Magnum Opus
TRAINING LIMITED

POLICIES AND PROCEDURES

GDPR and Data Protection Policy

Magnum Opus Training Limited

LAST REVIEWED	NEXT REVIEW DUE
September 2026	September 2027
APPROVED BY	**ROLE**
Mr S King	Headteacher

Signature



Karting Academy
MAGNUM OPUS TRAINING LTD

Boxing Academy
MAGNUM OPUS TRAINING LTD

Construction Academy
MAGNUM OPUS TRAINING LTD

Purpose and scope

Magnum Opus Training Limited protects the personal information it uses to deliver alternative provision, employ staff and run its services. This policy explains what we hold, why we use it, how people can exercise their rights, and the steps staff must take to keep it secure. It applies to our students, including adults aged 18 to 25, parents and carers, staff, applicants, commissioners and other contacts. It applies at all three sites and to information held on paper, LearnTrek, our secure cloud, company-managed phones, an encrypted backup PC and CCTV.

Magnum Opus is a data controller for the personal information it decides to collect and use. A commissioning school or local authority may be a separate controller for its own records and decisions. We will clarify each organisation's role and secure sharing arrangements in our commissioning and supplier records. Our ICO registration number is ZB865875. Scott King, Headteacher, is the internal data protection lead. Questions, rights requests and data protection complaints should be sent to office@magnumopustraining.com. Staff must report a suspected data incident directly to Scott King without delay.

The information we use and why

For students, we may hold identity and contact details, referrals and placement arrangements, attendance and behaviour records, work and progress, emergency contacts, EHCP information, health and support needs, and safeguarding records. For parents and carers we hold contact and communication information. For staff and applicants we hold recruitment, vetting, employment, training, payroll and relevant health or adjustment information. We also hold commissioner contacts, financial records and CCTV footage. We collect information from the person concerned, their parent or carer where appropriate, the commissioning school or local authority, and relevant professionals. We record the source when this matters to accuracy or safeguarding.

We use student information to assess whether we can meet a referral, plan and deliver provision, make reasonable adjustments, monitor attendance and progress, manage behaviour and safety, communicate with the school or local authority, and act on safeguarding concerns. We use staff and applicant information to recruit, employ, pay and support staff and meet vetting, safeguarding, tax and other legal duties. We use contact and finance information to manage contracts, invoices and enquiries. CCTV is used for site safety and security, subject to the controls below. We do not use student information for marketing.

Lawful use and sensitive information

We identify and record a UK GDPR Article 6 lawful basis for each use of personal information. Depending on the purpose, this may be performance of our contract with the person concerned, a legal obligation, or our legitimate interests in delivering a safe and effective service and managing the organisation. A contract with a school or local authority does not itself make the student a party to that contract. We do not treat the voluntary provision of information as consent. Where an optional activity genuinely relies on consent, we explain the choice and how consent can be withdrawn.

Health, disability, EHCP and some safeguarding information require an additional Article 9 condition. We record the relevant condition before using this information, including where the safeguarding of a child or an adult at risk meets the substantial public interest conditions in the Data Protection Act 2018. Where a Schedule 1 condition requires an appropriate policy document, we maintain one. Criminal offence information is handled only where an additional legal condition applies. We limit sensitive information to what is needed and review it when circumstances change.

Sharing and access

We routinely share relevant attendance and behaviour information with the commissioning school or local authority and, where appropriate, the student or their parent or carer. LearnTrek can email an attendance absence notice when the register is updated by 10:30 am to the linked primary contact and school or local authority officer. A manager checks recipient details and access permissions. Information that identifies other people or creates a safeguarding risk is assessed before disclosure. We share health, EHCP or safeguarding information with a school, local authority, social care, police, health service or another appropriate agency where it is necessary and lawful to support the person or protect someone from harm. This may occur without consent where the law permits or requires it. We keep a record of significant disclosures and their reasons.

Managers may access student records needed to run the provision. Teaching staff receive only the information needed for their role and for a student's support and safety. Staff records are kept separately in restricted secure cloud files, with access normally limited to Scott King. Access is reviewed when roles change and removed promptly when staff leave. We check the data protection terms and security arrangements for LearnTrek, cloud and messaging suppliers, including any access or transfers outside the UK.

Systems and everyday security

LearnTrek is the main student record, including attendance, behaviour and safeguarding information. Access is controlled by role and protected by multifactor authentication. The secure staff cloud also uses multifactor authentication. The backup PC is encrypted and used only by Scott King. Staff must use company-managed phones for the attendance WhatsApp chat, lock devices, keep accounts secure, and report loss or suspected access immediately.

The attendance WhatsApp chat uses student initials only. Initials can still identify a student to those who know the group, so the chat remains personal data. Staff must not post full names, EHCPs, health details, safeguarding details or detailed behaviour reports there. The attendance manager records the authoritative attendance information in LearnTrek. Staff are removed from the chat when they leave. Messages are deleted after one year unless they must be preserved for a documented incident, safeguarding matter or claim. Staff must use approved secure channels for more sensitive material.

Paper records are stored securely, kept out of public view and securely destroyed when due. Staff check addresses and recipients before sending information, use only approved storage and sharing methods, and avoid collecting or copying more information than necessary. Managers review access, backups and suppliers at least annually and after a significant incident or system change.

CCTV

Magnum Opus operates CCTV for site safety and security. Audio recording: none; the system records images only. Normal footage retention: 30 days. Signage: displayed at every site. Cameras must be positioned only where necessary, with access limited to authorised managers. Footage is not used for routine monitoring of staff or students. A request to view or share footage is assessed under data protection, safeguarding and law enforcement rules, with a record of the reason and disclosure. Footage needed for an incident, claim or investigation may be preserved for longer, with the reason and review date recorded.

Individual rights and requests

People may ask to access or correct their information and, where the law allows, ask for erasure, restriction, portability or object to a use of it. Some rights depend on the lawful basis and circumstances. A request may be made verbally or in writing; staff must forward it promptly to Scott King even if it does not mention data protection law. We verify identity and any representative’s authority proportionately. We normally respond to a subject access request within one month of receiving it, subject to lawful extensions or exemptions. We explain any refusal and the right to complain to the ICO.

A student who can understand the request should normally exercise their own rights. For a child, a parent or carer cannot automatically obtain the child's full record. We assess the child's understanding, wishes, best interests, the requester's parental responsibility or authority, and the sensitivity of the information. A competent child may authorise a parent to act. If a child is not competent, a person with parental responsibility may usually act where this is in the child's best interests. For an adult student, including a person aged 18 to 25, a parent or other representative needs the student's authority or an appropriate legal basis to act for them. We consider capacity and any lawful representative arrangements case by case. Safeguarding and third-party information are reviewed before release.

Data protection complaints

A person may complain about our handling of their personal information by emailing office@magnumopustraining.com or by contacting us through another reasonable channel. Scott King will arrange for the complaint to be logged, acknowledged within 30 days, investigated appropriately and answered with an outcome and any steps we will take. If Scott King is involved in the complaint, Rachel King or an independent external adviser will oversee it. A complaint about the service may also follow the Complaints Policy, but a data protection complaint receives this specific response. The person may also complain to the Information Commissioner's Office at ico.org.uk.

Personal data incidents

Staff must tell Scott King immediately about a lost device, wrong recipient, improper access, missing record, ransomware, accidental disclosure or any other suspected personal data breach. They must preserve evidence and follow instructions to contain the incident. Scott King records every breach, investigates the information and people affected, limits harm and documents the decision on notification. Where a breach is likely to create a risk to people's rights and freedoms, we notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where there is a high risk, we also tell affected people without undue delay unless a lawful exception applies. We review the cause and actions needed to prevent recurrence.

Retention and disposal

We keep information only while it serves a lawful purpose. The schedule below gives our starting periods and is reviewed against contract terms, safeguarding needs, claims and current guidance. A legal hold, investigation or continuing safeguarding need may require longer retention; the reason, owner and next review date must be recorded. Where the commissioning school or local authority needs the primary record, we agree secure transfer and avoid unnecessary duplicate retention. At the end of the period, we securely delete, shred or irreversibly anonymise information and record the action where appropriate.

Record	Normal retention and review
Student referral, placement, progress and routine support	Six years after the placement ends, or until the student's 25th birthday if later; review earlier if a commissioner holds the primary record.
Attendance and behaviour records	Six years from the record date, with longer retention only for a documented safeguarding, complaint or claim reason.
Child safeguarding records	Until the child's 25th birthday as a minimum working benchmark; records concerning child sexual abuse may require retention until the 75th birthday. Confirm transfer and case-specific requirements with the relevant safeguarding authority.
Adult safeguarding records	Six years after the final contact or case closure, then review; extend where the risk, statutory request or claim requires it.
Staff personnel records	Six years after employment ends, subject to a longer period for a claim or safeguarding allegation. Keep copies of DBS certificates only for as long as permitted by DBS guidance, normally no longer than six months after a decision.
Allegations of harm against staff involving a child	Until the staff member's normal retirement age or ten years from the allegation, whichever is later, unless the relevant safeguarding authority directs a longer period.
Applicant records for unsuccessful candidates	Six months after the decision, unless a longer period is needed for a documented claim or the person has agreed to a talent pool.
Invoices and VAT records	At least six years after the relevant financial year or transaction, subject to tax and contract requirements.
Attendance WhatsApp messages	One year from the message date, after the information is entered in LearnTrek; preserve only a documented

	incident, safeguarding or claim exception.
CCTV footage	30 days normally; preserve relevant footage for an incident, investigation or claim with a recorded review date.
Data protection requests, complaints and breach logs	Six years after closure, then review whether any open claim or regulatory matter requires longer retention.

Responsibility and review

All staff follow this policy, complete data protection training and raise incidents promptly. Managers limit access, check sharing and maintain accurate records. Scott King keeps the retention schedule, breach and request logs, checks supplier arrangements and reviews this policy at least annually or when law, systems or practice changes. The board of directors approves the policy.