DATA PROTECTION & GDPR POLICY

SEPTEMBER 2023

7 Doman Road, Camberley, Surrey. GU15 3DN
t. 01252 514999 **e.** info@overworld-amp.uk **w.** www.overworld-amp.uk

Contents

Policy Statement

To operate efficiently the Organisation is required to collect and use information about people with whom it works and the children and young people we provide a service to.

These may include members of the public, current, past, and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information to comply with the requirements of central Government.

The Organisation

- ✓ Is committed to ensuring personal data is responsibly managed and that it ensures compliance with current data protection legislation.
- ✓ Will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.
- ✓ Ensure Any person who handles personal data on behalf of the organisation (including all staff) must comply with this policy paying attention to the overarching data protection principles and the more detailed General Data Protection Regulation (GDPR) for the Organisation to comply with the applicable laws

All organisations that handle personal information are required to comply with the eight principles of Data Protection:

- ✓ Fairly and lawfully processed
- ✓ Processed for limited purposes
- ✓ Adequate, relevant, and not excessive
- ✓ Accurate and up to date
- ✓ Not kept for longer than is necessary
- ✓ Processed in line with your rights
- ✓ Secure

Not transferred to other countries without adequate protection

Scope

This Policy applies to

- All employees, agencies, contractors, volunteers, and temporary staff working for or on behalf of the Organisation.
- All personal data created or held by the Organisation in whatever format (e.g., paper, electronic, email, or other) and however it is stored, (for example ICT system/database, shared drive filing structure, workbooks, email, filing cabinet, shelving, and personal filing drawers).
- Personal data is information about living, identifiable individuals, or an identifier or identifiers that can be used to identify a living individual. It covers both facts and opinions about the individual. Such data can be part of a computer record or manual record.

Current data protection legislation does not apply to access to information about deceased individuals. However, the duty of confidentiality may continue after death.

Responsibilities

The Managing Director, Mark Pickering and the Chief Operating Officer, Simon Bradley have overall responsibility for ensuring that the Organisation meets the statutory requirements of any data protection legislation and overall responsibility for information management issues.

The Senior Managers ensure compliance with data protection legislation and this policy within the day-to-day activities of the Organisation.

All staff must read, understand & follow this policy & its procedures.

Any information and data held by agencies or contractors in relation to the Organisation, are responsible for their own compliance with data protection legislation and must ensure that personal information is kept and processed in line with data protection legislation.

Data Protection Principles

1. ***Lawfulness, Fairness & Transparency***

   "(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency'); - *Information Commissioner's Office*

   The first principle defines that data should be processed lawfully, fairly, and transparently.

   The data must be collected and processed on valid grounds (also known as a lawful basis), and the data should not be used for anything that breaks any laws (lawful). It must also be used in a way that does not unfairly affect the individual, such as by misleading them (fair). Finally, from the start of the process to the end, the data handler must be entirely open and honest about how the personal data is being used (transparent).

2. ***Purpose Limitation***

   "(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');" - *Information Commissioner's Office*

   The second principle defines that the use of data should be limited to the initial intended purposes.

This means being transparent and explaining from the start what the intended purposes are for using this data, and not straying from these purposes when using the data. This includes keeping a specific record of the intended purpose.
There are circumstances where you may be allowed to use the data for other purposes. These circumstances are:

- The new purpose is relevant to the initial purpose
- You receive new consent from the individual for the new purpose
- There is a legal obligation that requires you to use the data for a new purpose
- Archiving purposes that are in the public interest
- Purposes for historical or scientific research
- Statistical purposes

3. *Data Minimisation*

"(c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');" - *Information Commissioner's Office*
The third principle defines that the minimum amount of data required to carry out the intended purpose should be identified prior to collection, and then only this data is collected and processed.

Website contact forms are a fitting example. For a contact form, you typically only need:

- Name
- Email
- Phone
- Comments

That is because the "purpose" of the contact form is to enable and encourage people to contact you. Once you are in a conversation with the user and they transition from being an "enquiry" to a "lead" or "customer," you can ask for additional information as part of the client onboarding process.
Regular data audits are a key step to help ensure you are only ever asking for personal data that you absolutely need.

4. *Accuracy*

"(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay ('accuracy'); - *Information Commissioner's Office*

The fourth principle defines that an effort should be made to ensure the data you store, or process is accurate and up to date.
If information is misleading or incorrect, every measure should be taken to update and correct it, or to have it redacted and erased. For example, if someone has moved house, it may be necessary to update the data you hold

to reflect their new location or remove this information from the data base if you no longer have business with this person.

5. Storage Limitation

"(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');" - *Information Commissioner's Office*

The fifth principle defines that data should not be stored for longer than is required for the intended purposes.

The length of time the data is kept should be identified and justified prior to collection, with it then not being held for longer than this period. This should be regularly reviewed, erasing data where appropriate, plus individuals have the right to request erasure of their data if you no longer need it.

Exceptions to this include:

- Archiving data for purposes in the public interest
- Archiving data for scientific or historical research purposes
- Archiving data for statistical purposes

These exceptions are subject to safeguards that may be required to protect the individual, such as anonymisation or pseudonymisation.

6. Integrity & Confidentiality (Security)

"(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 ('integrity and confidentiality')." - *Information Commissioner's Office*

The sixth principle defines that data should be processed with integrity and should have the optimum protection from unauthorised access, ensuring it remains confidential where appropriate.
The necessary security measures should be in place to ensure data in your possession is not compromised accidentally or by an unauthorised person, be that lost, altered, or deleted.

Accountability

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')." - *Information Commissioner's Office*

Finally, these principles are underpinned by accountability; you must be accountable and responsible for compliance with the UK GDPR and its principles. It is on the data holder to ensure measures are taken to protect data.

The measures you can take include:

- Having data protection policies
- Having contracts and keeping records with external organisations who manage any data for you
- Maintaining records of your data processing activities
- Having necessary data security measures
- Recording and reporting
- g personal data breaches
- Assessing data protection impact for use of personal data where there are risks to the individual
- Having a dedicated data protection officer
- Signing up to certification schemes and following codes of conduct where necessary

The Organisation is responsible for and must be able to demonstrate compliance with the data protection principles listed above.

- the data shall be processed in accordance with the rights of data subjects.
- Personal data shall also not be transferred to a country unless that country or territory ensures an adequate level of data protection, or another secure method of transfer is guaranteed.

Notification

The Digital Economy Act 2017 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which the Organisation must be registered. The Organisation will review the Data Protection Register annually, prior to renewing its notification to the Information Commissioner, (https://ico.org.uk/esdwebpages/search).

Privacy Notices – see Appendix 2

Whenever information is collected about individuals, they must be made aware of the following at that initial point of collection:

- The identity of the data controller (The Organisation);
- Contact details of the Data Protection Officer;
- The purpose that the information is being collected for;
- Any other purposes that it may be used for;
- What the lawful basis is for processing the data;
- Who the information will or may be shared with;
- If the data is transferred outside of the EU, and if yes, how is it kept secure;
- How long the data will be kept for; and
- How data subjects can exercise their rights.

The Organisation will review its Privacy Notice annually and alert young people, parents, and other users to any updates.

Conditions for Processing

Processing of personal information may only be carried out where one of the conditions of Article 6 of the GDPR (Lawfulness of processing) has been satisfied.
Processing of special category (sensitive) personal data may only be carried out if a condition in Article 9 of the GDPR is met as well as one in Article 6. 8.

- Explicit consent
- Employment, social security, and social protection law
- Vital interests
- Not-for-profit bodies
- Made public by the data subject
- Legal claims and judicial acts
- Substantial public interest conditions
- Health or social care
- Public health
- Archiving, research and statistics

Data Protection Officer

The Company shall appoint a Data Protection Officer in line with the requirements of the GDPR, this will be the Chief Operations Manager, Simon Bradley.

Data Protection Impact Assessments

The Organisation will undertake risk Data Protection Impact Assessments where there is occasion that data is required in line with the requirements of the GDPR and as per the Information Commissioner's Office (ICO) guidance.

Data Breaches

Whenever a data breach or security alert is found, this must be immediately reported to the HR Administrator. In accordance with all data breaches and security alerts this will be passed onto the ICO in line with requirements of the GDPR and appropriate actions will be taken to minimise any issues that could arise.

Consent

Where data is processed for the use of marketing or streaming (for example within the company website, photographic image, or voice commentaries) it will ensure that the consent is freely given, specific, informed, and unambiguous, and the consent is recorded.

Direct Marketing

Where direct marketing is used (the promotion of aims and ideals as well as selling goods and services) via electronic communications e.g., email, SMS text, fax, or recorded telephone messages, it will only do so if the recipient has given explicit consent to receive them e.g., has ticked a box to 'opt in.'

Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause.
Relevant, confidential data should only be given to:

- Other members of staff on a need-to-know basis;
- Relevant Parents/Guardians;
- Other authorities if it is necessary in the public interest, e.g., prevention of crime, safeguarding;
- Other authorities, such as the Local Authority and schools to which a CYP is attending or referred from, and where there are legitimate requirements.

The Organisation will not disclose any recorded data in relation to a CYP which would be likely to cause harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records. Where there is doubt, or statutory requirements conflict, legal advice should be obtained. Where there are safeguarding concerns, the matter should be referred to the Designated Safeguarding Lead (DSL). When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she/they is likely to know the answers. Information should not be provided to other parties, even if related.

The Individual's Rights

Any person whose details are held by the Organisation is entitled to ask for a copy of information held about them (or for a CYP they are responsible for). They are entitled to see if the data held are accurate, and who it is shared with. When a request is received it must be dealt with promptly; a response must be provided as soon as possible and within one month.

Provision of Data to a child or young person (CYP)

In relation to the capacity of a CYP to make a subject access request, guidance provided by the Information Commissioner's Office has been that by the age of 12 a young person can be expected to have sufficient maturity to understand the nature of the request. A CYP may of course reach sufficient maturity earlier; each CYP should be judged on a case-by-case basis. If the CYP does not understand the nature of the request, someone with parental responsibility for the CYP, or a guardian, is entitled to make the request on behalf of the CYP and receive a response.

Parents' Rights

An adult with parental responsibility can access the information about their CYP, if the CYP is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the Organisation is entitled to request relevant documentation to evidence this as well as the identity of the requestor and CYP. The Organisation has the right to ask the CYP if they object to release of information to the Parent if the CYP is deemed mature enough to make such a decision.

Information Security

All members of staff should be constantly aware of the possibility of personal data being seen or accessed by unauthorised personnel. For example, possibilities may arise when computer screens are visible to the public; files may be seen by the cleaners if left on desks overnight (all papers must be locked in cabinets when not in use).

The use of computer passwords is a requirement of the Organisation to avoid unauthorised access. All personal removable devices such as laptops, USB sticks, mobile phones and digital cameras must not be used to store data unless they are encrypted, and complex password protected wherever possible.

Staff and visitors are not permitted to use their own devices for recording purposes unless with agreement from the Managing Director. Any recording by staff must be for work related matters and once complete transferred to a work owned device and the original recording deleted from their device.

Parents while using the Organisation's premises may only record their own CYP or when other parental permission given e.g. birthdays or events.

Members of staff if required to work away from the premises (at home) must ensure that any work device or paper file is secure while in their person. No personal data is ever to be left unattended off site e.g., in a car overnight, on view to family members when working at home.

All members of staff should take care when emailing personal data and always check the email address is correct and the right attachment has been attached. When copying to several people externally, all members of staff should always use the BC field and not the CC field or create a group.

Maintenance of Up-to-Date Data

Out of date information should be discarded if no longer relevant. Information should only be kept if needed, for legal or business purposes. Most relevant information should be kept for the period during which the person is associated with the Organisation plus an additional pre-determined period. The Organisation will hold a record of retention and disposal, see Appendix 1

Inaccurate Data

If an individual complains that the personal data held about them is wrong, incomplete, or inaccurate, the position should be investigated thoroughly including checking with the source of the information. This must be answered within one month. In the meantime, a caution should be marked on the person's file that there is a question mark over the accuracy. An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

Recording of Data

Records should be kept in such a way that the individual concerned can inspect them. It should also be remembered that at some time in the future the data may be inspected by the courts or some legal official. It should therefore be correct, unbiased, unambiguous, factual, and clearly decipherable/readable.

Photographs and Recorded Imagery

Whether or not a photograph comes under the data protection legislation is a matter of interpretation and quality of the photograph. However, the Organisation will seek to obtain parents' permission for the use of photographs outside of the centre and to record their wishes if they do not want photographs to be taken of their CYP, see Appendix 3

Breach of the Policy

Non-compliance with the requirements of data protection legislation by the members of staff could lead to serious action being taken by third parties against the Organisation. Non-compliance by a member of staff would therefore be considered a disciplinary matter which, depending on the circumstances, could lead to dismissal without notice. It should be noted that an individual can commit a criminal offence under the law, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the data controller.

Further Information

Further advice and information about data protection legislation, including full details of exemptions, is available from the ICO website at www.ico.org.uk,

Appendix 1: Data Retention and Disposal of Records Policy

Introduction

Records are defined as all those documents which facilitate the business carried out by the Organisation and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received, or maintained in hard copy or electronically.

Records provide evidence for protecting the legal rights and interests of the organisation and provide evidence for demonstrating performance and accountability.

Policy Statement

The Organisation must manage records effectively and in compliance with the General Data Protection Regulations (GDPR). As an organisation we collect, hold, store, and create significant amounts of data and information and this policy provides a framework of retention and disposal of categories of information and documents. This documents the framework through which this effective management can be achieved and audited.

This policy applies to all records created, received, or maintained by employees of the Overworld organisation while carrying out its functions.

Aims

To support members of the Organisation to:

- ✓ Efficiently and effectively store records and information;
- ✓ Preserve the confidential nature of the records and information stored;
- ✓ Use a secure record system;
- ✓ Respect privacy and disclosure
- ✓ Access the records appropriately and efficiently

Responsibilities

Mark Pickering, Managing Director & Simon Bradley, Chief Operations Manager hold ultimate responsibility for the retention of and ultimate destruction of records.

Individual staff and volunteers must ensure that records for which they are responsible are accurately maintained and safely stored

Retention of Records

The Organisation's retention periods are driven by legislation and/or business need. We assign clearly defined retention periods to our information to ensure it is kept for the appropriate length of time.

Each retention period has three elements:

- Trigger – the action which begins the retention period (e.g., 'End of Financial Year,' 'End of Employment,' 'No longer associated with the Organisation')
- Retention period – the length of time the information will be kept

- Action – either 'review' or 'destroy'
    - If the action is 'review' the information must be reviewed to ensure it is no longer required before destruction. Outcomes of a review may be – dispose, mark for permanent preservation, or temporary extension to review again at a future date
    - If the action is 'destroy,' this means the information can be destroyed without being reviewed in line with procedure.

Reviewing and Closure of Records

- Closure - no further papers can be added but the file can be used for reference.
- Manual records should be closed as soon as they have ceased to be of active use other than for reference purposes.
- When a file is due to be closed the appropriate member of staff should review the file and consult the schedule marking the front cover of the file to indicate the date on which the file can be destroyed, or whether it should be selected for permanent preservation or retained by the Organisation for research or litigation purposes.
- Minimum Retention Period required for each type of record is calculated from the point the file/record is closed
- Information should only be retained beyond its retention period in limited circumstances. When conducting a review, the following factors should be considered:
    - Is the information required to fulfil statutory or regulatory requirements?
    - Is the information relevant to ongoing litigation / subject to a legal hold?
    - Is the information the subject of an information request or relate to information recently disclosed in a response?
    - Is retention required to evidence events in the case of a dispute?
    - Does the information fall under the selection criteria for permanent preservation and transfer to the National Archives outlined in the Selection and Appraisal Methodology?
    - Is the information required for a Public Inquiry?
    - Is there another demonstrable business need for retaining the information?
    - If the information is deemed to still be required, an extension of two years is given, the information needs to be reviewed again at the end of the extension. The retention period must not be extended indefinitely.

Destroy

Where the disposal action is 'Destroy' the records should be kept for the period stated and then destroyed by in accordance with the directions on recycling and shredding.

All records containing personal information, or sensitive policy information, should be made either unreadable or un-reconstructable before destruction

Authorisation must be given by the Managing Director

The Freedom of Information Act 2000 requires a record containing what has been destroyed, when it was destroyed and the individual who authorised the destruction. The HR Administrator completes and maintains this

Records should be destroyed with the level of security required by the confidentiality of their contents. For example, if records containing special category data or protectively marked papers have been shredded, the shredded paper should be handled securely and not dumped

Records awaiting destruction must be stored securely. Paper records should be placed into the confidential waste bins and documents stored on electronic systems should be deleted, including back-ups. Deletions should be carried out by someone with appropriate access to the system from which they are being deleted

Digital documents should be deleted and not overwritten. When information is destroyed, all copies of the information should be destroyed at the same time (both digital and physical). Information cannot be considered to have been completely destroyed unless all copies have been destroyed as well.

Permanent Preservation

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to an archive. A database of the records sent to the archives is maintained by the HR Administrator.

The appropriate staff member, when archiving documents should record in this list the following information: -

- File reference (or another unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

Transferring Information to Other Media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

Retention and Disposal Schedule

Our Retention and Disposal Schedule sets out our retention periods. Information must be kept for the length of time defined in the Schedule unless there is a legal requirement to destroy it sooner. The records contained within these functional areas provide evidence and information about its business activities that are important for the efficient operation of the Organisation.

Business management/Administration			
Document type	Retention period	Trigger	Action
Agendas for and minutes from Director's meetings	Permanent	Meetings commonly refer to confidential issues relating to the business and staff and may be required retrospectively.	Signed originals should be kept as a paper version. Director meeting minutes file
Reports presented to Directors	Permanent	Reports may contain confidential information relating to individuals and business	Signed originals should be kept as a paper version. Director Report file
Business plan created and administered by the Overworld organisation	Retained for operational use and reference	Until superseded or whilst relevant	Secure Disposal Electronic and paper versions
Policy documents administered by the Overworld organisation	Retained for operational use and reference	Until superseded or whilst relevant.	Secure Disposal Electronic and paper versions
Records relating to complaints dealt with by the Overworld organisation	Six years after the resolution of the complaint then review need to retain for a further six years	Disputes may be reinitiated. Status of dispute must be reviewed before deletion	Secure Disposal Electronic and paper versions
Business correspondence with LEA/placing school/associated professionals to include minuted meetings	Retain for six years	From the end of the partnership Legal and business reasons/LGA Retention	Secure Disposal Electronic and paper versions
Correspondence and general filing created by Managing Director and other members of staff with administrative responsibilities	Destroy after 5 years if there is no further action or addition	No further action or addition.	Secure Disposal Electronic and paper versions
Business related correspondence, written and electronic between staff.	Destroy after 3 years	If no longer relevant	Secure Disposal Electronic and paper versions
Correspondence with the public or external organisations which cannot be linked and stored with other records relating to a specific process and there is no	Destroy after 5 years if there is no further action or addition	No further action or addition. If closed, and new activity begins. A new volume of the file should be created, and the retention period of the old volume be	Secure Disposal Electronic and paper versions

identified process or function in the Retention Schedule. • Letters • Emails • General Correspondence/files		brought into line with the new volume.	
Unstructured Records that do not support a business process i.e. No existing place for them in a filing structure and none will be created. (Paper and electronic including emails) • Compliment slips • Catalogues • Trade journals • Suppliers Promotional material • Course/seminar/ conference invitations • Trivial messages or notes that are not related to business • Requests for stock information • Advertising material • Out of date distribution list	Destroy as soon as any use has ceased		Standard Disposal
Overworld TAPP Prospectus	Retained for operational use and reference	Until superseded or whilst relevant.	Secure Disposal Electronic and paper versions
Visitors' books and signing in sheets	Current year + 6 years		Secure Disposal Electronic and paper versions

Strategy Communications and Marketing			
Document type	Retention Period	Trigger	Action
Strategy - Communications & Marketing Records relating to customers: • Customer database • Sign up to subscribe • Competition entries	Retain while current. Retained for 1 month	Until recipient unsubscribes	Secure Disposal Electronic and paper versions
Strategy - Communications & Marketing, Records relating to Business Sponsorship and all advertising	Retain for 6 years	From date of sponsorship and renewed sponsorship Limitation Act 1980	Secure Disposal Electronic and paper versions
Strategy - Communications & Marketing, Records relating to Corporate Marketing database	Retain for 6 years	From year records created Limitation Act 1980	Secure Disposal Electronic and paper versions
Strategy - Communications & Marketing, Records relating to Public Relations and interaction with the media: • Records of events including • Photographs depicting identified individuals • Video & audio digital files • Press releases • Correspondence	Retain for 6 years unless of historical value which is archived	From date of event	Secure Disposal Electronic and paper versions
Strategy - Communications & Marketing, Records relating to the development and promotion of Local Authorities Campaigns and events	Permanent if significant event. Retain 7 years if minor campaign or event	From date of event	The National Archives Retention Guidance 2012 Secure Disposal Electronic and paper versions

Children and Young People (CYP)			
Document type	Retention period	Trigger	Action
Monitoring forms/reports	Date of birth of pupil + 22 years	Data protection Regulation Unless child protection applies, in which case retain for 25 years from DOB;	Secure Disposal Electronic and paper versions
Child protection information held on safeguarding file (paper)	Held on secured file until pupil reaches 25 years of age	Keeping children safe in education Statutory guidance for schools and colleges Working together to safeguard children.	
Child protection information held on safeguarding file (electronic)	Until young person reaches 25 years of age. Principal copy with the appropriate local authority.	Keeping children safe in education Statutory guidance for schools and colleges Working together to safeguard children.	
Attendance Register	Three years after the end of the academic year	Guidance provided by Pupil Registration Regulations 2006. Regulation 14	
Educational Health and Care Plan	Date of birth of pupil + 22 years		
Individual Risk Assessment	Date of birth of pupil + 22 years	Reviewed and updated	
Images of CYP - signed consent forms by parent / guardian	Date of signing + 5 years; or at end of project; or when young person no longer attends Overworld	Images should not be reused outside of the time period or for other projects other than that specified on the form	
Any other records created in the course of contact with CYP maintained for Overworld's own use	Current year + 3 years	Review information held and either allocate further retention period or destroy	

Parent/Guardian			
Document type	Retention period	Trigger	Action
Correspondence with parent/guardian	6 years	From the end of the partnership Legal and business reasons/LGA Retention	Secure Disposal Electronic and paper versions
Formal minuted meetings with parents/guardians	6 years	From the end of the partnership Legal and business reasons/LGA Retention	
Parental/Guardian personal information. • Contact details • Address • Email address • Written consent	6 years	From the end of the partnership Legal and business reasons/LGA Retention	

Human Resources			
Document type	Retention period	Trigger	Action
Interview notes and recruitment records (including pre-employment vetting information) *unsuccessful candidates*	Date of interview + 1 year	Employment not offered	Secure Disposal Electronic and paper versions
Interview notes and recruitment records (including pre-employment vetting information) • *successful candidates*	End of employment + 7 years	End of employment	All recruitment information to be added to staff personnel file, except DBS checks. Secure Disposal Electronic and paper versions, end of employment +7 years.
Pre-employment vetting information • successful candidates' DBS checks	Maximum of date of check + 6 months	No requirement to retain copies of DBS certificates. NOT be retained for longer than 6 months	Secure Disposal Electronic and paper versions
Staff files (main personnel file)	End of employment + 7 years	End of employment Limitation Act (1980)	
Record of child protection allegation made against staff	For Substantiated, False, Unsubstantiated and Unfounded Normal retirement age + 10 years	If found to be malicious destroy immediately after investigation.	
Staff appraisal / assessment records	Current appraisal + 6 years	On going	
Staff timesheets	Current year + 6 years	Financial regulations	
Staff sickness records, excluding ill-health referrals (self-certification, doctor's certificates)	Current year + 3 years	On going	
Staff sickness records • ill health referrals	End of employment + 7 years	Limitation Act (1980) Add to main personnel file	
Staff maternity and paternity pay records	Current year + 3 years	Statutory Maternity Pay Regulations (1986) (as amended	
Disciplinary proceedings • warnings	End of employment + 7 years	Limitation Act (1980 Add to main personnel file	
Disciplinary proceedings substantiated or unsubstantiated	a) outcome letter: end of employment + 7 years b) all other records: close of case + 7 years	Limitation Act (1980 Add to main personnel file	
Disciplinary proceedings • false or malicious	a) outcome letter: end of employment + 7 years b) all other records: shred at close of case	Limitation Act (1980 Add to main personnel file	

Disciplinary proceedings safeguarding / child protection related	Until normal pension age, or for 10 years from date of allegation, whichever is longer	DfE 'Keeping Children Safe in Education' guidance (regularly updated)	
Records of industrial tribunals, disciplinary panels, appeals	7 years from end of process	Limitation Act 1980 can apply Outcome letter add to main personnel file	
Records held under Retirement Benefits Schemes	End of employment + 7 years	(Information Powers) Regulations 1995	

Insurance and certification			
Document type	Retention period	Trigger	Action
Employers' liability certificate	Permanent	Permanent while business is operational	Destroy as confidential waste or delete securely from electronic systems once business closes
Policy Schedules and Documentation	Three years after policy termination	Commercial requirement	Secure Disposal Electronic and paper versions
Correspondence relating to claims	Three years after settlement	Commercial requirement	Secure Disposal Electronic and paper versions

Financial			
Document type	Retention period	Trigger	Action
Business correspondence with LEA/placing school/associated professionals	Retain for six years	From the end of the partnership	Legal and business reasons/LGA Retention Destroy as confidential waste or delete securely from electronic systems
Business correspondence with parent/guardian	Retain for six years	From the end of the partnership	Legal and business reasons/LGA Retention Destroy as confidential waste or delete securely from electronic systems
Annual accounts including payroll	Six years from year of accounts	Requirement of HMRC and the DfE academies financial handbook	Secure Disposal Electronic and paper versions
Loans and grants	12 years from last payment of loan then review annually	Requirement of HMRC and the DfE academies financial handbook	Secure Disposal Electronic and paper versions
Student grant applications	Three years from and of year of application year then review annually	Requirement of HMRC and the DfE academies financial handbook	Secure Disposal Electronic and paper versions
Budget management records and associated paperwork	Three years from life of budget	Requirement of HMRC and the DfE academies financial handbook	Secure Disposal Electronic and paper versions
Invoices, receipts, orders, requisitions, delivery notices	Six years from fiscal year of transaction	Requirement of HMRC and the DfE academies financial handbook	Secure Disposal Electronic and paper versions
Banking records and associated paperwork	Six years from fiscal year in which record, or document created	Requirement of HMRC and the DfE academies financial handbook	Secure Disposal Electronic and paper versions
Records of identification and collection of debt	Six years from fiscal year of record creation	Requirement of HMRC and the DfE academies financial handbook	Secure Disposal Electronic and paper versions
Business fund cheque books, paying in books, ledgers, invoices, receipts, bank statements, journey books	Six years from year item created	Requirement of HMRC and the DfE academies financial handbook	Secure Disposal Electronic and paper versions

Health and Safety			
Document type	Retention period	Trigger	Action
Health and safety policies	Life of policy + 7 years	Policy Reviewed and updated	Secure Disposal Electronic and paper versions
Risk assessments: general	Date of risk assessment + 7 years (update regularly)	Limitation Act (1980) Risk Assessments Reviewed and updated	
Risk assessments: exposure to noise, vibration, lead, asbestos, chemicals, and biohazards (including COSHH)	Date of risk assessment + 40 years (update regularly)	Control of Substances Hazardous to Health Regulations (2002), Regulation 11 Control of Asbestos at Work Regulations (2012), Regulation 19	
Risk assessments: exposure to radiation	Date of risk assessment + 50 years	Ionising Radiation Regulations 1999 (SI 1999/3232)	
Accident reporting: adults a) accident books b) F2508-RIDDOR forms c) local accident investigation records	Current year + 3	Social Security (Claims and Payments) Regulations (1979), Regulation 25 Social Security Administration Act (1992), Section 8. Limitation Act (1980)	
Accident reporting: children a) accident books b) F2508-RIDDOR forms c) local accident investigation records	Date of birth of child + 22 years	Social Security (Claims and Payments) Regulations (1979), Regulation 25 Social Security Administration Act (1992), Section 8. Limitation Act (1980)	
Violent incident reporting (VIR)	Current year + 3 years	Limitation Act (1980)	
Physical intervention forms	Date of birth of child + 22 years		
Fire precaution logbooks (e.g., records of drills and tests)	Current year + 6 years	Limitation Act (1980)	
Accessibility plans	Current year + 6 years	Equalities Act (2010)	
Health and safety training records	While current + 6 years, unless records apply for limited period (e.g., First Aid Certificates)	On going	
Maintenance records for any work equipment, including ladders, trollies, PPE, PAT etc	Current year + 10 years	On going	
Health and safety inspection records, including: □ site inspections	Current year + 3 years	On going	

Premises			
Document type	Retention period	Trigger	Action
Lease agreement of all property	Expiry of lease + 7 years	Retain on file duration of lease agreement	Secure Disposal Electronic and paper version
Documents relating to design/plan	Expiry of lease + 7 years	Retain on file duration of lease agreement	
Records relating to the letting of premises	Current year + 3 years	Retain on file while relevant	
Burglary, theft, and vandalism report forms	Current year + 6 years	Insurance and police investigation	
All records relating to maintenance reporting including any scheduled work.	Current year + 6 years	Full maintenance log held by Alfa Laval	
Inventories of equipment and furniture	Current year + 6 years	On going	
Insurance papers	While current	On going	
CCTV	Retain for 31 days until overwritten unless used in legal case when CCTV footage will become part of case file and stored in a digital format so it can be retained for 6 years	CCTV is controlled by Alfa Laval. Limitation Act 1980 (Section 2) CCTV Code of Practice (Revised Edition 2008) section 8.3	

Information Technology			
Document type	Retention Period	Trigger	Action
IT – Data storage, Records relating to data storage management: • Routine back-up, Archiving, • Deletion	1 year	At end of administrative use	Secure
IT – Data storage, Records relating to data retrieval management: • Requests to recover data	6 months	From date of last action, business needs	
IT – Faults All records relating to fault reporting	1 year	From year records created LGA Retention Tool	
IT – Hardware All records relating to developing, modifying and maintaining ICT systems	6 years	From decommissioning of implemented system or last action of abandoned system Limitation Act 1980 (Section 2)	
IT – Licencing Records relating to software licencing	6 years	From date system decommissioned LGA Retention Tool	
IT – Monitoring Records relating to monitoring and testing of systems	1 year	At end of administrative use LGA Retention Tool	

			Disposal Electronic
IT – Networks All records relating to the implementation and management of computer networks used by the Overworld Organisation.	6 years	From date system superseded LGA Retention Tool	
IT – Security All records relating to the creation and implementation of policy and procedures relating to information security	3 years	From year records created LGA Retention Tool	
IT – Security Records relating to breaches or attempted breaches of ICT security	6 years	From final action Limitation Act 1980 (Section 2)	
IT – Users Records relating to the provision of IT function for all service areas allowing them to store personal data and custodians for all business software used across the Overworld Organisation: • Opening, maintenance & closure of user accounts • Reported faults with IT user groups and action taken to resolve issues	1 year	From year records created LGA Retention Tool	
IT – Users All information relating to user profiles for information systems	6 years	From year records created LGA Retention TooL	
IT – Website Records relating to provision of Online services to clients	3 years	From creation of records LGA Retention Tool	

Appendix 2 - Privacy Notice

We comply with all the requirements of the UK GDPR

Why we collect & use information on the children & young people (CYP) who attend Overworld?

- ✓ to support them in their holistic goals
- ✓ to monitor & report their progress in line with their goals
- ✓ to provide appropriate pastoral care
- ✓ to assess the quality of our services
- ✓ to keep them & everyone around them safe (food allergies, emergency contact details etc)

The categories of personal information that we collect, hold & might share include:

- ✓ Personal information (such as age, name & address)
- ✓ Characteristics (such as gender identity, preferred pronouns)
- ✓ Attendance information (sessions attended, absences etc)
- ✓ How they travel to & from the centre
- ✓ Relevant medical, special educational needs & behavioural information
- ✓ CCTV is in operation within the centre to keep everyone safe; this will not be shared unless we are legally authorised to do so by the Police

The General Data Protection Regulation allows us to collect & use CYP information with consent of the data subject, where we are complying with a legal requirement, where processing is necessary to protect the vital interests of a data subject or another person & where processing is necessary for the performance of a tack carried out in the public interest or in the exercise of official authority vested in the controller. When the personal information is Special Category Information, we may rely on processing being in the substantial public interest in addition to consent of the data subject & the vital interest of the data subject or another.

Collecting personal information

The client – parent/carer, placing local authority or school - provide us this information in the best interests of the CYP on a voluntary basis. You may ask us to stop processing this information at any time.

How we store CYP data

We hold CYP data in accordance with our retention schedule found in our *Data Protection, GDPR & IT Policy*.

Who we share CYP information with

- ✓ The CYP's school or the local authority, if they have the contract with us
- ✓ For CYP placed by their parent/carer it is unlikely that we will share information outside of the organisation unless there is a safeguarding concern
- ✓ With social services & other authorities if legally obliged, see our *Safeguarding Policy & Procedures*

You have the right to:

- ✓ Object to processing of personal data that is likely to cause or is causing, damage or distress
- ✓ Prevent processing for the purpose of direct marketing
- ✓ Object to decisions being taken by automated means
- ✓ In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed;
- ✓ Claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern

Please contact the Data Protection Officer, Simon Bradley simon.bradley@overworld-amp.uk or Managing Director Mark Pickering. markp@overworldnetwork.com

Appendix 3 - Photography & Videos Consent Form

This information explains the reasons why & how the Organisation may take & use photographs & videos of its service users. It should be read alongside our E-Safety Guidelines & Acceptable Use Form (appendix 2 – E-Safety Policy). Please outline your agreement as either a parent/carer for a young person <18yrs or a young person >16yrs, by completing this consent form.

Why do you we take & use photographs & videos?

- Primarily to develop your/your CYP interests in creative media/streaming etc & for any formal (certificated) project work
- For displays in the centre
- For promotional purposes on our social media platforms & website etc

Who else takes & uses images & videos?

Only members of staff & CYP will be taking videos or photographs as part of their work.

What are the conditions of use?

This consent form is valid indefinitely unless you, or the young person, asks us to take down their content. The photographs & videos taken are stored securely & when they are no longer required, they are disposed of safely & securely.

Safeguarding

In order to send off for ASDAN or AIM certificates, we will need to use your/your CYP full name. We will not use the personal details or full names of anyone in any photograph or video, on websites, social media or any printed publication

I provide consent to:

(please circle)

Yes No	Taking & using photographs &/or videos of my CYP on any managed & maintained websites
Yes No	Taking & using photographs &/or videos of my CYP to share as evidence of progress with their school/local authority representative
Yes No	Taking & using photographs &/or videos on internal displays such as posters, screens, noticeboards or otherwise, that can only be seen by approved visitors, staff & CYP
Yes No	Taking & using photographs &/or videos on external displays such as posters, screens, noticeboards or otherwise, that can be seen by members of the public.

Declaration

Signed ……..

Print name ……..

Date ……

For those CYP who are working online only or cannot sign, a verbal acknowledgment will be recorded by a mentor. Email agreement is also accepted.