MY OASIS

Therapeutic Alternative Provision

Data Protection/ GDPR Policy 2026/2027

Date of last review: February 2026

Date of next review: February 2027

CHARLOTTE LOWE
PSYCHOLOGICAL SERVICES LTD

MY OASIS

www.charlottelowepsychologicalservices.co.uk

www.my-oasis.uk

Contents

Purpose and Scope

My Oasis Therapeutic Alternative Provision (referred to as the "school")/Charlotte Lowe Psychological Services Ltd collects and processes personal data relating to staff, students, parents/carers, governors, visitors, and other individuals. This policy ensures that all personal data is collected, stored, and processed in accordance with:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018 (DPA 2018).
- Data (Use and Access) Act.

This policy applies to all personal data, whether held on paper, electronically, or otherwise, and covers:

- Staff (employees, contractors, volunteers).
- Students and former students.
- Parents, carers, and individuals with parental responsibility.
- Governors and visitors.

Legislative Framework

This policy is informed by and complies with the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR) – which sets out the core principles, lawful bases for processing, individual rights, data security requirements, and rules governing international transfers of personal data.
- Data Protection Act 2018 – which supplements and tailors the UK GDPR for the UK, including provisions relating to special category data, criminal offence data, enforcement powers, and processing for education and safeguarding purposes.
- Information Commissioner's Office (ICO) Guidance – which provides authoritative regulatory guidance on data protection compliance, subject access requests, data breaches, and good practice standards.
- Education (Student Information) (England) Regulations 2005 – which give parents and individuals with parental responsibility a statutory right of access to a child's educational record.

Definitions

Term	Definition
Personal data	Any information relating to an identified or identifiable living individual (e.g., name, address, ID number, online identifiers, biometric data).
Special categories of personal data	Sensitive data requiring higher protection, including race, religion, politics, trade union membership, health, genetics, sexual orientation, or sex life.
Criminal offence data	Data relating to criminal convictions or offences.
Processing	Any operation on personal data, including collection, storage, use, disclosure, alteration, erasure, or destruction, whether automated or manual.
Data subject	The identified or identifiable individual whose personal data is processed.
Data controller	A person or organisation that determines the purposes and means of processing personal data.
Data processor	A person or organisation, other than an employee, that processes data on behalf of the controller.
Personal data breach	Any accidental or unlawful loss, alteration, destruction, or unauthorised disclosure or access to personal data.

The Data Controller

My Oasis processes personal data relating to parents/carers, students, staff, governors, visitors and others, and therefore is a data controller.

My Oasis is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

Roles and Responsibilities

This policy applies to all staff employed at CLPS Ltd / My Oasis Therapeutic Alternative Provision and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body

The governing body is responsible for ensuring My Oasis complies with all data protection obligations.

Data Protection Officer (DPO)

- Oversees implementation of this policy.
- Monitors compliance with UK GDPR/DPA 2018.
- Provides annual reports to the governing board.
- Acts as first contact for data subjects and the ICO.

Headteacher

Represents the data controller on a day-to-day basis.

All Staff

- Process personal data lawfully and in line with this policy.
- Inform My Oasis/CLPS of any changes to personal data.
- Contact the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
- If they have any concerns that this policy is not being followed.
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside of the UK and any countries recognised by the UK as providing an adequate level of data protection.
- If there has been a data breach.
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
- If they need help with any contracts or sharing personal data with third parties.

Data Protection Principles

The GDPR is based on data protection principles that My Oasis must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Retained for no longer than is necessary for the purposes for which it is processed.
- Processed securely to prevent unauthorised access, loss, or damage.

This Data Protection policy sets out how My Oasis aims to comply with these principles.

Collecting Personal Data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual or another person, i.e. to protect someone's life.
- The data needs to be processed to perform a task carried out in the public interest or in the exercise of official authority.
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a student) has given explicit consent.
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law.
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.
- The data needs to be processed for the establishment, exercise or defence of legal claims.
- The data needs to be processed for reasons of substantial public interest as defined in legislation.
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a student) has given consent.
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
- The data needs to be processed for reasons of substantial public interest as defined in legislation. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Collection, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

Data Sharing

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.

- Our suppliers or contractors need data to enable us to provide services to our staff and students, for example, IT companies. When doing this, we will:

    - Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law.
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so. We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff. Where we transfer personal data internationally, we will do so in accordance with data protection law.

Subject Access Requests and Individual Rights

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual.
- Correspondence address.
- Contact number and email address.

- Details of the information requested.

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded as being mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may be granted without the express permission of the student. This is not a rule, and a student's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded as being mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule, and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant).
- Will provide the information free of charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the student or another individual.

- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent, and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO, or they can seek to enforce their subject access right through the courts.

Other 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 (in certain circumstances).
- Prevent the use of their personal data for direct marketing.
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement).
- 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).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Parental Requests to View Educational Records

Parents/carers, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the student concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual.

Our approach at My Oasis is to be collaborative with the parent and/or carer with regards to their child's educational needs. A parent and/or carer can therefore request their records by submitting a request to the Headteacher.

Photographs and Videos

As part of our school's activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for all/any school purposes as detailed within our photography and videography consent form. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the student, and consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Any photographs and videos taken by parents/carers at school events off school premises for their own personal use are not covered by data protection legislation, photographs are not permitted on school grounds, and we ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons.

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 suitably qualified DPO and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in the relevant data protection law.
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to the rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents, including this policy, any related policies and privacy notices.
- Conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK and any countries recognised by the UK as providing an adequate level of data protection, where different data protection laws will apply.
- Maintaining records of our processing activities, including:

    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and any countries recognised by the UK as providing an adequate level of data protection and the safeguards for those, retention periods and how we are keeping the data secure.

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as school laptops and mobile phones that contain personal data, are kept secure when not in use, and data is removed from devices and transferred to a secure location as soon as possible (please refer to our E-safety and Acceptable Use Policy).
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Personal information is not to be taken off-site.

- Passwords must be sufficiently strong (for example, at least 12+ characters or a secure passphrase), containing letters and numbers, are used to access school computers, laptops and other electronic devices. Staff and students are reminded that they should not reuse passwords from other sites.
- The use of Encryption software to protect all portable devices and removable media, such as laptops.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal Data Breaches

My Oasis will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the correct procedure set out within this policy.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches within the school context may include, but are not limited to:

- A non-anonymised dataset being published on the school's website, which shows the exam results of students eligible for the student premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing personal data about students.

Training

Data protection will form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every year and shared with the full governing board.

Policy Links

This data protection policy is linked to our:

- Safeguarding and Child Protection Policy.
- Code of Conduct.
- E-safety and Acceptable Use Policy.

Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

The DPO will investigate the report and determine whether a breach has occurred.

To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost.
- Stolen.
- Destroyed.
- Altered.
- Disclosed or made available where it should not have been.
- Made available to unauthorised people.

The DPO will alert the headteacher and the chair of governors.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure).

The DPO will assess the potential consequences, based on how serious they are and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO 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's 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), in case it is challenged at a later date by the ICO or an individual affected by the breach. At My Oasis, documented decisions are stored with our Data Protection Officer.

A description of the nature of the personal data breach will be given, including, where possible:

- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will 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.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.

- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

As above, any decision on whether to contact individuals will be documented by the DPO.

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

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

- Facts relating to the breach.
- Effects.
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to Minimise the Impact of Data Breaches

We will take the actions set out below to mitigate the impact of different types of data breaches, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information or special category data, including information related to any safeguarding or child protection records, will be transferred in line with KCSIE, and a record of this transfer will be kept within the appropriate secure unit.

However, if special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error. If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT provider to recall it. In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information 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 ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the website owner or administrator to request that the information be removed from their website and deleted.

If a school laptop containing sensitive personal data is stolen or hacked, the staff member must report this immediately to the DPO.