DATA PROTECTION AND GDPR

V4 OCTOBER 2026

Author	Training and Quality Manager
Review Date	August 2027

Tilford House, Tilford Business Park, Weydon Lane, Farnham, Surrey. GU9 8QT
t. 01252 514999 **e.** info@overworld-amp.uk **w.** www.overworld-amp.uk

Version 2 Sep 24	Complete re-write.
Version 3 Sep 25	Updated Legal and Statutory Framework. New section on our use of cloud-based MS 365, MyConcern and Edukey. Added a full section clarifying when and how consent is sought, with emphasis on children's rights and capacity under UK GDPR. New section outlining the process for assessing risk before implementing new technologies or high-risk data practices. Expanded explanation of the requirement for third parties to comply with UK GDPR and have data processing agreements in place. ICO's Children's Code (Age Appropriate Design Code) to show alignment with best practice for digital platforms used with children.
Version 4 Oct 26	Updated with KCSiE 2026. Streamlined for readability. New section 7.5 Personal Devices, Photography and Recording

Contents

1. INTRODUCTION 3
2. SCOPE 3
3. LEGAL AND GUIDANCE FRAMEWORK 3
4. ROLES AND RESPONSIBILITIES 3
5. DATA PROTECTION PRINCIPLES 4
6. PROCESSING PERSONAL DATA 5
7. INFORMATION SECURITY 6
8. DATA SHARING 6
9. DATA BREACHES 7
10. INDIVIDUAL RIGHTS 7
11. RETENTION AND DISPOSAL OF PERSONAL DATA 8
12. MONITORING AND REVIEW 8
APPENDIX 1. SUBJECT ACCESS REQUESTS (SAR) 9
APPENDIX 2. PERSONAL DATA BREACH PROCEDURE 11
APPENDIX 3: DATA RETENTION AND DISPOSAL OF RECORDS 12
Business Management/Administration 13
Strategy Communications and Marketing 16
Young People 18
Parent/Guardian 19
Human Resources 20
Insurance and certification 22
Financial 23
Health and Safety 25
Premises 27
Information Technology 28
Appendix 4 - Privacy Notice ..... **Error! Bookmark not defined.**
Appendix 5 - Photography and Videos Consent Form 32

1. INTRODUCTION

This policy sets out how Overworld AMP Limited ("the Provision") collects, uses, stores, shares and protects personal data in accordance with UK data protection legislation.

The Provision is committed to ensuring that personal information is processed lawfully, fairly, securely and transparently, while respecting the rights and freedoms of individuals. This policy applies to all personal data processed by the Provision, regardless of whether it is held electronically, in paper records or by authorised third-party processors.

The policy supports the Provision's wider safeguarding, information security and governance arrangements and applies to all Directors, employees, contractors, volunteers and others who process personal data on behalf of the Provision.

2. SCOPE

This policy applies to all personal data processed by the Provision, regardless of the format in which it is held or the means by which it is processed.

It applies to all Directors, employees, contractors, volunteers, agency staff and any other individuals who process personal data on behalf of the Provision.

The policy covers personal data relating to young people, parents and carers, employees, applicants, volunteers, contractors, commissioners, visitors and any other identifiable individuals whose information is processed by the Provision.

All third-party organisations that process personal data on behalf of the Provision must comply with applicable data protection legislation and the terms of any relevant data processing agreement.

3. LEGAL AND GUIDANCE FRAMEWORK

The policy is underpinned by the following legislation and statutory guidance:

- UK General UK GDPR and Data Protection Act 2018 (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998 (Article 8 – Right to respect for private and family life)
- Protection of Freedoms Act 2012
- Keeping Children Safe in Education (2026)
- Working Together to Safeguard Children (2026)
- ICO guidance: www.ico.org.uk
- ICO CCTV Code of Practice

4. ROLES AND RESPONSIBILITIES

4.1. **The Directors** have overall responsibility for ensuring that the Provision complies with its obligations under UK data protection legislation. They will ensure that appropriate policies, procedures and resources are in place to support the secure and lawful processing of personal data.

4.2. **Data Protection Officer** is responsible for overseeing the implementation of this policy and promoting compliance across the Provision. Their responsibilities include:

- monitoring compliance with data protection legislation;
- providing advice and guidance to staff;
- managing data protection enquiries, requests and breaches;
- liaising with the Information Commissioner's Office (ICO), where appropriate;
- maintaining records relating to data protection compliance; and
- ensuring that staff receive appropriate data protection training.

4.3. **The Senior Leadership Team (SLT)** ensure that staff within their areas understand and follow this policy, implement appropriate security measures, and report any actual or suspected data protection concerns without delay.

4.4. **All Staff, Volunteers and Contractors** must

All individuals who process personal data on behalf of the Provision are responsible for:

- complying with this policy and related procedures;
- processing personal data lawfully, fairly and securely;
- protecting confidential information from unauthorised access, loss or disclosure;
- reporting suspected data breaches or security incidents immediately;
- completing required data protection training; and
- seeking advice where they are unsure how personal data should be handled.

Failure to comply with this policy may result in disciplinary action and, where appropriate, referral to relevant regulatory or legal authorities.

5. DATA PROTECTION PRINCIPLES

The Provision processes personal data in accordance with the principles set out in UK GDPR. Personal data will be:

5.1 Lawfulness, Fairness and Transparency

Personal data will be processed lawfully, fairly and transparently. Individuals will be informed about how their information is used through appropriate privacy notices and communications.

5.2. Purpose Limitation

Personal data will be collected for specified, explicit and legitimate purposes and will not be processed in a manner that is incompatible with those purposes, unless permitted by law.

5.3. Data Minimisation

The Provision will collect and retain only the personal data that is necessary to fulfil its educational, safeguarding, legal and operational responsibilities.

5.4. Accuracy

Reasonable steps will be taken to ensure that personal data is accurate, complete and kept up to date. Inaccurate or incomplete information will be corrected or deleted without undue delay.

5.5. Storage Limitation

Personal data will not be retained for longer than is necessary. Records will be managed and securely disposed of in accordance with the Provision's Retention Schedule and applicable legal requirements.

5.6 Integrity and Confidentiality

Appropriate technical and organisational measures will be implemented to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage.

5.7 Accountability

The Provision is responsible for demonstrating compliance with UK data protection legislation through appropriate policies, procedures, staff training, governance arrangements and record keeping.

6. PROCESSING PERSONAL DATA

The Provision processes personal data only where there is a lawful basis to do so under UK GDPR and the Data Protection Act 2018. The lawful basis relied upon will depend on the nature and purpose of the processing.

6.1. Lawful Basis for Processing

The Provision may process personal data where it is necessary:

- to fulfil a legal obligation;
- to perform a task carried out in the public interest or in the exercise of official authority;
- for the legitimate interests of the Provision or another organisation, provided these interests do not override the rights and freedoms of the individual;
- to perform or enter into a contract; or
- where consent has been obtained, where this is the appropriate lawful basis.

6.2. Special Category Data

The Provision may process special category personal data, such as information relating to health, ethnicity or religion, where permitted by law and where an appropriate condition for processing has been met.

Special category data will be processed only where it is necessary to support education, safeguarding, welfare, employment, legal obligations or other legitimate functions of the Provision.

6.3. Criminal Offence Data

Information relating to criminal offences or allegations will only be processed where there is a lawful basis and a specific legal condition permitting such processing. Access to this information will be restricted to those with a legitimate need to know.

6.4. Young People's Personal Data

The Provision recognises that young people's personal data requires particular protection. Information relating to young people will be processed only where necessary to support education, safeguarding, welfare and the Provision's statutory or contractual responsibilities.

Where consent is relied upon as the lawful basis for processing, it will be obtained from the appropriate individual in accordance with applicable legislation.

6.5. Automated Decision-Making and Artificial Intelligence

The Provision does not make decisions about individuals solely through automated processing where this would produce legal or similarly significant effects.

Artificial intelligence (AI) tools may be used to support administrative or educational activities. Staff must not input confidential or personal information into publicly available AI systems unless this is authorised and appropriate safeguards are in place. AI-generated content must always be reviewed by a member of staff and must not replace professional judgement, safeguarding responsibilities or human decision-making.

7. INFORMATION SECURITY

The Provision is committed to protecting personal data through appropriate technical and organisational measures designed to prevent unauthorised access, loss, alteration, disclosure or destruction.

7.2 Access Controls

Access to personal data will be restricted to authorised individuals who require the information to carry out their duties. Access permissions will be reviewed periodically and removed promptly when no longer required.

7.3 Secure Storage

Personal data will be stored securely, whether in electronic or paper format. Electronic records will be protected through appropriate security measures, including password protection, multi-factor authentication where appropriate, encryption and secure backups. Paper records containing personal information will be stored securely and accessible only to authorised personnel.

7.4 Use of Devices and Systems

All staff are responsible for using the Provision's systems and devices securely and in accordance with this policy, the *Employee Handbook* and the *Online Safety Policy*.

Reasonable steps must be taken to protect personal data when working remotely or using portable devices, including ensuring that devices are secured against unauthorised access and that confidential information is not left unattended or accessible to others.

7.5 Personal Devices, Photography and Recording

Staff must not use personal devices to take photographs, videos or audio recordings in connection with their work for the Provision.

Photographs, videos and audio recordings required for an authorised work purpose must only be made using equipment and systems provided or expressly approved by the Provision and in accordance with the Provision's safeguarding and data protection requirements.

Staff must not record meetings, conversations or other workplace activities without prior authorisation. Where recording is authorised, participants will normally be informed before recording begins.

Requests to record as a reasonable adjustment or for another legitimate purpose should be agreed in advance so that appropriate arrangements and safeguards can be put in place.

7.6 Passwords and Authentication

Staff must use strong passwords, protect authentication credentials and must not share login details with others. Multi-factor authentication will be used where appropriate to strengthen the security of organisational systems.

7.7 Information Security Awareness

All staff will receive appropriate training and guidance to help them understand their responsibilities for protecting personal data and recognising potential information security risks.

8. DATA SHARING

The Provision will share personal data only where there is a lawful basis to do so and where the sharing is necessary, proportionate and in the best interests of the individual, particularly where safeguarding responsibilities apply.

8.1 Sharing Personal Data

Personal data may be shared with:

- local authorities and commissioning bodies;
- schools, colleges and other education providers;
- health and social care professionals;
- safeguarding partners and law enforcement agencies;
- regulatory and inspection bodies;
- examination and awarding organisations; and
- other organisations where there is a lawful basis or legal obligation to do so.

Information will be shared in accordance with UK GDPR, the Data Protection Act 2018 and relevant safeguarding legislation and guidance.

8.2 Safeguarding

The Provision recognises that data protection legislation does not prevent the sharing of information where this is necessary to safeguard or promote the welfare of a child or vulnerable individual.

Where there are concerns about a young person's safety or wellbeing, information will be shared promptly with appropriate agencies in accordance with the Provision's Safeguarding (Young Person Protection) Policy and statutory guidance.

8.3 Third-Party Processors

Where third-party organisations process personal data on behalf of the Provision, appropriate contractual arrangements will be in place to ensure that personal data is processed securely, lawfully and only in accordance with the Provision's instructions.

The Provision will undertake appropriate due diligence when appointing third-party processors and will monitor compliance where appropriate.

9. DATA BREACHES

The Provision takes all actual and suspected personal data breaches seriously and will respond promptly to minimise the risk of harm to individuals and the Provision.

A personal data breach may include the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All staff, volunteers and contractors must report any actual or suspected personal data breach immediately to the Data Protection Lead, regardless of how minor the incident may appear.

The Data Protection Lead will assess the breach, take appropriate action to contain and investigate the incident, determine whether notification to the Information Commissioner's Office (ICO) or affected individuals is required, and maintain appropriate records of the breach and the actions taken.

All personal data breaches will be managed in accordance with the *Provision's Data Breach Procedure* (Appendix 2).

10. INDIVIDUAL RIGHTS

Under UK GDPR and the Data Protection Act 2018, individuals have rights in relation to the personal data held about them. The Provision is committed to respecting these rights and responding to requests in accordance with applicable legislation.

Individuals may have the right to:

- be informed about how their personal data is collected and used;
- request access to their personal data (Subject Access Request);

- request the rectification of inaccurate or incomplete personal data;
- request the erasure of personal data where applicable;
- request the restriction of processing in certain circumstances;
- object to the processing of personal data where permitted by law;
- request the transfer of personal data where the right to data portability applies; and
- not be subject to decisions based solely on automated processing where these produce legal or similarly significant effects.

The Provision will consider all requests fairly and respond within the statutory timescales unless an exemption or extension permitted by law applies.

Individuals who are dissatisfied with the way their personal data has been handled should raise their concerns with a member of the SLT in the first instance.

Procedures for making and responding to Subject Access Requests are set out in Appendix 1 – Subject Access Request Procedure.

11. RETENTION AND DISPOSAL OF PERSONAL DATA

The Provision will retain personal data only for as long as it is necessary to fulfil the purpose for which it was collected, to meet legal, safeguarding, regulatory and operational requirements, or to establish, exercise or defend legal claims.

Retention periods are determined in accordance with statutory requirements, recognised sector guidance and the Provision's operational needs. Personal data will be reviewed periodically and securely disposed of when it is no longer required.

Electronic records will be securely deleted where appropriate, and paper records containing personal information will be destroyed using secure disposal methods to prevent unauthorised access or disclosure.

Where personal data is subject to an ongoing safeguarding matter, investigation, complaint, legal proceedings or other legitimate requirement, it may be retained for longer than the standard retention period.

Further information is contained within Appendix 3 – Records Retention Schedule.

12. MONITORING AND REVIEW

The Directors are responsible for ensuring that appropriate arrangements are in place to support compliance with this policy.

The Data Protection Lead will monitor the implementation of this policy, oversee compliance with data protection legislation and recommend updates where required.

This policy will be reviewed annually, or sooner where there are significant changes to legislation, statutory guidance, organisational practice or identified areas for improvement.

APPENDIX 1. SUBJECT ACCESS REQUESTS (SAR)

Under Article 15 of the UK General UK GDPR and Data Protection Act 2018 (UK GDPR), individuals have the right to obtain confirmation that their personal data is being processed and, where this is the case, to access that personal data and associated information.

Overworld AMP Limited ("the Provision") is committed to responding to Subject Access Requests (SARs) lawfully, fairly and without undue delay.

A1.1. Making a Request

Subject Access Requests may be made verbally or in writing. To ensure requests are handled efficiently, the Provision encourages requests to be made in writing and addressed to the Data Protection Officer at info@overworld-amp.uk.

Requests should clearly describe the information being sought. Where a request is unclear, the Provision may ask for further information to help identify the records requested.

A1.2. Verifying Identity

Before personal information is disclosed, the Provision must be satisfied as to the identity of the requester. Where appropriate, the Provision may request evidence of identity, such as:

- Passport
- Driving licence
- Recent utility bill
- Birth or marriage certificate
- Bank or mortgage statement
- Other suitable identification

Where a request is made on behalf of another individual, the Provision may also require evidence of parental responsibility, legal authority or other appropriate authorisation before releasing any information.

A1.3. Requests Relating to Young People

Young people have the right to request access to their own personal data where they have sufficient maturity and understanding to exercise that right.

Where a request is made on behalf of a young person, the Provision will consider whether the young person has the capacity to understand the nature of the request and whether they wish their information to be disclosed.

Where a young person is not considered capable of exercising this right independently, a person with parental responsibility or another authorised representative may make the request on their behalf.

A1.4. Fees

The Provision will normally provide information free of charge.

A reasonable administrative fee may be charged where:

- a request is manifestly unfounded or excessive, particularly where requests are repetitive; or
- additional copies of information previously provided are requested.
- If a fee is payable, the requester will be informed before the request is processed.

A1.5. Timescales

The Provision will respond to Subject Access Requests without undue delay and, in any event, within one calendar month of receiving:

- the request;
- sufficient information to identify the requested records; and
- satisfactory proof of identity, where required.

Where a request is particularly complex or multiple requests have been received from the same individual, the response period may be extended by up to a further two months. Where an extension is necessary, the requester will be informed within the initial one-month period and provided with an explanation.

A1.6. Review of Information

Before information is disclosed, the Provision will review all records to determine whether any exemptions under the UK GDPR or Data Protection Act 2018 apply.

Information may be withheld or redacted where disclosure would:

- reveal the personal data of another individual;
- prejudice the prevention or detection of crime;
- compromise safeguarding arrangements;
- be likely to cause serious harm to the physical or mental health of any individual; or
- otherwise fall within a statutory exemption.

Where appropriate, third-party information will be removed or redacted before disclosure unless it is reasonable and lawful to disclose it.

A complete copy of the original records will be retained where redactions have been made in order to provide an audit trail of the information disclosed.

A1.7. Providing Information

Information will normally be provided electronically unless another format is requested or considered more appropriate.

Where requested, information may be explained by an appropriate member of staff to ensure that the information provided is clear and understandable.

Where hard copies are provided, appropriate measures will be taken to ensure the secure delivery of personal information.

A1.8. Complaints And Further Information

Individuals who are dissatisfied with the handling of a Subject Access Request should raise their concerns with the Data Protection Lead in the first instance.

If concerns cannot be resolved, individuals have the right to make a complaint to the Information Commissioner's Office (ICO).

Website: https://www.ico.org.uk

Telephone: 0303 123 1113

APPENDIX 2. PERSONAL DATA BREACH PROCEDURE

A personal data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All staff, volunteers, contractors and others acting on behalf of the Provision are responsible for reporting actual or suspected personal data breaches immediately.

A2.1. Reporting a Breach

Any actual or suspected personal data breach must be reported immediately to the Data Protection Officer.

Reports should include, where known:

- the nature of the breach;
- the date and time the breach occurred or was discovered;
- the type of personal data involved;
- the number of individuals potentially affected;
- any immediate actions already taken; and
- any known or suspected risks.

Staff must report concerns immediately even where all the information is not yet available.

A2.2. Immediate Response

Upon becoming aware of a personal data breach, the Provision will take reasonable steps to:

- contain the breach and prevent further loss or unauthorised disclosure;
- recover personal data where possible;
- preserve relevant evidence;
- assess the nature and extent of the incident; and
- minimise any potential harm to affected individuals.

A2.3. Assessment

The Data Protection Lead will assess:

- the type and sensitivity of the personal data involved;
- how many individuals are affected;
- the likelihood and severity of any risk to individuals' rights and freedoms;
- whether the personal data has been recovered;
- whether further protective action is required; and
- whether the breach must be reported to the Information Commissioner's Office (ICO) or other agencies.

All decisions and actions taken will be appropriately documented.

A2.4 Notification

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the Provision will notify the Information Commissioner's Office (ICO) without undue delay and, where required, within 72 hours of becoming aware of the breach.

Where the breach is likely to result in a high risk to the rights and freedoms of individuals, the affected individuals will also be informed without undue delay, unless an exemption applies.

Where appropriate, the Provision may also notify commissioning authorities, safeguarding partners, law enforcement agencies or other relevant organisations.

A2.5. Recording the Breach

All personal data breaches, regardless of whether they are reportable to the ICO, will be recorded. Records will include:

- the facts relating to the breach;
- the effects of the breach;
- decisions made;
- actions taken to contain and resolve the incident; and
- measures introduced to reduce the likelihood of recurrence.

A2.6. Learning and Improvement

Following a personal data breach, the Provision will review the circumstances of the incident and implement any necessary improvements to policies, procedures, systems, training or security arrangements to reduce the risk of similar incidents occurring in the future.

A2.7. Complaints and Further Information

Anyone with concerns about the handling of a personal data breach should contact the **Data Protection Officer** in the first instance.

Further information is available from the Information Commissioner's Office (ICO):

- Website: https://www.ico.org.uk
- Telephone: 0303 123 1113

APPENDIX 3: DATA RETENTION AND DISPOSAL OF RECORDS

The retention periods below are based on current statutory requirements, HMRC requirements, the IRMS Schools Toolkit and other recognised sector guidance. Where legislation or statutory guidance changes, the statutory requirement will take precedence over this schedule.

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 Provision	Retained for operational use and reference	Until superseded or whilst relevant	Secure Disposal Electronic and paper versions
Policy documents administered by the Provision	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 LA/placing Organisation/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 Directors 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 identified process or function in the Retention Schedule. • Letters • Emails • General Correspondence/files	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 brought into line with the new volume.	Secure Disposal Electronic and paper versions
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

The Provision 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 and 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 and 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 and 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 and Marketing, Records relating to Public Relations and interaction with the media: • Records of events including • Photographs depicting identified individuals • Video and 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 and	Permanent if significant event.	From date of event	The National Archives Retention

Marketing, Records relating to the development and promotion of Local Authorities Campaigns and events	Retain 7 years if minor campaign or event		Guidance 2012 Secure Disposal Electronic and paper versions

Young People			
Document type	Retention period	Trigger	Action
Monitoring forms/reports	Date of birth of pupil + 22 years	UK GDPR and Data Protection Act 2018 Unless child protection applies, in which case retain for 25 years from DOB;	Secure Disposal Electronic and paper versions
Young Person protection information held on safeguarding file (paper)	Date of birth + 25 years	Keeping children safe in education Statutory guidance for schools and colleges Working together to safeguard children.	
Young Person protection information held on MyConcern	Date of birth + 25 years	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	
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 Young People - 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 YP maintained for the Provision'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	
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	Current year + 3 years	On going	

certificates)			Secure Disposal Electronic and paper versions
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 Organisation/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	HMRC requirements and accepted accounting practice	Secure Disposal Electronic and paper versions
Loans and grants	12 years from last payment of loan then review annually		Secure Disposal Electronic and paper versions
Student grant applications	Three years from and of year of application year then review annually		Secure Disposal Electronic and paper versions
Budget management records and associated paperwork	Three years from life of budget		Secure Disposal Electronic and paper versions
Invoices, receipts, orders, requisitions, delivery notices	Six years from fiscal year of transaction		Secure Disposal Electronic and paper versions
Banking records and associated paperwork	Six years from fiscal year in which record, or document created		Secure Disposal

			Electronic and paper versions
Records of identification and collection of debt	Six years from fiscal year of record creation		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		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 landlord	
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	Information Commissioner's Office (ICO) guidance on Video Surveillance (CCTV)	

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 Disposal Electronic
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 IRMS Schools Toolkit	
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 IRMS Schools Toolkit	
IT – Monitoring Records relating to monitoring and testing of systems	1 year	At end of administrative use IRMS Schools Toolkit	
IT – Networks All records relating to the implementation and management of computer networks used by the Overworld Organisation.	6 years	From date system superseded IRMS Schools Toolkit	
IT – Security All records relating to the creation and implementation of policy and procedures relating to information security	3 years	From year records created IRMS Schools Toolkit	

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 and closure of user accounts • Reported faults with IT user groups and action taken to resolve issues	1 year	From year records created IRMS Schools Toolkit	
IT – Users All information relating to user profiles for information systems	6 years	From year records created IRMS Schools Toolkit	
IT – Website Records relating to provision of Online services to clients	3 years	From creation of records IRMS Schools Toolkit	

APPENDIX 4 - PRIVACY NOTICE

Who We Are

Overworld AMP Limited ("the Provision") is committed to protecting the privacy and personal information of young people, parents and carers, employees, volunteers and others who engage with our services.

This Privacy Notice explains how we collect, use, store and share personal information in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Why We Collect Personal Information

We collect and process personal information to:

- deliver education and alternative provision services;
- support young people's learning, wellbeing and individual outcomes;
- safeguard and promote the welfare of young people;
- monitor attendance, engagement and progress;
- communicate with parents, carers, commissioners and partner organisations;
- comply with our legal and regulatory obligations; and
- maintain the safety and security of our premises and services.
- The Information We Collect
- Depending on the services provided, we may collect and process:
- personal details, including names, addresses, dates of birth and contact information;
- emergency contact details;
- attendance and engagement records;
- education records and progress information;
- safeguarding and welfare information;
- health information, dietary requirements and medical needs;
- Special Educational Needs and Disabilities (SEND) information;
- behaviour and risk management records;
- equality and diversity information where appropriate;
- photographs and video recordings where consent or another lawful basis applies; and
- CCTV recordings for safeguarding, security and crime prevention purposes.

Lawful Basis for Processing

The Provision processes personal data in accordance with UK GDPR and the Data Protection Act 2018.

Depending on the purpose, we rely on one or more of the following lawful bases:

- compliance with a legal obligation;
- performance of a task carried out in the public interest;
- legitimate interests;
- performance of a contract; or
- consent, where this is the appropriate lawful basis.
- Where special category personal data is processed, we will ensure that an appropriate condition for processing under the Data Protection Act 2018 is also met.

Where We Obtain Information

Personal information may be obtained from:

- parents and carers;
- young people;
- schools and colleges;

- local authorities;
- health and social care professionals;
- other agencies involved in supporting the young person; and
- information generated through the Provision's day-to-day operation.

How We Store Information

Personal information is stored securely using appropriate technical and organisational measures designed to protect against unauthorised access, loss or disclosure.

Information is retained only for as long as necessary in accordance with the Provision's Records Retention Schedule and applicable legal requirements.

Who We Share Information With

Where there is a lawful basis, information may be shared with:

- commissioning local authorities;
- schools and education providers;
- health professionals;
- social care services;
- safeguarding partners;
- law enforcement agencies;
- regulatory and inspection bodies; and
- other organisations where sharing is required by law or is necessary to safeguard a young person.

The Provision will never sell personal information to third parties.

Your Rights

Under UK GDPR, individuals have rights which may include the right to:

- be informed about how personal data is used;
- request access to personal data;
- request correction of inaccurate information;
- request erasure where applicable;
- request restriction of processing;
- object to certain types of processing;
- request data portability where applicable; and
- complain about the way personal information has been handled.

Further information about exercising these rights can be found in the Provision's Data Protection Policy.

Contact Us

If you have any questions about this Privacy Notice or how your personal information is processed, please contact the Data Protection Officer info@overworld-amp.uk.

If you remain dissatisfied, you have the right to complain to the Information Commissioner's Office (ICO).

Website: https://www.ico.org.uk

Telephone: 0303 123 1113

APPENDIX 5 - PHOTOGRAPHY AND VIDEOS CONSENT FORM

Overworld AMP Limited ("the Provision") uses photographs, video recordings and other digital media to support learning, celebrate achievement and promote the Provision.

This form explains how photographs and videos may be used and asks for your consent where this is required.

Please read this form alongside the Provision's *Data Protection and GDPR Policy*.

Why We Use Photographs and Videos

Photographs and videos may be used to:

- support learning and accredited coursework (including ASDAN, AIM Qualifications and other awarding organisations);
- develop young people's skills in photography, film-making, streaming and other creative media;
- record and celebrate achievements;
- share progress with parents, carers, named schools and local authorities;
- create displays within the Provision; and
- promote the Provision through its website, social media channels and other publicity materials.

Who May Take Photographs or Videos

Photographs and videos may be taken by:

- authorised members of staff;
- young people participating in supervised educational activities; or
- approved external professionals working on behalf of the Provision.

All photography and video activities will be appropriately supervised and carried out in accordance with the Provision's safeguarding arrangements.

Storage and Security

Photographs and videos will be stored securely and accessed only by authorised individuals.

They will be retained only for as long as necessary in accordance with *the Provision's Data Protection Policy*.

Consent may be withdrawn at any time for future use. Withdrawal of consent will not affect any lawful use of images that took place before consent was withdrawn.

Safeguarding

The Provision will never publish personal information alongside photographs or videos where this would place a young person at increased risk.

Where awarding organisations require identifying information (such as a young person's name or date of birth) in support of accredited work, this information will be shared only where necessary and in accordance with the *Provision's Data Protection Policy*.

Consent

Please indicate whether you consent to the following uses of your/your young person’s image. Please tick either "Yes" or "No" for each use listed below. You may consent to some uses and not others.

Uses of your/your young person's image	Yes	No
As part of accredited coursework which will only go to the awarding body.	☐	☐
To be shared with my parents/carers, my named school, if applicable and my caseworker as evidence of my time at Overworld AMP.	☐	☐
To be displayed within the Provision e.g. displays, noticeboards or digital screens.	☐	☐
To be published on the Provision's website.	☐	☐
To be published on the Provision's official social media channels.	☐	☐
To be used in promotional materials e.g. leaflets, prospectuses or presentations.	☐	☐

Declaration

Young Person (required for young people aged 16 and over)

I have read and understood this Photography and Video Consent Form and understand how my photographs and videos may be used.

Name: _____

Signature: _____

Date: _____

Parent/Carer (required for young people under 16 years of age)

I have read and understood this Photography and Video Consent Form and give consent for the uses indicated above.

Name: _____Relationship to Young Person: _____

Signature: _____

Date: _____

Parent/Carer Acknowledgement (optional for young people aged 16–17)

I confirm that I have read this Photography and Video Consent Form and understand how photographs and videos may be used by the Provision.

Name: _____Relationship to Young Person: _____

Signature: _____

Date: _____