BUS-019-1.0a Data Protection Policy

January 2026

1 PURPOSE

This policy demonstrates MGTS's commitment to protecting the privacy and personal data of all individuals with whom we interact, including learners, staff, employers, and other stakeholders. The policy ensures compliance with the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR), whilst supporting MGTS's mission to deliver high-quality education, training, and assessment services.

The purpose of this policy is to:

- Establish clear principles for the lawful, fair, and transparent processing of personal data
- Ensure compliance with all data protection legislation and regulatory requirements
- Protect the rights and freedoms of individuals whose personal data we process
- Provide clear guidance to staff on their data protection responsibilities
- Demonstrate accountability and transparency in our data processing activities
- Minimise data protection risks and maintain stakeholder trust

This policy applies to all personal data processed by MGTS in any format, including digital, paper-based, and audio-visual records, across all our activities and locations.

2 SCOPE

This policy applies to:

All MGTS Personnel:

- Senior leadership team and Board of Trustees
- All employees including managers, tutors, assessors, Training Development Advisers (TDAs), administrators, and support staff
- Contractors, consultants, volunteers, and temporary staff
- Subcontractors when processing data on behalf of MGTS

All Personal Data Subjects:

- Current, former, and prospective learners and apprentices
- All MGTS staff and job applicants
- Employers and workplace supervisors
- External verifiers, awarding body representatives, and inspectors
- Suppliers, service providers, and business contacts
- Website users and enquirers
- Any other individuals whose personal data MGTS processes

All Data Processing Activities:

- Learner recruitment, enrolment, and progression tracking
- Staff recruitment, employment, and performance management

- Assessment and certification processes
- Employer engagement and partnership management
- Marketing and communications activities
- Financial transactions and record keeping
- Health and safety management
- Safeguarding and welfare support

All Locations and Systems:

- Training centres in Coventry and Redditch
- Workplace learning environments
- Digital systems, databases, and cloud services
- Paper-based filing systems and archives
- Mobile devices and remote working arrangements

3 LEGISLATIVE AND REGULATORY FRAMEWORK

This policy ensures full compliance with:
Primary Data Protection Legislation:

- **UK General Data Protection Regulation (UK GDPR)** - comprehensive data protection framework
- **Data Protection Act 2018** - UK implementation and supplementary provisions
- **Privacy and Electronic Communications Regulations (PECR) 2003** - electronic marketing and cookies
- **Human Rights Act 1998** - right to respect for private and family life

Sector-Specific Legislation:

- **Education Act 2002** - processing pupil information and educational records
- **Apprenticeships, Skills, Children and Learning Act 2009** - learner data and skills records
- **Children Act 2004** - safeguarding and child protection data
- **Equality Act 2010** - processing sensitive equality monitoring data

Regulatory Requirements:

- **Ofsted Data Collections** - regulatory reporting and inspection data
- **Education and Skills Funding Agency (ESFA) Data Requirements** - funding and performance data
- **Institute for Apprenticeships and Technical Education (IfATE) Data Standards** - apprenticeship data
- **Awarding Body Data Sharing Agreements** - assessment and certification data
- **HMRC and Companies House Requirements** - employment and corporate data

4 DATA PROTECTION PRINCIPLES

MGTS adheres to the seven key principles of data protection under UK GDPR:

4.1 Lawfulness, Fairness and Transparency

Lawful Basis for Processing:

- All personal data processing is based on at least one of the six lawful bases under Article 6 UK GDPR
- For special category data, we identify an additional condition under Article 9
- Clear privacy notices explain our lawful basis and purpose for processing
- Regular review of lawful bases to ensure continued appropriateness

Fair and Transparent Processing:

- Personal data is processed fairly and in accordance with data subjects' reasonable expectations
- Clear, concise, and easily understandable privacy information provided at collection
- No hidden or unexpected use of personal data
- Transparent communication about data sharing and disclosure

4.2 Purpose Limitation

Specific and Legitimate Purposes:

- Personal data collected only for specified, explicit, and legitimate purposes
- Clear documentation of purposes in data protection registers and privacy notices
- No further processing incompatible with original purposes without additional lawful basis
- Regular review of processing purposes to ensure continued relevance

Compatible Use:

- Assessment of compatibility when considering additional uses of existing data
- Consideration of relationship between original and new purposes
- Appropriate safeguards for any compatible further processing
- Clear communication of any changes in processing purposes

4.3 Data Minimisation

Adequate, Relevant and Limited Processing:

- Collection and processing limited to what is necessary for identified purposes
- Regular review of data collection forms and processes to eliminate unnecessary fields
- Consideration of alternative approaches that require less personal data
- Staff training on data minimisation principles and practical application

Proportionate Processing:

- Balancing test between organisational needs and individual privacy
- Consideration of less intrusive alternatives
- Regular assessment of whether all collected data remains necessary
- Prompt deletion of data that is no longer required

4.4 Accuracy

Accurate and Up-to-Date Data:

- Reasonable measures to ensure personal data accuracy at collection
- Systems and processes to identify and correct inaccurate data
- Regular data cleansing and verification exercises
- Clear procedures for individuals to update their personal information

Correction of Inaccuracies:

- Prompt rectification of inaccurate personal data when identified
- Communication of corrections to relevant recipients where appropriate
- Investigation of underlying causes of data inaccuracies
- System improvements to prevent recurrence of accuracy issues

4.5 Storage Limitation

Limited Retention Periods:

- Personal data kept only for as long as necessary for identified purposes
- Clear retention schedules for different categories of personal data
- Automatic deletion processes where technically feasible
- Regular review and disposal of records that have exceeded retention periods

Secure Disposal:

- Secure deletion or destruction of personal data at end of retention period
- Certificate of destruction for physical media containing sensitive data
- Verification of complete data removal from all systems and backups
- Documentation of disposal activities for audit purposes

4.6 Integrity and Confidentiality (Security)

Appropriate Technical Measures:

- Encryption of personal data in transit and at rest where appropriate
- Access controls and user authentication systems
- Regular security updates and vulnerability assessments
- Backup and disaster recovery procedures

Organisational Measures:
- Staff training on data security responsibilities
- Clear desk and clear screen policies
- Incident response procedures for data breaches
- Regular review and testing of security measures

4.7 Accountability
Demonstrable Compliance:
- Comprehensive records of processing activities
- Privacy impact assessments for high-risk processing
- Regular compliance audits and reviews
- Data protection officer oversight and guidance

Governance and Oversight:
- Senior management accountability for data protection compliance
- Board oversight of data protection risks and performance
- Integration of data protection into business processes and decision-making
- Regular reporting on data protection matters

5. COMMUNICATION, TRAINING AND CPD FOR STAFF

5.1 Communication Strategy
Policy Awareness:
- All staff receive comprehensive data protection training during induction
- Policy accessible through MGTS internal systems and staff handbooks
- Regular updates and reminders about data protection responsibilities
- Clear guidance documents and quick reference materials available
- Annual Data Protection Awareness Week with focused activities

Culture Development:
- Senior leadership visible commitment to data protection principles
- Integration of privacy considerations into business planning and operations
- Recognition and reward for good data protection practices
- Open communication about data protection challenges and solutions
- Regular consultation with staff on data protection improvements

5.2 Mandatory Training Requirements
Induction Training for All Staff:
- Overview of UK GDPR and Data Protection Act 2018 requirements
- Understanding of MGTS data protection policies and procedures
- Recognition of personal data and special category data
- Lawful bases for processing and consent requirements
- Individual rights and how to respond to requests
- Data security responsibilities and incident reporting
- Practical scenarios relevant to education and training contexts

Role-Specific Training:
- **Management**: Data protection leadership, impact assessments, and breach management
- **Tutors and Assessors**: Learner data protection, assessment records, and confidentiality
- **TDAs**: Workplace data sharing, employer liaison, and mobile working security
- **Administrators**: Data entry, record management, and system security
- **IT Staff**: Technical security measures, access controls, and data backup procedures

5.3 Continuing Professional Development
Ongoing Training Programme:
- Annual refresher training covering latest legal developments and best practices
- Specialist workshops on topics such as data sharing, consent, and subject access requests
- Scenario-based learning using real examples from education and training sector
- External training opportunities including conferences and professional development
- Peer learning sessions sharing experiences and best practices across the organisation

Competence Assessment:
- Regular assessment of staff data protection knowledge and skills
- Competency frameworks for different roles and responsibilities
- Individual development plans incorporating data protection learning needs
- Recognition of data protection qualifications and certifications
- Integration with performance management and career development processes

6. PROCESS FOR MONITORING DATA PROTECTION COMPLIANCE

6.1 Continuous Monitoring Framework
Regular Compliance Monitoring:
- **Monthly**: Review of data protection incidents, complaints, and subject access requests
- **Quarterly**: Analysis of data protection training completion and compliance audits
- **Annually**: Comprehensive review of data protection policies, procedures, and effectiveness
- **Ongoing**: Monitoring of data processing activities against documented purposes and lawful bases

Key Performance Indicators:
- **Incident Response**: Time to detect, report, and resolve data breaches
- **Subject Rights**: Response times and quality for individual rights requests
- **Training Compliance**: Percentage of staff completing mandatory data protection training
- **Audit Results**: Compliance scores from internal and external data protection audits
- **Stakeholder Satisfaction**: Feedback on data protection arrangements from learners and staff

6.2 Documentation and Record Keeping
Records of Processing Activities (ROPA):
- Comprehensive register of all data processing activities under Article 30 UK GDPR
- Details of purposes, categories of data, recipients, retention periods, and security measures
- Regular review and updating of processing records
- Integration with privacy notices and impact assessments
- Annual validation of processing records with data controllers and processors

Compliance Documentation:
- Privacy impact assessments for high-risk processing activities
- Data sharing agreements with employers, awarding bodies, and other partners
- Consent records and withdrawal tracking systems
- Data breach register and incident response documentation
- Training records and competence assessments for all staff

6.3 Audit and Review Processes
Internal Audit Programme:
- Regular internal audits of data protection compliance across all departments
- Focus on high-risk areas such as special category data and international transfers
- Review of technical and organisational security measures
- Assessment of staff compliance with data protection policies and procedures
- Follow-up actions and improvement plans for identified non-compliance

External Validation:
- Independent data protection audits by qualified external auditors
- Penetration testing and security assessments of IT systems
- Legal review of data sharing agreements and privacy notices
- Benchmarking against sector best practices and regulatory guidance
- Certification schemes and accreditation where available and appropriate

7. REPORTING PROCEDURES FOR POTENTIAL BREACHES

7.1 Data Breach Definition and Recognition
What Constitutes a Data Breach:
- **Confidentiality breach**: Unauthorised access to or disclosure of personal data

- **Integrity breach**: Unauthorised or accidental alteration of personal data
- **Availability breach**: Accidental or unauthorised loss or destruction of personal data
- **Near miss incidents**: Situations that could have resulted in a breach but were prevented

Common Breach Scenarios in Education:
- Email sent to wrong recipient containing learner information
- Loss or theft of devices containing personal data
- Unauthorised access to student information systems
- Ransomware or malware affecting data systems
- Physical documents left in unsecured locations
- Verbal disclosure of confidential information to unauthorised persons

7.2 Immediate Response Procedures
Discovery and Initial Response (Within 1 Hour):
- Immediate containment to prevent further unauthorised access or disclosure
- Secure the affected systems or physical materials
- Inform line manager and Quality and Compliance Manager immediately
- Document initial details of the incident including time, location, and potential impact
- Preserve evidence and avoid actions that might compromise investigation

Initial Assessment (Within 4 Hours):
- Assessment of breach severity and potential impact on individuals
- Identification of categories and approximate numbers of affected data subjects
- Evaluation of likelihood of harm to individuals' rights and freedoms
- Determination of whether breach meets threshold for ICO notification
- Decision on need for immediate protective measures or communication

7.3 Investigation and Reporting
Formal Investigation Process:
- **Incident Response Team**: Quality and Compliance Manager, IT Manager, relevant department head
- **Evidence Gathering**: Comprehensive investigation of cause, scope, and impact
- **Risk Assessment**: Evaluation of actual and potential harm to affected individuals
- **Containment Review**: Assessment of effectiveness of immediate response measures
- **Root Cause Analysis**: Investigation of underlying causes and system weaknesses

External Reporting Requirements:
- **ICO Notification**: Within 72 hours if breach likely to result in risk to individuals' rights and freedoms
- **Regulatory Bodies**: Notification to Ofsted, ESFA, or awarding bodies where contractually required
- **Law Enforcement**: Involvement of police where criminal activity suspected
- **Insurance Companies**: Notification under professional indemnity or cyber insurance policies
- **Data Subjects**: Direct notification without undue delay if high risk to rights and freedoms

8. ACTIONS FOR POTENTIAL BREACHES INCLUDING CONTAINMENT PROCESS

8.1 Immediate Containment Measures
Technical Containment:
- **System Isolation**: Disconnection of affected systems from networks to prevent spread
- **Access Revocation**: Immediate suspension of user accounts and access credentials
- **Data Recovery**: Activation of backup and recovery procedures where data has been lost
- **Security Patches**: Emergency application of security updates to address vulnerabilities
- **Monitoring Enhancement**: Increased system monitoring to detect any ongoing unauthorised activity

Physical Containment:
- **Secure Area**: Isolation of affected physical areas and equipment
- **Document Recovery**: Collection and secure storage of any physical documents involved
- **Access Control**: Restriction of access to affected areas to authorised personnel only

- **Evidence Preservation**: Securing of physical evidence for investigation purposes

8.2 Communication and Stakeholder Management
Internal Communication:
- **Leadership Notification**: Immediate briefing of CEO and senior management team
- **Staff Communication**: Appropriate communication to affected staff while maintaining confidentiality
- **Board Reporting**: Formal reporting to Board of Trustees for significant breaches
- **Union Consultation**: Involvement of trade union representatives where staff data affected

External Communication:
- **Regulatory Notification**: Formal notification to ICO and other relevant regulatory bodies
- **Partner Communication**: Notification to employers, awarding bodies, and subcontractors where appropriate
- **Data Subject Notification**: Clear, timely communication to affected individuals about the breach and response
- **Media Management**: Coordinated response to any media enquiries about the breach

8.3 Remedial Actions and Recovery
Short-term Remedial Actions:
- **System Restoration**: Recovery of affected systems and data from secure backups
- **Security Enhancement**: Implementation of additional security measures to prevent recurrence
- **Process Review**: Immediate review and update of affected policies and procedures
- **Staff Support**: Provision of support and guidance to staff involved in or affected by the breach
- **Monitoring**: Enhanced monitoring of affected systems and individuals for signs of ongoing impact

Long-term Improvement Measures:
- **System Upgrades**: Investment in improved technical security measures and systems
- **Process Improvement**: Review and enhancement of data handling procedures
- **Training Enhancement**: Additional training for staff on lessons learned from the breach
- **Policy Updates**: Revision of data protection policies and procedures based on breach experience
- **Risk Assessment**: Updated risk assessments and privacy impact assessments

9. DATA RETENTION AND RECORDS MANAGEMENT

9.1 General Retention Principles
Legal and Regulatory Requirements:
- Retention periods based on legal obligations, regulatory requirements, and legitimate business needs
- Regular review of retention schedules to ensure continued appropriateness
- Clear documentation of retention decisions and their justification
- Coordination with legal team on litigation hold and regulatory investigation requirements

Retention Schedule Framework:
- **Category-based retention**: Different periods for different types of personal data
- **Purpose-based retention**: Aligned with original purpose for data collection
- **Risk-based retention**: Longer periods for high-risk data or where longer retention reduces risk
- **Individual circumstances**: Consideration of specific circumstances affecting retention needs

9.2 Specific Retention Periods for Education Records
Assessment Records (Minimum 3 Years Retention):
- **Assessment portfolios**: All assessment evidence and marking records for 3 years from completion
- **Internal verification records**: IQA sampling and standardisation records for 3 years
- **External verification records**: EV visit reports and action plans for 3 years
- **Appeals and complaints**: Assessment-related appeals and outcomes for 3 years

- **Reasonable adjustments**: Records of assessment adjustments and their effectiveness for 3 years

Internal Assessment Records (12 Months from Certification Date):
- **Formative assessment records**: Ongoing assessment feedback and progress tracking for 12 months post-certification
- **Summative assessment outcomes**: Final unit grades and completion records for 12 months post-certification
- **Assessment planning documents**: Assessment schedules and planning records for 12 months post-certification
- **Learner feedback**: Assessment-related feedback from learners for 12 months post-certification

Examination Records (2 Years Retention):
- **External examination scripts**: Marked exam papers and associated materials for 2 years
- **Exam board correspondence**: Communication with awarding bodies about exams for 2 years
- **Special arrangements**: Exam access arrangements and their implementation for 2 years
- **Exam centre reports**: Annual reports and statistical returns to exam boards for 2 years
- **Exam security records**: Invigilation reports and security documentation for 2 years

9.3 Extended Retention Periods
Employment Records:
- **Personnel files**: Core employment records for 7 years after termination
- **DBS checks**: Confirmation of checks (not certificates themselves) for duration of employment plus 6 months
- **Training records**: Professional development and qualification records for 7 years
- **Disciplinary records**: Formal disciplinary actions for 7 years after resolution
- **Health and safety records**: Accident reports and safety training for 7 years

Financial and Commercial Records:
- **Student fees and funding**: Financial records relating to learners for 7 years
- **Contracts and agreements**: Data sharing agreements and commercial contracts for 7 years after expiry
- **Insurance records**: Professional indemnity and public liability documentation for 7 years
- **Audit records**: Internal and external audit reports and working papers for 7 years

Safeguarding and Welfare Records:
- **Safeguarding records**: Child protection and vulnerable adult records until age 25 or 7 years after last contact
- **Welfare support records**: Mental health and wellbeing support documentation for 7 years
- **Reasonable adjustments**: Disability and learning support records for 7 years after programme completion
- **Incident reports**: Health, safety, and welfare incidents for 7 years

10. INDIVIDUAL RIGHTS UNDER UK GDPR

10.1 Right to Be Informed
Transparency Requirements:
- Clear and accessible privacy notices provided at point of data collection
- Layered approach to privacy information with summary and detailed versions
- Regular review and updating of privacy notices to reflect changes in processing
- Proactive communication about any significant changes to data processing

Privacy Notice Content:
- Identity and contact details of data controller and Data Protection Officer
- Purposes of processing and lawful basis for processing
- Categories of personal data and sources of data
- Recipients or categories of recipients of personal data
- Retention periods or criteria for determining retention periods

- Individual rights and how to exercise them
- Right to withdraw consent and right to complain to ICO

10.2 Right of Access (Subject Access Requests)
SAR Response Process:

- **Receipt and acknowledgement**: Written acknowledgement within 3 working days
- **Identity verification**: Appropriate verification of requestor identity and authority
- **Scope clarification**: Discussion with requestor to clarify scope of request where necessary
- **Data gathering**: Comprehensive search across all systems and locations
- **Response preparation**: Compilation of response in accessible format with explanatory information
- **Response delivery**: Secure delivery within one month of receipt (extendable by two months for complex requests)

Information to Provide:

- Confirmation of whether personal data is being processed
- Copy of personal data in intelligible format with explanatory information
- Purposes of processing, categories of data, and recipients
- Retention periods and sources of data where not obtained directly
- Information about automated decision-making including profiling
- Right to rectification, erasure, restriction, or objection

10.3 Right to Rectification
Rectification Process:

- **Receipt and assessment**: Evaluation of rectification request and supporting evidence
- **Investigation:** Verification of accuracy of existing data and proposed corrections
- **Correction implementation**: Update of records across all relevant systems and locations
- **Third party notification**: Communication of corrections to recipients where appropriate
- **Response to individual**: Confirmation of actions taken and any limitations or exceptions

Rectification Obligations:

- Correction of inaccurate personal data without undue delay
- Completion of incomplete personal data including supplementary statements
- Communication of rectification to recipients unless impossible or disproportionate effort
- Documentation of rectification actions for audit and compliance purposes

10.4 Right to Erasure (Right to be Forgotten)
Grounds for Erasure:

- Personal data no longer necessary for original purpose
- Withdrawal of consent where consent was the lawful basis
- Objection to processing where no overriding legitimate interests
- Personal data unlawfully processed or subject to legal obligation for erasure
- Personal data of child collected in relation to information society services

Erasure Process:

- Assessment of grounds: Evaluation of whether erasure request meets legal criteria
- Balancing test: Consideration of competing interests including freedom of expression
- Technical implementation: Secure deletion from all systems, backups, and archives
- Third party notification: Reasonable steps to inform recipients of erasure request
- Response and documentation: Confirmation to individual and maintenance of audit trail

10.5 Right to Restrict Processing
Grounds for Restriction:

- Accuracy of personal data contested by data subject
- Processing unlawful but data subject opposes erasure
- MGTS no longer needs data but individual requires it for legal claims
- Objection to processing pending verification of legitimate interests

Restriction Implementation:

- System flagging: Technical measures to prevent further processing

- Access controls: Limitation of access to restricted data to authorised personnel only
- Process documentation: Clear recording of restriction reasons and scope
- Lifting restrictions: Process for removing restrictions when grounds no longer apply

10.6 Right to Data Portability
Portability Requirements:
- Data processed by automated means based on consent or contract
- Provision of data in structured, commonly used, and machine-readable format
- Direct transmission to another controller where technically feasible
- No adverse effect on rights and freedoms of others

Portability Process:
- **Scope assessment**: Determination of data subject to portability rights
- **Format selection**: Agreement on appropriate format for data transmission
- **Data preparation**: Compilation of data in portable format with necessary validation
- **Secure transmission**: Direct transfer to new controller or secure provision to individual

10.7 Right to Object
Grounds for Objection:
- Processing based on legitimate interests or performance of public task
- Direct marketing (absolute right to object)
- Processing for scientific, historical research, or statistical purposes
- Automated decision-making including profiling

Objection Response:
- **Assessment of grounds**: Evaluation of reasons for objection and legal basis for processing
- **Balancing test**: Consideration of compelling legitimate grounds for continued processing
- **Cessation of processing**: Immediate cessation where no overriding legitimate interests
- **Alternative arrangements**: Implementation of alternative approaches where possible

11. DATA SHARING AND THIRD PARTY PROCESSING

11.1 Data Sharing Principles
Lawful Data Sharing:
- Clear lawful basis for all data sharing activities
- Data sharing agreements in place with all regular recipients
- Minimum necessary data shared for specified purposes
- Regular review of data sharing arrangements and their necessity

Data Sharing Categories:
- **Regulatory sharing**: Required disclosures to Ofsted, ESFA, awarding bodies
- **Employer sharing**: Learner progress and assessment information with employers
- **Subcontractor sharing**: Data processed by Reaseheath College and other partners
- **Professional sharing**: Information sharing for safeguarding and welfare purposes
- **Emergency sharing**: Urgent disclosures for health, safety, or child protection

11.2 Data Processing Agreements
Controller-Processor Agreements:
- Written agreements with all data processors under Article 28 UK GDPR
- Clear specification of processing purposes, duration, and types of data
- Processor obligations for security, confidentiality, and data subject rights
- Rights of audit, inspection, and termination of processing relationships
- Data breach notification requirements and incident response procedures

Key Processor Relationships:
- **IT service providers**: Cloud hosting, software maintenance, and technical support
- **Subcontractors**: Reaseheath College and other training delivery partners
- **Professional services**: Legal, HR, financial, and consultancy services
- **Marketing providers**: Email marketing, website management, and communications
- **Examination services**: Awarding bodies and assessment organisations

11.3 International Data Transfers

Transfer Safeguards:

- Adequacy decisions for transfers to countries with adequate protection
- Standard Contractual Clauses (SCCs) for transfers to non-adequate countries
- Binding Corporate Rules (BCRs) for multinational organisation transfers
- Regular review of transfer mechanisms and their continued validity

Transfer Documentation:

- Transfer impact assessments for high-risk international transfers
- Documentation of safeguards and protection measures
- Records of transfer recipients and purposes
- Regular review of transfer arrangements and security measures

12. DATA SECURITY AND TECHNICAL MEASURES

12.1 Technical Security Measures

Access Controls:

- **User authentication**: Multi-factor authentication for access to systems containing personal data
- **Role-based access**: Access permissions based on job role and business need
- **Regular access reviews**: Quarterly review of user permissions and access rights
- **Automated access management**: System-driven provisioning and de-provisioning of access
- **Privileged access management**: Enhanced controls for administrative and high-privilege accounts

Data Encryption:

- **Data at rest**: Encryption of databases, file systems, and storage devices
- **Data in transit**: Encryption of network communications and data transfers
- **Email encryption**: Automatic encryption of emails containing personal data
- **Mobile device encryption**: Full device encryption for laptops, tablets, and smartphones
- **Backup encryption**: Encryption of all backup media and cloud storage

12.2 Organisational Security Measures

Physical Security:

- **Secure premises**: Access controls, CCTV, and alarm systems for MGTS facilities
- **Clear desk policy**: Requirements for securing physical documents and materials
- **Secure storage**: Locked filing cabinets and secure storage areas for sensitive documents
- **Visitor management**: Sign-in procedures and escort requirements for visitors
- **Equipment security**: Asset tagging, inventory management, and secure disposal procedures

Personnel Security:

- **Background checks**: DBS checks and employment verification for all staff
- **Confidentiality agreements**: Signed confidentiality clauses in employment contracts
- **Security awareness**: Regular training on data security responsibilities and threats
- **Incident reporting**: Clear procedures for reporting security incidents and concerns
- **Access termination**: Immediate revocation of access upon termination of employment

12.3 Business Continuity and Disaster Recovery

Backup and Recovery:

- **Regular backups**: Automated daily backups of all systems containing personal data
- **Backup testing**: Regular testing of backup integrity and recovery procedures
- **Offsite storage**: Secure offsite storage of backup media with appropriate encryption
- **Recovery time objectives**: Defined targets for system recovery following incidents
- **Business continuity planning**: Comprehensive plans for maintaining operations during disruptions

Incident Response:

- **Incident response team**: Designated team with clear roles and responsibilities
- **Response procedures**: Step-by-step procedures for different types of security incidents
- **Communication plans**: Internal and external communication procedures during incidents

- **Recovery procedures**: Detailed procedures for system recovery and business resumption
- **Post-incident review**: Analysis of incidents and implementation of improvement measures

13. PRIVACY BY DESIGN AND IMPACT ASSESSMENTS

13.1 Privacy by Design Principles

Proactive not Reactive:

- Privacy considerations embedded in system design and business processes
- Anticipation and prevention of privacy issues before they occur
- Regular privacy risk assessments for new systems and processes
- Privacy champions in each department to promote privacy-aware practices

Privacy as the Default:

- Maximum privacy protection applied without requiring action from individuals
- Minimal data collection and processing as standard operating procedure
- Automatic application of appropriate retention periods and deletion schedules
- Default security settings that protect privacy and personal data

Full Functionality:

- Privacy protection that enables rather than restricts business operations
- User-friendly privacy controls and transparency measures
- Integration of privacy requirements with operational efficiency
- Innovation in privacy-protective technologies and approaches

13.2 Data Protection Impact Assessments (DPIAs)

When DPIAs are Required:

- Processing likely to result in high risk to rights and freedoms of individuals
- Systematic monitoring of publicly accessible areas on large scale
- Processing special category data or personal data relating to criminal convictions
- New technologies or innovative processing approaches
- Processing that may prevent individuals accessing services or opportunities

DPIA Process:

- **Scoping**: Clear description of processing operations and their context
- **Risk assessment**: Identification and evaluation of privacy risks to individuals
- **Mitigation measures**: Design and implementation of measures to reduce identified risks
- **Consultation**: Engagement with stakeholders including data subjects where appropriate
- **Review and monitoring**: Ongoing review of DPIA conclusions and risk mitigation effectiveness

13.3 Privacy-Enhancing Technologies

Technical Privacy Measures:

- **Pseudonymisation**: Replacement of identifying information with pseudonyms where possible
- **Data minimisation tools**: Automated systems to limit data collection to necessary minimum
- **Anonymisation techniques**: Statistical disclosure control and differential privacy methods
- **Access logging**: Comprehensive logging of access to personal data for audit purposes
- **Automated deletion**: System-driven deletion of data at end of retention periods

14. RESPONSIBILITIES

14.1 Board of Trustees

- **Strategic oversight**: Setting data protection strategy and risk tolerance
- **Performance monitoring**: Regular review of data protection performance and incidents
- **Resource allocation**: Ensuring adequate resources for data protection compliance
- **Accountability**: Ultimate accountability for data protection compliance and culture

14.2 Chief Executive Officer (David Bridgens)

- **Executive leadership**: Visible leadership and commitment to data protection principles
- **Strategic direction**: Integration of data protection into business strategy and operations
- **Resource provision**: Allocation of appropriate resources for data protection activities

- **Culture development**: Promoting a privacy-aware organisational culture
- **External accountability**: Representing MGTS data protection commitments to stakeholders

14.3 Quality and Compliance Manager (Jordan Geoghegan)
- **Policy oversight**: Supporting implementation of data protection policies and procedures
- **Compliance support**: Assisting with monitoring compliance with data protection requirements
- **Quality integration**: Ensuring data protection is integrated with quality management systems
- **Audit coordination**: Coordinating internal and external audits including data protection elements
- **Regulatory liaison**: Supporting engagement with regulatory bodies on compliance matters
- **Documentation support**: Supporting maintenance of compliance documentation and evidence

14.4 Data Protection Lead (Karli Soanes)
- **Policy implementation**: Leading day-to-day implementation of data protection policies
- **Compliance monitoring**: Monitoring compliance with data protection requirements
- **Training coordination**: Ensuring all staff receive appropriate data protection training
- **Incident management**: Leading response to data protection incidents and breaches
- **Stakeholder liaison**: Working with ICO, awarding bodies, and other data protection stakeholders
- **Documentation maintenance**: Maintaining records of processing activities and compliance evidence
- **Rights management**: Managing individual rights requests and subject access requests
- **Risk assessment**: Conducting privacy impact assessments and data protection risk evaluations

14.4 Director of Finance & HR (Ruth Smith)
- **HR data protection**: Ensuring compliance in all employment-related data processing
- **Staff training**: Supporting data protection training and awareness programmes
- **Employment practices**: Implementing privacy-aware recruitment and employment procedures
- **Financial data**: Ensuring appropriate protection of financial and payment data
- **Vendor management**: Data protection oversight of HR and finance service providers
- **Policy development**: Contributing to development of employment-related data protection policies

14.5 IT Manager/Service Providers
- **Technical security**: Implementing and maintaining technical security measures
- **System administration**: Secure configuration and management of IT systems
- **Access management**: Managing user accounts, permissions, and access controls
- **Backup and recovery**: Ensuring secure backup and disaster recovery procedures
- **Security monitoring**: Monitoring systems for security threats and vulnerabilities
- **Incident response**: Technical response to data security incidents and breaches

14.6 Curriculum Leaders and Teaching Staff
- **Learner data**: Appropriate handling of learner assessment and progress data
- **Assessment records**: Secure management of assessment evidence and feedback
- **Confidentiality**: Maintaining confidentiality of learner information
- **Data sharing**: Appropriate sharing of learner information with employers and partners
- **Privacy awareness**: Incorporating privacy awareness into learner interactions
- **Incident reporting**: Reporting data protection concerns and potential breaches

14.7 Training Development Advisers (TDAs)
- **Workplace data**: Secure handling of learner data in workplace environments
- **Employer liaison**: Appropriate data sharing with employers while protecting privacy
- **Mobile working**: Secure practices when working remotely or in employer premises
- **Progress tracking**: Secure recording and transmission of learner progress data
- **Confidentiality**: Maintaining confidentiality in workplace discussions and reviews
- **Incident awareness**: Recognition and reporting of data protection risks in workplace settings

14.8 All Staff Members

- **Personal responsibility**: Understanding and complying with data protection policies
- **Data handling**: Secure handling of personal data in daily work activities
- **Privacy awareness**: Considering privacy implications of decisions and actions
- **Training compliance**: Completing mandatory data protection training
- **Incident reporting**: Reporting data protection concerns and potential breaches
- **Continuous learning**: Keeping up to date with data protection requirements and best practices

15. COOKIES AND ONLINE PRIVACY

15.1 Website and Online Services

Cookie Policy:

- Clear information about cookies used on MGTS websites and online services
- Consent mechanisms for non-essential cookies
- Easy-to-use cookie preference settings
- Regular audit of cookies and tracking technologies
- Compliance with Privacy and Electronic Communications Regulations (PECR)

Online Privacy Measures:

- Privacy-friendly website design and functionality
- Secure transmission of all online form submissions
- Clear privacy notices for all online services
- Appropriate consent mechanisms for online data collection
- Regular security testing of web applications and services

15.2 Digital Learning Platforms

Learning Management Systems:

- Privacy-aware configuration of learning platforms
- Appropriate consent for learning analytics and tracking
- Secure handling of learner-generated content
- Clear data retention policies for online learning activities
- Regular review of platform privacy settings and data flows

Assessment Platforms:

- Secure online assessment and examination systems
- Appropriate identity verification without excessive data collection
- Secure storage and transmission of assessment responses
- Clear policies on monitoring and proctoring during assessments
- Compliance with awarding body requirements for digital assessment

16. SPECIAL CATEGORY DATA AND CRIMINAL CONVICTIONS

16.1 Special Category Personal Data

Categories Processed by MGTS:

- **Health data**: Medical information for reasonable adjustments and occupational health
- **Disability data**: Information about disabilities for support and accessibility purposes
- **Ethnic origin**: Equality monitoring and reporting data
- **Religious beliefs**: Accommodation of religious observances and dietary requirements
- **Sexual orientation**: Equality monitoring and anti-discrimination measures

Lawful Basis for Special Category Data:

- **Explicit consent**: Clear, informed consent for processing where appropriate
- **Employment law**: Processing necessary for employment rights and obligations
- **Vital interests**: Processing to protect life or physical safety of individuals
- **Equality monitoring**: Processing for equality of opportunity and treatment monitoring
- **Substantial public interest**: Processing for education and training provision

16.2 Criminal Convictions and Offences Data

DBS Checks and Criminal Records:

- Processing limited to roles requiring DBS checks under legal authority
- Secure handling and storage of DBS certificate information
- Confirmation records only - certificates not retained beyond verification
- Clear policies on recruitment decisions involving criminal records
- Compliance with Rehabilitation of Offenders Act and DBS Code of Practice

Safeguarding Context:

- Processing of criminal conviction data for safeguarding purposes
- Information sharing with police and social services where appropriate
- Secure record keeping for safeguarding investigations and actions
- Clear legal basis for processing under safeguarding legislation
- Regular review of necessity and proportionality of processing

17. DATA SUBJECT COMPLAINTS AND ICO REPORTING

17.1 Internal Complaints Process

Data Protection Complaints:

- Clear procedure for individuals to raise data protection concerns
- Designated contact points for data protection complaints
- Investigation process that is fair, thorough, and timely
- Written response to complainants with clear explanation of findings
- Escalation procedures for unresolved complaints

Complaint Resolution:

- Remedial action to address substantiated complaints
- System improvements to prevent recurrence of issues
- Communication of resolution to affected individuals
- Learning and improvement from complaint analysis
- Integration with overall complaints and quality processes

17.2 ICO Interaction and Reporting

Regulatory Relationship:

- Proactive engagement with ICO guidance and consultation
- Prompt response to ICO enquiries and investigations
- Cooperation with ICO audits and assessment visits
- Implementation of ICO recommendations and enforcement actions
- Regular review of ICO guidance and sector-specific advice

Annual Return and Reporting:

- Data protection fee payment and annual return submission
- Accurate reporting of processing activities and risk levels
- Updates to ICO registration following significant changes
- Sector-specific reporting requirements where applicable
- Transparency reporting on data protection activities

18. CONTACT INFORMATION AND SUPPORT

18.1 Internal Data Protection Contacts

Data Protection Lead: Apprenticeship Funding & Contracts Coordinator - Karli Soanes
Midlands Group Training Services Limited
Gulson Road, Coventry CV1 2JG
Tel: 02476 630333, Ext. 761
Email: karli.soanes@mgts.co.uk

Alternative Contacts:
CEO: David Bridgens - david.bridgens@mgts.co.uk
Quality and Compliance Manager: Jordan Geoghegan - jordan.geoghegan@mgts.co.uk

Director of Finance & HR: Ruth Smith - ruth.smith@mgts.co.uk
Post: Data Protection Requests, MGTS, Gulson Road, Coventry CV1 2JG

18.2 External Support and Regulatory Contacts
Information Commissioner's Office (ICO): Tel: 0303 123 1113
Website: www.ico.org.uk
Email: casework@ico.org.uk
Live Chat: Available on ICO website
ICO Breach Reporting: Online: https://ico.org.uk/for-organisations/report-a-breach/
Tel: 0303 123 1113
Professional Support: Association of Data Protection Officers (ADPO):
Website: www.dpo-association.org
International Association of Privacy Professionals (IAPP):
Website: www.iapp.org

19. APPENDICES

19.1 Glossary of Key Terms
Controller: MGTS as the organisation that determines the purposes and means of processing personal data

Processor: Third parties who process personal data on behalf of MGTS under written contract

Data Subject: Any identified or identifiable individual whose personal data is processed

Personal Data: Any information relating to an identified or identifiable natural person

Special Category Data: Sensitive personal data requiring additional protection (health, ethnicity, religion, etc.)

Lawful Basis: Legal justification for processing personal data under Article 6 UK GDPR

Consent: Freely given, specific, informed indication of agreement to processing

Data Breach: Breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access

Privacy Impact Assessment: Assessment of privacy risks associated with data processing activities

Data Protection by Design: Integration of data protection principles into system design and business processes

19.2 Quick Reference Guides
Subject Access Request Response Checklist:
- Identity verification completed
- Scope of request clarified
- Comprehensive data search conducted
- Third party data considered and redacted where necessary
- Response prepared in accessible format
- Response delivered within statutory timeframe
- Documentation maintained for audit purposes

Data Breach Response Checklist:
- Immediate containment measures implemented
- Incident documented with key details
- Risk assessment conducted
- ICO notification submitted if required (within 72 hours)
- Data subjects notified if high risk (without undue delay)
- Investigation completed and documented
- Remedial actions implemented
- Lessons learned and improvements identified

This policy demonstrates MGTS's commitment to protecting the privacy and personal data of all individuals with whom we interact. We recognise that trust is fundamental to our relationships with learners, staff, employers, and other stakeholders, and we are committed to maintaining the highest standards of data protection and privacy.

Policy Owner: Chief Executive Officer

Date	Summary of Changes	Version:	Author (Updated by):
19th January 2026	New policy implemented – all other versions of this policy have now been superseded	1.0	Jordan Geoghegan Quality & Compliance Manager

Next Review: See Document Control Register

Policy Approved By:

David Bridgens
Chief Executive Officer
19.01.2026