision.

Applicable law may allow or require us to refuse to provide you with access to some or all of the personal data that we hold about you, or we may have destroyed, erased, or made your personal data anonymous in accordance with our record retention

obligations and practices. If we cannot provide you with access to your personal data, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

5. Signature and Acknowledgement

I, _____, confirm that the information provided on this form is correct and that I am the person whose name appears on this form. I understand that: (1) The Oasis must confirm proof of identity and may need to contact me again for further information; (2) my request will not be valid until the Oasis receives all of the required information to process the request; and (3) I am entitled to one free copy of the personal data I have requested, and acknowledge that for any further copies I request, the Oasis may charge a reasonable fee based on administrative costs.

If you would like to receive a copy of the personal data you are requesting access to, please indicate below whether you would like a hard copy or an electronic copy:

____ Hard copy.

____ Electronic copy.

PLEASE SEND THIS FORM TOGETHER WITH THE NECESSARY PROOF OF IDENTITY TO **admin@oasischildcare.org.uk** OR **Oasis Childcare Centre, Lower-Quarter Ludgvan, Penzance TR20 8EX** FOR THE ATTENTION OF **Lorna Trudgeon.**

_____

Signature

_____

Date

6. Authorised Person Signature

I, _____, confirm that I am authorised to act on behalf of the data subject. I understand that the Oasis must confirm my identity and my legal authority to act on the data subject's behalf, and may need to request additional verifying information.

_____

Signature

_____

Date