

Data Protection Policy

OASES works with children, young people, school staff and members of the general public. As part of our duty of care we must make sure that all of these people are kept safe at all times. Part of this duty of care involves the protection of their individual data.

OASES also has an obligation to protect the personal data of its staff and its consultants.

OASES supplies data to third parties in the form of evidence of work completed to: grant giving organizations; Local Authorities (where work has been commissioned); other charities (where work has been commissioned). In all cases OASES will ensure that the data collected is in the charity's/organisations legitimate interests and it does not override the rights and freedoms of the beneficiary who owns it.

To ensure that we achieve the above, and remain compliant in the eyes of the law, OASES will follow the guidance outlined within the government's General Data Protection Regulation (GDPR) and the Data Protection Bill.

Last Updated: 20th April 2018

The GDPR provides a set of 'Guiding Privacy Principles' which set out how organisations should be managing personal data, these are basically an overview of what Data Controllers should bear in mind to ensure compliance with the regulation. OASES will follow the six privacy principles detailed in Article 5 of the GDPR which are as follows:

PRINCIPLE 1: LAWFULNESS, FAIRNESS AND TRANSPARENCY - Any processing or storage of personal data will be done in accordance with the stipulations of the GDPR. OASES will ensure that the data subject is informed about the processing of their data, and the processing matches the description provided in the first place.

PRINCIPLE 2: PURPOSE LIMITATION - The GDPR stipulates that personal data can only be collected for "specified, explicit and legitimate purposes". OASES will be upfront and clear to the data subject regarding the lawful basis for data collection and what the data will be used for. The processing of such data will be limited to the originally stated purpose.

PRINCIPLE 3: DATA MINIMISATION - The GDPR stipulates that any personal data processed should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". OASES will not collect more data than is strictly required for the purpose at hand.

PRINCIPLE 4: ACCURACY - The GDPR requires personal data to be “accurate and, where necessary, kept up to date”. OASES will ensure that the personal data that we process/store is accurate and kept up-to-date.

PRINCIPLE 5: STORAGE LIMITATION - The GDPR requires personal data to be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”. OASES will not keep personal data for any longer than is necessary.

PRINCIPLE 6: INTEGRITY AND CONFIDENTIALITY- The GDPR requires Data Controllers to process personal data “in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage”. OASES will ensure that all personal data collected is kept safe and secure.

The OASES CEO and the OASES Board are the Data Controllers for OASES. It is therefore the responsible of the OASES CEO and the OASES Board to ensure and demonstrate compliance.

A Data Controller is ‘the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data’

The OASES CEO and the OASES Board will guarantee that all of the Privacy Principles are met across the entire lifecycle of the personal data within OASES control. Our responsibility for compliance will cover all third-party processors in addition to our own internal systems.

Although OASES does not require a Data Protection Officer as it is not:

- A public authority.
- An organisation which carries out regular and systematic monitoring of individuals on a large scale.
- An organisation that carries out large scale processing of special categories of data, such as health records, or information about criminal convictions.

In the interests of best practice the OASES CEO and the OASES Board have appointed the Durham County Council Advisor for Sustainability Education (Richard Hurst) as their Data Protection Officer.

Ensuring Data Protection

In order to operate successfully, and achieve the charity's stated objectives, OASES needs access to the personal data/some sensitive personal data detailed within the OASES Information Audit.

Personal Data – Data that is concerned with an identifiable, living individual (e.g. Name, Age, Address, IP addresses, Internet Cookies etc.).

Sensitive Personal Data – data pertaining to an individual's: race or ethnic origin; political opinions; religious beliefs; affiliation with a Trade Union; physical or mental health; sexual orientation; commission or alleged commission of an offence.

OASES Personal Data

The Personal Data most commonly used by OASES, as identified within the OASES Information Audit, is as follows:

- Personal data of OASES staff – OASES must have the written permission of staff (Consent) to use and store this data unless the law (Legal Obligation) decrees otherwise.
- Contact details of individual teachers – OASES must have written evidence of Consent, from the individual, to use this data.
- Testimonials - OASES must have written evidence of Consent, from the individual, to use their testimonial IF their name is placed against the testimonial.
- Project Evidence - OASES must have written evidence of Consent, from the individual, to use this data OR the individual must be informed of the Legitimate Interests of the Funder (e.g. evidence of delivery and impact) and agree to the processing.
- Accredited Course Work - OASES must process this data to fulfil the obligations of a Contract but it is best practice to obtain evidence of Consent from the individual.

OASES Sensitive Personal Data

OASES does not hold personal sensitive data for its clients but it does hold such data for its employees, volunteers and job applicants. This data will be treated with special care.

- Employee Data – to be placed in a clearly named employee file and stored alphabetically within the lockable OASES Filing Cabinet. Employees to Consent to all data retention. Stipulated deletion time frames to be observed.
- Volunteer Data - to be placed in a clearly named volunteer file and stored alphabetically within the lockable OASES Filing Cabinet. Volunteers to Consent to all data retention. Stipulated deletion time frames to be observed.

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

- Job Applicants – all application forms to be stored within a clearly labelled (by Job) file and placed within the OASES Filing Cabinet. Once the successful candidate has accepted the job all other applications forms should be immediately shredded.

Not all data that OASES holds is considered personal (e.g. generic school email addresses, generic company details, photographs). This data will also, however, be tracked in the OASES Information Audit following best practice.

- Photographs - *OASES must have written evidence of Consent, from the individual, to use this data. If a child's photograph is taken, and the child is under the age of 16 (this may be 13), then written evidence of consent must be supplied by the child's parent / guardian. NOTE: no child's name should be attached to photographs at any point.*

Collection, Use, Storage, Access and Deletion of Personal Data

In order to comply with data protection law and the GDPR, OASES' handling of personal data is documented as follows:

Collection

In order to collect, use and store an individual's personal data (e.g. name, address, date of birth, email, telephone number etc.) OASES must have a 'Lawful Basis' for doing so.

'Lawful Basis' includes:

1. the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
2. processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a **legal obligation** to which the controller is subject (e.g. taxation);
4. processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;
6. processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Consent

Where another lawful basis does not exist OASES will use 'Evidence of Consent' as its Lawful Basis for collecting, using and retaining personal data.

Definition of Consent

The GDPR defines *'the consent of the data subject'* as *'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'*.

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

All OASES evidence of consent documentation must follow the above.

Evidence of Consent

If gathering data and relying on Consent as the justification the consent must be:

- * Specific * Informative * Clear * Prominent * Freely Given * Properly Documented
- * Easily withdrawn * Verifiable

Areas requiring Consent for the use of beneficiary data should be clearly set out, including how the data is to be held, what it is to be used for and how long it will be stored.

An individual must be able to 'opt in' to Consent. Consent cannot be implied through non-action / unticking a consent box. Hence, whenever OASES ask for consent there must be a **YES / NO** option.

If a child is under the age of 16 parental evidence of consent must be collected.

In most instances Consent can be acquired through the use of a Privacy Notice:

OASES Privacy Notice

In order to collect and use personal data (data that belongs to an individual) it is necessary to place a OASES Privacy Notice upon the documentation.

The OASES Privacy Notice must state:

- Our identity - That OASES (trading as OASES) is a Registered Charity no: 1041301
- Our intentions for the data that is collected - (e.g. funder evidence; to market our products and services).
- Our lawful basis for processing their data - (In OASES's case this is likely to be either due to 'Consent' or 'Legitimate Interest' as defined above.).
- How long we intend to keep their data - (e.g. marketing – indefinitely; specific project – for x years beyond the lifetime of the project; finance – for 7 years)
- That the individual has a right to complain to the ICO - (Information Commissioners Office) if they think there is a problem with the way that we are handling their data.

The GDPR requires that the information provided within the Privacy Notice is concise, easy to understand and clear (especially if dealing with young people).

EXAMPLE: Based on Consent

'OASES is the trading name for OASES a Registered Charity (no. 1041301). We would like to contact you about our services now and in the future (indefinitely) but we require your consent to do so. You have the legal right to withdraw your consent at any time and, if

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

withdrawn, we will ensure that your data is removed from all OASES systems. We will not give your data to anyone else and we promise to store your data safely and securely on our LiveDrive, cloud-based network. If you do not feel that we have handled your data appropriately you have the right to complain to the Information Commissioners Office. Do you consent to our use of your data for OASES marketing purposes YES / NO'

Legal Obligation

Occasionally OASES may hold data out of Legal Obligation. Where this is the case the individual will be informed of the obligation (e.g. employee NI for taxation purposes, Financial records for HMRC).

Vital Interest

OASES occasionally holds medical consent forms for its clients (e.g. children left during the summer play programme). These will be retained in a secure place upon the staff member's person during the course of the activity and then disposed of immediately once the child/children have been returned to their parent/guardian.

If working with a school group it is the expectation that the teachers will retain all medical consent.

Public Interest

OASES completes DBS check upon their staff every 5 years. The DBS Form is retained by the individual staff member. The DBS number is recorded upon Livedrive within OASES PROGRAMMES NEW – Management - OASES Personnel – DBS.

Legitimate Interest

Occasionally OASES may use Legitimate Interest as the lawful basis for collecting and using an individual's personal data. This allows the processing of the data when it is in the charity's legitimate interests, provided it does not override the rights and freedoms of the beneficiary. Currently, there are not explicit definitions of what is legitimate in every context. Legitimate Interest covers data collection for purposes such as:

- Network security;
- Fraud prevention;
- Maintaining existing client relationships;
- Direct marketing and more.

OASES believes that we have a Legitimate Interest in obtaining personal data under the following circumstances:

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

- If there is a need to demonstrate to funders the work that has been undertaken and provide an audit trail which can be validated.

If using Legitimate interest as the basis for data collection it is good practice to complete a Legitimate Interest Assessment (found within OASES PROGRAMMES NEW – Management – Data Protection – OASES GDPR & Data Protection Documents – Data Protection Template Forms – Assessment of Legitimate Interest Form) by:

1. Assessing whether a legitimate interest exists;

Is there a legitimate interest in processing the data?

Why is the data important to the objectives of OASES or the funder?

Have the legitimate interests been communicated to the beneficiary (e.g. specified on attendance registers)?

2. Establishing the necessity for processing the data;

Is processing the data really necessary or are there alternatives that can be used? Are there other ways to achieve the OASES or the funder's objectives?

3. Undertaking a balance of interests test.

Do the beneficiaries rights override the legitimate interests of OASES and/or the funder?

To ascertain the balance of interests ask the following:

- Would the beneficiary expect the data to be processed?
- Would the beneficiary share the same interest in the data being processed?
- Would the beneficiary come to any harm through the data being processed?
- Is the data sensitive?
- Is the legitimate interest a fundamental right?
- Will there be any impact upon the beneficiary if the data is processed?
- Are there controls in place to limit any negative impact on the beneficiary?

A beneficiary must be informed if their data is being collected under 'Legitimate Interest'.

The beneficiary has the right to object to their data being processed on the basis of legitimate interest. If a beneficiary objects the data must not be processed in this way (unless compelling legitimate grounds can be established e.g. taxation law).

USE

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

Any personal data collected by OASES can only be used for the declared purpose(s) (e.g. those stipulated by the 'Evidence of Consent') unless the data is required by law (e.g. taxation purposes). For example, if contact is established with a school through project delivery a separate consent form must be evidenced before the school can be contacted with general OASES promotional material. OASES staff should consequently endeavour to secure such consent during the lifetime of the project, when working directly with the individual staff member.

If personal data needs to be circulated (e.g. employee salary details within financial reports) the data should be anonymised.

Storage

OASES shall only store personal data if there is a legitimate reason for holding onto it. Care should be taken to ensure that data is only stored for the time period stipulated by law / for which the consent exists.

All data stored by OASES must be accurate and kept up-to-date. If OASES staff become aware of any changes in their own or others data they should alert the relevant Data Processor immediately.

All data must be tracked through the OASES Information Audit to enable ease of access and identification.

All OASES staff must follow the procedures of storage detailed in the OASES Information Audit.

The OASES Information Audit will be reviewed annually to ensure accuracy.

All data stored by OASES is backed up through our cloud based provider (Livedrive) on a continual basis. Livedrive also stores files so that previous versions of the same file are kept, enabling files to be downloaded or reverted.

Livedrive keeps all deleted files for 30 days, to enable document recovery from accidental deletion.

Office Storage

All data stored by OASES must be kept as up-to-date as possible.

The OASES registered offices are within Esh Winning Primary School. The school operates CCTV, but OASES would only have access to this information if it were required by law (e.g. if OASES experienced a theft and the Police requested the CCTV footage).

Access to the building can be restricted and entry to the OASES office is restricted.

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

Entry to the building is via an electronic sliding door. When the community facility (library) is open, the public have unrestricted access. When the library is closed entry can only be gained through the use of a key fob.

Access to the OASES office is restricted at all times. Entry can only be gained through the use of a key fob. Only OASES staff and the school (the Lettor) have such key fobs. The office itself is open-plan with direct views of the door. There are direct views in and out of the office to the outside world. The latter means that no data of a personal nature can be left visible within the office (e.g. on desks or display boards).

Paper copies of all personal data are to be kept in either the lockable filing cabinets (key held by the OASES CEO), the office walk in cupboard (key held by the OASES Office Manager) or the OASES CEO's lockable cupboard (key held by the OASES CEO).

Paper copies of all personal sensitive data are to be kept in the lockable filing cabinets (key held by the OASES CEO).

Paper copies of all personal data are to remain in the OASES office (the EWE Centre) at all times unless evidence of consent has been provided to allow its removal.

Electronic Storage

OASES use Esh Winning Primary School's server. This server is located within the school building. Access to the server is restricted by...

OASES owns several desktops, laptops, ipads for use by OASES staff. OASES staff are not allowed to use their own personal computing equipment for work purposes.

The OASES laptops and computers are protected by:

- Encryption – using Windows BitLocker. Wherever possible the TPM is also activated.
- Virus Software –

No sensitive personal data is held on ???.

No personal data is held on individual OASES computer or laptops.

Personal data IS held within the cloud-based system that OASES uses to store all OASES data. This cloud-based system is called LiveDrive. LiveDrive is operated from within the UK, is GDPR compliant and is password protected.

Hence, for someone to access the personal data stored electronically by OASES they must know the password to get onto the individual unit or the password of the Livedrive system. Passwords are changed every 6 months.

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

The OASES ipads do not carry any personal data but they are used for delivery purposes, which may involve data collection. No personal data collected (including photographs and film footage) can be collected without evidence of consent. Any data collected must be removed from the ipad (and stored appropriately, following OASES Data Protection guidance) as soon as possible and before subsequent use.

In order for OASES Staff to use their personal mobile phones to access work emails their phone must be deemed safe (by the Data Protection Officer) and password protected at all times.

Data Access

All data must be stored quickly, securely and in a manner that enables easy access to individual records.

All data storage must be tracked through the OASES Information Audit so that it can be identified and accessed quickly and easily.

Individuals have the right to access their data at any time and to request that it be updated or destroyed. OASES must comply with such requests within 1 month. All data must be stored in a format that can be copied onto a USB drive and given to the subject upon their request.

Data must be destroyed upon request unless there is a lawful basis for keeping the data (e.g. evidence for a court of law, taxation purposes).

No data can be passed onto a third party without the individuals consent / there is a case for legitimate interest.

Evidence of Consent

Evidence of consent must be stored in a specific 'OASES Evidence of Consent' file within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection – OASES Evidence of Consent. All evidence of consent must be dated upon entry.

Paper copies of all evidence of consent should also be made and placed within a lever arch 'Data Protection, Evidence of Consent' file. The latter is kept within the lockable office cupboard. All evidence of consent must be stored so that an individual's data can be easily re-traced:

Within the 'OASES Evidence of Consent' electronic file and the 'Data Protection, Evidence of Consent' paper file, separate sections will exist for:

- Personnel Data.
- Project data.

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

- CPD data.
- Schools data.
- OASES, Schools Outdoor Learning Network Member data.
- Photograph permission data.
- Miscellaneous contacts data.

Within these sections (in most cases) data will be stored alphabetically by School and then by an Individuals Forename – Surname (for more details see below).

- It is the responsibility of all staff to ensure that the correct evidence of consent exists before using a person's individual data.
- All staff must secure evidence of consent during their normal course of work following OASES policies and procedures for data collection (e.g. use of a correctly worded Privacy Notice).
- All staff must supply evidence of consent to the OASES Office Manager immediately for filing.
- All staff must store data according to the location specified in the OASES Information Audit.
- It is the responsibility of all Data Processors to ensure that the 'OASES Evidence of Consent' electronic file and the 'Data Protection, Evidence of Consent' paper files are kept up-to-date.
- It is the responsibility of all Data Processors to ensure that individual 'Project Data Consent Forms' exists, so that data can be traced and accessed whenever necessary.
- It is the responsibility of the Office Manager to ensure the data protection evidence of consent is stored as stipulated:

Personnel Data

The Personnel Data file within the Evidence of Consent folder on Livedrive contains all OASES staff, Board member, volunteer and Next of Kin consent forms. Each is stored under its relevant title (Staff; Board; Volunteer; Next of Kin) and then by Forename – Surname in alphabetical order and dated.

Actual data on staff is stored within the Personnel filing cabinet within the OASES office and upon Livedrive: OASES PROGRAMMES NEW – Management – OASES Personnel – Staff Details. For payment purposes staff details are also stored within SAGE.

Project Data

This file contains evidence of consent for the use of personal data to evidence project delivery. This evidence will be stored by Project. The evidence of consent itself will be stored by the activity (e.g. School, Volunteers, Family Events), and then by Forename – Surname in alphabetical order and dated.

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

Within each Project folder there will be a 'Project Data Consent Form' stipulating what personal data has been collected, why, how, where it is stored and for how long it can be kept. The data itself will also be stored by Project, within: OASES PROGRAMMES NEW – PROGRAMMES – **Project** – 0 Generic Materials – Project Delivery – Monitoring and Evaluation.

Data consent must either be obtained from the beneficiary, or the beneficiary made aware of OASES / the Funders 'Legitimate Interest' in holding their data (i.e. for Project monitoring, evidence of delivery and evaluation purposes). If this evidence exists the data can be used for reporting purposes. Reports containing personal data will be stored within: OASES PROGRAMMES NEW – PROGRAMMES – **Project** – 0 Generic Materials – *Project Reports*.

Once the data has been held for the time frame stipulated by the funder / commissioning agent (e.g. Charity, Local Authority, Organization) the relevant Project file and associated data will be deleted from all OASES systems along with the associated evidence of consent.

CPD Data

This file contains evidence of consent for OASES to process the personal data of course participants to enable them to gain course accreditation through One Awards and the NOCN.

For courses the Learner will complete the following which are kept on livesrie and in locked cupboards:

Sign in sheet - paper– name, school, email address

Booking Form – paper and electronic – name, school, email, car registration, dietary and medical, signature

Learner Portfolio – name, school, signature, names of other staff, photos

Monitoring & Evaluation- quotes, signature, name, school

Information sheet – paper copy or electronic-

The course participant data is held within Livedrive:

OASES PROGRAMMES NEW – PROGRAMMES – Accredited Active Learning – 0 Generic Materials –

OASES PROGRAMMES NEW – PROGRAMMES – Accredited Forest Schools – 0 Generic Materials –

OASES PROGRAMMES NEW – PROGRAMMES – CPD – 0 Generic Materials –

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

Learner Portfolios & OASES PROGRAMMES NEW – PROGRAMMES – Accredited Forest Schools – 0 Generic Materials – Learner Portfolios.

Course participant details can also be found within the Bookings section of the aforementioned files, stored by month of engagement.

Sharing of CPD data- Car registrations will be shared with venues including Forestry England and Ushaw.

Contacts including email addresses will be shared with Test and Trace.

Group emails will use 'bcc' so that email addresses are not shared with others.

Schools Data

This file contains evidence of consent for the use of personal data to contact school staff regarding OASES offers and promotions. This evidence will be stored by School and then Forename – Surname in alphabetical order and dated.

The data itself will be stored within a spreadsheet which can be found in OASES PROGRAMMES NEW – Administration – Master, Schools Contacts.

OASES, Schools Outdoor Learning Network Member Data

This file contains evidence of consent for the use of personal data to contact school staff regarding the OASES, Schools Outdoor Learning Network meetings, offers and promotions, credits. This evidence will be stored by School and then Forename – Surname in alphabetical order and dated.

The data itself will be stored within a spreadsheet which can be found in OASES PROGRAMMES NEW – Promotion – OASES, Schs Outdoor Learning Network – OASES Network Member Spreadsheet

Photograph Permission Data

This file within Livedrive contains all of the evidence of consent for any photographs taken. The evidence will be stored by Project and labelled in a similar manner to the photograph itself, to enable ease of access e.g. EoC SGP, Pittington Sch. Council 2.3.18. The photographs themselves will be stored within the individual Project file under OASES PROGRAMMES NEW – PROGRAMMES – **Project** – 0 Generic Materials - Images.

Each photograph will be labelled with the content and dated, according to when it was taken e.g. Pittington Sch. Council 2.3.18. **On no account will children's names be used when labelling.** Only photographs that have the necessary evidence of consent will be stored.

Good photographs, with permission to be used for marketing purposes, will be stored within *OASES PROGRAMMES NEW – Promotion – IMAGES*. Within this folder they will be This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

separated into *Photography for print only* and *Photography with full usage* dependent upon the consent provided.

The Office Manager will maintain a separate spreadsheet within which will record the photographs submitted, in chronological order, so that images of children can be identified and disposed of after 5 years. This spreadsheet can be found within: *OASES PROGRAMMES NEW – Promotion – IMAGES – OASES Photography Permission Spreadsheet*.

A paper file will also be kept of any images taken. These photographs and the associated evidence of consent will be labelled as described above (to enable ease of tracking) and annotated.

The template for photography evidence of consent is stored within: *OASES PROGRAMMES NEW – Administration – TEMPLATE Forms – Photo Consent*.

Miscellaneous Contact Data

This file contains evidence of consent for areas of activity not previously listed. This evidence will be stored in alphabetical order and dated.

The contents of this file will be reviewed on an annual basis to determine if a new, separate 'Data File' should be created.

The data is stored within a spreadsheet placed within OASES PROGRAMMES NEW – Administration – CONTACTS - Miscellaneous Contacts.

Disposal

Once evidence of consent has been given, unless time limited (as determined by the Evidence of Consent Form; the Privacy Notice or by Law) it will be assumed that it will remain in place.

If an individual withdraws their consent their data will be removed from the OASES I.T. systems immediately and any paper copies will be shredded.

Data Holding Periods

Staff data shall be removed from the OASES systems upon termination of their Employment Contract unless they have stated otherwise through the OASES Staff Data Consent Form.

Project delivery evidence shall be held for 3 years upon project completion, unless otherwise stipulated by the funder.

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

Images of children that are 5 years old will be automatically removed from the OASES I.T. systems, website, social media etc. immediately and any paper copies will be shredded unless the individual gives express, written evidence of consent to retain use.

Evidence of all financial transactions will be kept for 7 years, or as stipulated by HMRC.

Evidence of all course materials (e.g. Learner Portfolios) and associated personal data will be kept for 7 years, as required by One Awards / NOCN.

OASES Personnel & Data Protection

OASES Staff Responsibilities

The need for staff compliance with the GDPR and Data Protection Laws is stated within individual **employment contracts**, ensuring that staff are aware of their lawful obligations to protect an individual's data. Individual employment contracts and **Job Descriptions** also stipulate whether or not individual staff members are **Data Processors** or **Data Controllers**.

Most OASES staff are **Data Processors** *'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'*

The OASES CEO and the OASES Board are the Data Controllers for OASES. A **Data Controller** is *'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'*

All staff have an obligation to follow the OASES data protection systems and policies, to ensure client confidentiality and protection. Failure to comply with the data protection systems and policies laid down by the OASES Data Controllers will mean that individual staff assume personal liability (and may be fined accordingly, by the ICO, if a data breach occurs) and may be subject to disciplinary procedures.

As Data Processors, all OASES staff must inform the Data Controllers if they believe that OASES is processing data in a manner that breaches the GDPR or the Data Protection Bill. They must also immediately inform the Data Controllers if a Data Breach occurs.

All staff will receive specific training in Data Protection and GDPR compliance:

- Through the OASES induction process.
- Whenever there are changes to the laws governing data protection.

During the monthly Team Meetings data protection and GDPR compliance will be discussed under OASES Policies and Procedures, as a regular article.

OASES Board Responsibilities

The OASES Board are responsible for ensuring that OASES follows data protection law.

All Trustees will receive specific training in Data Protection and GDPR compliance:

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

- Whenever there are changes to the laws governing data protection.
- During the Quarterly OASES Board meetings, as a regular article.

OASES Volunteer Responsibilities

The need for volunteer compliance with the GDPR and Data Protection Laws is stated within the OASES individual **Volunteer Guidance** document, ensuring that all volunteers are aware of their lawful obligations to protect an individual's data. Volunteers are **Data Processors** but shall only process personal data under the direct supervision of a OASES member of staff.

All volunteers have an obligation to follow the OASES data protection systems and policies, to ensure client confidentiality and protection. Failure to comply with the data protection systems and policies laid down by the OASES Data Controllers will mean that individual volunteer assume personal liability (and may be fined accordingly, by the ICO, if a data breach occurs).

As Data Processors, all volunteers must inform their supervisor if they believe that OASES is processing data in a manner that breaches the GDPR or the Data Protection Bill. They must also immediately inform their supervisor if a Data Breach occurs.

All volunteers will receive specific support in Data Protection and GDPR compliance from their supervisor.

OASES Staff Data

Only data required by law is kept on OASES staff unless explicit consent is given by the individual.

During the OASES staff induction process all staff are supplied with a **OASES Personnel Details Record Form** and a **OASES Staff Data Consent Form**.

The **OASES Personnel Form** - collects data about the staff member (Name, Address, Contact details, Next of Kin details, Bank Account Details, NI) necessary for human resource management, payroll and staff safety.

The **OASES Staff Data Consent Form** - details the type of data that OASES may wish to / have to hold on each staff member and for what purpose. Individual staff can then elect to allow OASES access, unless the data is deemed necessary by law (e.g. HMRC).

Data pertaining to individual staff is held upon the OASES staff systems for:

- the duration of their employ
- for 6 months beyond or
- indefinitely

As stipulated by the employee on the **OASES Staff Data Consent Form**, unless OASES is required to hold onto their data for longer by law (e.g. 7 years for HMRC).

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

The personal data of OASES staff is protected as follows:

- Paper copies are filed within the personnel filing cabinet which is locked. The key is held by the OASES CEO. The filing cabinet is located within the OASES office. The office itself is key fob protected.
- Electronic data pertaining to OASES staff only to exist upon password protected I.T. equipment and is stored upon Livedrive, a password protected cloud based storage system (see Data Storage).
- The personal data of staff is not removed from the office without prior consent of the individual concerned (e.g. consent is provided on the **OASES Staff Data Consent Form**).

OASES Staff Next of Kin

For health and safety reasons we ask that we are notified of OASES next of kin and that this information be placed upon the **'EWE Centre Staff Contact Information'** sheet for the duration of their employ. To include the personal details of the OASES staff members next of kin we require their next of kin's consent. All staff are issued with a **'Next of Kin Data Consent Form'**. If the next of kin consents then their personal data will be included within the **'EWE Centre Staff Contact Information'** sheet.

OASES Board Data

Only data required by the Charity Commission and Companies House is kept on OASES Board members, unless explicit consent is given by the individual.

Upon agreeing to be a Trustee all OASES Board members will supply a **OASES Trustees Information Form**. The information on this form is used to register the Trustee with the Charity Commission. Paper copies of this form are stored in the CEO's lockable cupboard (key held by the OASES CEO). Electronic copies of this form are password protected and stored upon Livedrive.

OASES Volunteer Data

Only data required by law is kept on OASES volunteers unless explicit consent is given by the individual.

During the OASES volunteer introduction all volunteers are supplied with a **OASES Volunteer Guidance** document, a **OASES) Volunteer Details Form** and a **OASES Volunteer Data Consent Form**.

The **OASES) Volunteer Details Form** - collects data about the volunteer (Name, Address, Contact details, Next of Kin details, Bank Account Details, NI) necessary for human resource management, mileage payments and safety reasons.

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

The **OASES Staff Data Consent Form** - details the type of data that OASES may wish to / have to hold on each volunteer member and for what purpose. Individual volunteers can then elect to allow OASES access, unless the data is deemed necessary by law (e.g. HMRC).

Data pertaining to individual volunteers is held upon the OASES staff systems for:

- the duration of their volunteering
- for 6 months beyond or
- indefinitely

As stipulated by the employee on the **OASES Volunteer Consent Form**, unless OASES is required to hold onto their data for longer by law (e.g. 7 years for HMRC).

The personal data of OASES volunteers is protected as follows:

- Paper copies are filed within the personnel filing cabinet which is locked. The key is held by the OASES CEO. The filing cabinet is located within the OASES office. The office itself is key fob protected.
- Electronic data pertaining to OASES volunteers only to exists upon password protected I.T. equipment and is stored upon Livedrive, a password protected cloud based storage system (see Data Storage).
- The personal data of volunteers is not removed from the office without prior consent of the individual concerned (e.g. consent is provided on the **OASES Volunteer Consent Form**).

Data Breach

Data Breach – ‘A breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (i.e. it is more than just losing personal data).’

If a data breach is detected the OASES CEO and the OASES Board must be informed immediately. The OASES CEO and the OASES Board must investigate any data breaches to ascertain:

- What data has been breached and how sensitive the data is.
- How the data breach has occurred.
- The likelihood that the breach will lead to a risk to the rights and freedoms of an individual.
- Who needs to be informed about the data breach.
- How to prevent any future data breach from occurring.

Reporting Data Breaches

If the data breach is likely to result in a risk to the rights and freedoms of an individual(s) (e.g. it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage) the OASES CEO must report it to the following agencies:

- The Charity Commission - www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity.
- The ICO - www.ico.org.uk/for-organisations/report-a-breach/. OASES must inform the ICO within 72 hours if a data breach of this nature occurs. Failure to do so can result in a fine.
- The individual at risk.

OASES Data Risk

OASES does not hold very much data that presents a risk to the rights and freedoms of the individual (e.g. it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage). Staff bank account details and medical information are the primary area of risk. All paper documents pertaining to staff bank account details and medical information shall remain in the OASES office at all times and be stored in the lockable filing cabinet. Only staff with the appropriate authority shall have access to these documents. Where an electronic version is

This policy document and other Data Protection and the GDPR documentation (including template forms) can be found within Livedrive: OASES PROGRAMMES NEW – Management – Data Protection

kept it should be password protected and only stored on a OASES device which is encrypted.

Data Protection by Design and Data Protection Impact Assessments

OASES does not deal with data that is of high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

Hence does not require a Data Protection by Design and Data Protection Impact Assessments.

Data Protection Officer

Although OASES does not have to formally designate a Data Protection Officer as it is not:

- A public authority
- An organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
- An organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions

In the interests of best practice the Advisor for Sustainability Education, will act as the OASES Data Protection Officer.