

# Responsible and Ethical AI Use Policy

Policy implemented: November 2025

Last reviewed: March 2026

Next review due: November 2026

Our policies are regularly updated and reviewed. However, occasionally policies may be reviewed after the set next review date after some consultation and research. In these rare occasions, the out-of-date policy will remain **VALID** until it is reviewed by the policy sponsor.

## 1. Summary

This policy establishes guidance and governance for the **safe, ethical, and responsible use of generative AI** across Salutem Care and Education. It ensures AI is applied to enhance operational efficiency, support professional decision-making, and improve the quality of care and education services, while maintaining the highest standards of privacy, safety, and regulatory compliance.

Generative AI technologies, including large language models such as ChatGPT, offer transformative potential in streamlining administrative processes, reducing paperwork, and providing actionable insights. This policy ensures that these benefits are realised responsibly and safely. However, these benefits must be balanced with robust safeguards to ensure compliance with the **UK Data Protection Act 2018, GDPR**, and sector-specific regulatory frameworks from the **Care Quality Commission (CQC), Ofsted, Estyn**, and **CIW**.

We are committed to leveraging AI responsibly to support colleagues, enhance service delivery, and uphold ethical standards. AI is to be used as a **colleague**, supporting human decision-making rather than replacing professional judgment. By adhering to this policy, colleagues contribute to a culture of **innovation, safety, and person-centred care**, ensuring that the dignity, privacy, and wellbeing of all individuals remain paramount.

## Scope

- Applies to all colleagues, including Support Workers, Managers, Principals, Senior Managers, and shared services colleagues.
- Covers any application of generative AI in documentation, analysis, communication, decision support, or service delivery.
- Relevant across Children's residential, Adult Residential, Day Care provisions, Supported Living, shared, and educational settings.
- Includes approved AI platforms (Ask Emma and Co-Pilot); prohibits use of public AI tools for sensitive or identifiable data.

## 2. Document Control

Initial purpose and scope of the new policy/procedure agreed by:	Melinda Glover, August 2025
Sponsor Technical review carried out:	Luke Laville, November 2025
Final Information Governance quality check carried out:	Melinda Glover, November 2025
Date implemented:	March 2026
Version Number:	V2.1
Date of the next review:	November 2026
Department responsible:	Quality Team and Digital & System Implementation
Job Title of Lead Person:	Group Improvement & Development Manager
Author / Main Contact, including their job title (if different from above):	Christopher Bell, Gary Laville, and Luke Laville.

In addition to this policy, local authorities and other commissioners may have their own policies, procedures and guidance which locations must comply with. These policies should complement this policy.

However, there may be additional requirements put in place by local authorities and other commissioners and these must be adhered to. Changes must not be made to Saludem's policies and procedures without corporate approval but, where needed, local procedures should be developed to accompany these.

### EQUALITY AND DIVERSITY STATEMENT

We are committed to the fair treatment of all in line with the Equality Act 2010. An equality impact assessment has been completed on this policy to ensure that it can be implemented consistently regardless of any such factors and all will be treated with dignity and respect.

# 3. Contents

- 1. Summary ..... 1
- 2. Document Control ..... 3
- 3. Contents ..... 4
- 4. Definitions ..... 5
- 5. Principles ..... 6
- 6. Areas of Governance ..... 8
- 7. Areas of Responsibility ..... 12
- 8. Learning and Development ..... 13
- 9. Associated Documents ..... 14
- 10. Useful Links ..... 15
- 11. References ..... 16
- 12. Version Control ..... 17

This policy must be brought to the attention of all employees.

The controlled version of this policy and its associated documents are available on BLINK. Printed or downloaded copies are uncontrolled and may not be up to date.

## 4. Definitions

**Artificial intelligence (AI):** Computer systems capable of performing tasks that typically require human intelligence, such as interpreting language, recognising patterns, making decisions, or learning from data.

**Generative AI:** A subset of AI that creates new content (e.g., text, images, audio) based on learned data patterns. Examples include ChatGPT, Claude, and large language models.

**Natural language processing (NLP):** A branch of AI focused on understanding, interpreting, and generating human language, enabling tools to draft documents, summarise records, and assist in communication.

**Digital social care data security and protection toolkit (DSPT):** A framework used to assess digital health and social care technologies, ensuring they meet standards for data protection, safety, and usability.

**Data protection impact assessment (DPIA):** A formal process to identify and mitigate risks related to personal data processing, required before implementing new ai tools or workflows.

**AI hallucinations:** Incorrect, misleading, or fabricated outputs generated by AI that must be identified and corrected to prevent errors or misinformation.

**Zero data retention:** A policy requiring that AI vendors do not store, reuse, or share any organisational inputs or sensitive data beyond the immediate session.

**Ask Emma:** Our approved AI platform, compliant with data privacy, security, and sector-specific regulations.

**Co-pilot, not autopilot:** The principle that AI supports human decision-making but does not replace professional judgement, especially in safeguarding, care planning, or education decisions. It does also not replace professional judgement during HR processes.

**Inclusive prompting:** The practice of using respectful, person-centred, bias-free language when interacting with AI systems to generate outputs.

**Trusted vendors:** AI providers that demonstrate compliance with GDPR, sector regulations, data security standards, and zero data retention policies.

**Feedback loops:** Mechanisms for colleagues to report experiences, challenges, or improvements related to AI tools to support continuous learning and refinement.

**Safeguarding alerts / decisions:** Situations where AI outputs may inform but cannot autonomously determine safeguarding actions for vulnerable children, adults, or students.

**Human oversight:** The requirement that a qualified professional reviews and validates any AI-generated content or recommendation before it influences care, education, operational or HR related decisions.

**Operational boundaries:** Clear limits on AI use, e.g., drafting documents allowed; autonomous safeguarding or HR decisions prohibited.

## 5. Principles

The following outlines the core principles underpinning the responsible and effective use of AI at Salutem Care and Education. AI is recognised as a **value-adding tool** that can automate routine tasks, streamline workflows, and provide actionable insights, allowing colleagues to devote more time to **person-centred care**. Human oversight remains essential; AI is designed to **support, not replace, professional judgement**. Safeguards, including **data protection by design**, ensure sensitive information is managed securely from the outset. Continuous improvement is embedded through colleague feedback, targeted training, and iterative refinement of AI tools and practices.

**Value-Adding Tool:** AI can enhance efficiency by supporting tasks such as drafting care documents, summarising records, generating reports, or providing data-driven insights. Leveraging **Natural Language Processing (NLP)**, AI can analyse language and trends within our systems, delivering intelligent, actionable insights to improve care and education outcomes.

**Human Oversight:** AI functions as a **colleague**, offering suggestions and supporting decision-making. Final decisions always rest with qualified professionals, ensuring that **compassion, expertise, and ethical judgment** remain central to care and educational practice.

**Data Protection by Design:** AI tools must comply with **GDPR, the UK Data Protection Act 2018**, and sector-specific regulations. Measures such as **zero data retention** with trusted AI partners are mandatory to safeguard sensitive health, personal, and educational information. We have completed the **Digital Social Care Data Security and Protection Toolkit (DSPT)** and commits to **annual reviews** to maintain compliance.

**Continuous Improvement:** AI systems evolve through **colleague feedback, ongoing training, and iterative refinement**, enhancing both service quality and operational efficiency. By integrating lessons learned and user insights, AI supports innovation and improved outcomes across children's, adult, Supported living, educational and shared services.

**Limitations of AI:** AI lacks the ability to experience empathy, moral reasoning, or ethical judgment. It cannot replace human understanding, professional intuition, or ethical decision-making. AI should therefore always be regarded as a **complementary tool** that enhances, rather than substitutes for, human judgement and care expertise.

**Output Quality and Verification:** Colleagues must critically evaluate all AI-generated outputs before incorporating them into official records. For example, when using AI to draft **care plans, personal plans, risk assessments, PDP or audit documents**, colleagues should:

- Review content for **accuracy, relevance, and appropriateness**.

- Identify and correct any **AI hallucinations**—false or misleading outputs that may occur.
- Cross-check information against **trusted sources**.
- Seek guidance from **senior colleagues** if there is any uncertainty.

Approved AI tools should provide **transparency**, including references or explanations for the outputs generated, to support verification and accountability.

**Generating Support Alongside the Decision Maker:** AI is intended to **support human decision-making**, not replace it. Colleagues must:

- Use AI-generated outputs as **drafts or decision support**, validating all critical content before adopting it into an individual's record.
- Avoid “black box” AI tools that do not provide sources or explanations for their outputs.
- Always maintain **human oversight**, ensuring final decisions are made by qualified professionals.

**Data Privacy and Security:** Protecting personal and sensitive data is paramount. Colleagues must:

- **Never input personally identifiable or protected health information** into unsecured public AI platforms (e.g., ChatGPT, Claude, Grok).
- Use **only approved platforms** that are Ask Emma or Co-Pilot, which comply with data protection standards.
- Ensure third-party vendors follow strict privacy requirements, including **zero data retention policies** and data processing agreements.
- Complete a **Data Protection Impact Assessment (DPIA)**, in consultation with the Data Protection Officer (DPO), before deploying new AI tools or workflows handling personal data.

**Bias Prevention and Inclusive Use:** AI tools must be used in ways that **promote equity, inclusivity, and person-centred practice**. Colleagues should:

- Apply **inclusive prompting**, ensuring language and outputs are respectful, unbiased, and person-centred.
- Flag and correct any AI outputs reflecting **stereotypes or discriminatory assumptions**. Repeated issues should be escalated to management for review and potential AI retraining.
- Exercise **professional judgement**, recognising that outputs may not fully reflect reality and should be corroborated with observation, direct engagement, and human insight.
- Critically assess the **source, reliability, and validity** of AI-generated information.

AI should be regarded as a **supportive tool**, complementing human expertise, active listening, and observational skills, rather than replacing professional judgment or ethical decision-making.

## 6. Areas of Governance

**AI in Safeguarding and Decision-Making:** AI must **never be used to make autonomous decisions** in safeguarding, clinical or HR-related scenarios. Human professionals are always required to validate and approve decisions affecting vulnerable children, adults, or students. AI should function as a “**co-pilot, not autopilot**”, supporting but never replacing professional judgment.

### Key Principles:

- **Human Oversight:** Final decisions, particularly those involving HR, safeguarding or vulnerable individuals, must always involve trained professionals.
- **Supplementary Role:** AI enhances decision-making by supporting analysis, summarisation, and documentation, complementing active listening, observational skills, and person-centred practices.
- **Transparency:** Any use of AI in decision-making must be documented internally. Colleagues should clearly acknowledge where AI contributed to decisions so that senior colleagues can review and maintain accountability.
- **Appeal and Review:** AI outputs do not eliminate errors; colleagues must maintain the ability to challenge, review, and amend AI-supported decisions as required.

### HR-Related Matters:

To ensure that HR-related matters are addressed in a timely and effective manner, we request that all communications be submitted in a direct and personal format. The use of automated tools, such as AI, to generate grievance submissions is not permitted. This can hinder our ability to properly assess and resolve the matter in a meaningful way. We ask individuals to engage personally when submitting concerns or responses within our internal processes, as this allows for clearer communication and more efficient resolution of issues.

### Meeting Notes and Documentation Guidance

- AI may draft or summarise meeting notes for internal reference.
- AI usage at meetings, Emma AI will detail the following message on joining meetings; *All parties agree the contents summary will be shared unless explicitly opted out during this meeting. Full transcripts are not to be shared internally or externally unless agreed with all participants.*
- All AI-generated notes must be **reviewed and approved by a line manager or qualified colleague**.
- Sensitive discussions, safeguarding, or HR content **cannot rely solely on AI summaries**.

- Storage, retention, and sharing must comply with organisational records management policy.

**People We Support Involvement:** Decisions affecting individuals must actively incorporate their **voices, views, and preferences**. All actions and decisions must comply with the **Mental Capacity Act 2005**, safeguarding legislation, and other relevant legal frameworks.

### **Policy Compliance and Colleagues Responsibilities**

- All colleagues are required to **familiarise themselves** with this policy.
- Managers are responsible for **reinforcing understanding** through team meetings and supervision.
- The **Data Protection Officer (DPO)** will oversee AI compliance, provide guidance, review DPIAs, and act as the point of contact for data subjects or regulatory authorities.
- **Subject Access Requests (SARs) and Information Rights:** Individuals (or their authorised representatives) have the right to request access to their personal data. Any Subject Access Request or other information rights request (e.g., rectification, erasure, restriction, objection) relating to AI-supported records or outputs must be handled in line with Salutem's Subject Access Request / Information Rights Policy and escalated promptly to the Data Protection Officer (DPO). Colleagues must not respond directly unless authorised, and must preserve relevant records (including AI-generated drafts that have been saved into official systems) in accordance with records management and retention requirements.

**DPO Responsibilities:** The DPO is responsible for:

- Ensuring compliance with **data protection regulations** and AI-related best practices.
- Providing guidance on **data privacy** in relation to AI systems.
- Reviewing and approving **Data Protection Impact Assessments (DPIAs)** for all AI projects.
- Acting as the primary contact for **data subjects and supervisory authorities** regarding AI and data protection concerns.

### **Training and Competency**

- **All Colleagues:** Basic orientation covering responsible AI use, data protection, and spotting inaccuracies.
- **Role Dependent:** Advanced training on verifying AI outputs, overseeing AI-based processes, and supervising teams using AI tools.

### **Monitoring, Audit, and Continuous Improvement**

- **Quality Audits:** Regular audits of AI-generated documents to ensure **accuracy, compliance, and safe use**.

- **Incident Response:** Any misuse, error, or data breach will be investigated under established disciplinary processes.
- **Continuous Improvement:** This policy and associated training will be **regularly reviewed** to reflect technological advancements, regulatory changes, and best practice.
- **Policy Updates:** Amendments will be made as required to remain compliant with legal and sector standards.

**Vendor Management: We will partner exclusively with AI vendors** who demonstrate:

- Compliance with **GDPR and sector-specific regulations**.
- Robust **data security measures** and zero data retention policies.
- Transparency and accountability in AI tool design and outputs.

## Family and Representative Communication

To ensure transparency, trust, and compliance with data protection and regulatory standards, colleagues must follow a formal process for informing families, carers, and relevant representatives about the intended use of AI. This process ensures that individuals and their families representatives understand how AI is used, what data is involved, and the safeguards in place to protect privacy, dignity, and wellbeing.

### 1. Advance Notification

Families, carers, and authorised representatives will be informed **in advance** whenever AI tools are used in ways that may relate to:

- Documentation, summarisation, or report drafting involving the individual
- Care planning or educational planning support
- Communication tools used in meetings or reviews
- Accessibility and personalised support technologies
- Any workflow where AI may process or analyse information connected to the individual

Notification will be delivered through existing communication channels.

### 2. Information Provided

Communication will include:

- The **purpose** of using AI
- The **type of AI tools** used (e.g., Ask Emma, Microsoft Copilot)
- The **data protection safeguards**, including zero data retention on processed data
- Assurance of **human oversight**, reiterating that AI does *not* make decisions

- Confirmation that no unapproved thirdparty AI systems are used
- How outputs are reviewed for accuracy, safety, and appropriateness
- The individual's and family's **rights**, including raising queries or concerns

### 3. Assurance of Safeguards

Families will be reassured that:

- Salutem only uses **approved, secure AI platforms** compliant with GDPR, the UK Data Protection Act, and sector regulators
- **No personally identifiable information** is entered into public AI systems
- AI functions strictly as a **supportive tool**, with final decisions always made by professionals
- AI-generated content is **reviewed and validated** by colleagues before being recorded or applied
- Data submitted to approved AI platforms is processed under a **zero data retention model**

### 4. Ongoing Engagement

Families will be:

- Offered opportunities to ask questions
- Informed of any significant updates or changes in AI-related processes
- Given explanations during reviews about how AI may have supported documentation or analysis

### 5. Consent and Legal Context

Use of AI does *not* replace or change requirements under:

- The Mental Capacity Act 2005
- Safeguarding legislation
- Data protection laws

Where formal consent is required under existing legal frameworks, those processes continue unchanged.

### 6. Responding to Concerns

Any family or representative raising concerns about AI use will receive:

- A clear explanation of how AI is used safely
- Assurance of human oversight
- Escalation routes

Concerns will be logged and reviewed as part of **continuous improvement** and **AI governance monitoring**

## 7. Areas of Responsibility

Effective governance and safe use of AI rely on clearly defined responsibilities at all levels of the organisation.

### Board / Executive Leadership

- Provide **strategic oversight** of AI adoption, governance, and ethical use.
- Ensure sufficient **resources, staffing, and training** are available for safe AI integration.
- Approve and periodically review the **AI Policy** and associated guidance.

### Data Protection Officer (DPO)

- Oversee compliance with **data protection regulations** related to AI systems.
- Provide guidance on **data privacy and security**, including DPIAs for new AI tools.
- Approve and review **Data Protection Impact Assessments (DPIAs)** for all AI projects.
- Serve as the **primary point of contact** for data subjects and regulatory authorities.

### Managers / Senior Colleagues

- Ensure colleagues **understand and adhere** to the AI policy.
- Facilitate **training, supervision, and discussions** on AI use within teams.
- Monitor **AI outputs, accuracy, and ethical application** in daily practice.
- Escalate incidents or concerns relating to AI misuse or data breaches.

### Colleagues

- Use AI tools in accordance with **policy, guidance, and approved platforms**.
- Critically review and **validate AI-generated outputs** before recording or implementing.
- Report **errors, biases, or unsafe practices** promptly to line managers or the DPO.
- Participate in **training, feedback mechanisms, and continuous improvement** initiatives.

### Systems / IT Team

- Ensure AI platforms are **secure, authorised, and regularly maintained**.
- Manage access controls, **user permissions, and software updates**.
- Support staff in **safe integration of AI into operational workflows**.

## Quality and Compliance Team

- Conduct **audits of AI-generated outputs** to ensure compliance with data protection, safeguarding, and regulatory standards.
- Monitor adherence to **policy, training requirements, and lessons learned**.
- Report findings to senior management and support continuous improvement.

## AI Vendors / External Partners

- Adhere to **trusted vendor agreements**, GDPR compliance, and zero data retention policies.
- Provide **transparent explanations of AI outputs** and ensure ethical, safe use.
- Collaborate with Saluitem colleagues to **resolve technical or operational issues** efficiently.

# 8. Learning and Development

We are committed to ensuring that all colleagues are **confident, competent, and safe** in their use of AI technologies. Ongoing learning and development are critical to maximise the benefits of AI while maintaining high standards of care, education, and operational excellence.

**Training and Support:** Colleagues will receive structured guidance on the **safe and effective use of AI**, including:

- Understanding the **capabilities and limitations** of AI systems.
- Recognising and correcting **inaccuracies or AI hallucinations**.
- Applying **best practice principles** in care, education, and operational workflows.
- Ensuring AI is used ethically, inclusively, and in line with regulatory requirements.

Training will be **role-specific**:

- **All colleagues:** Basic orientation covering responsible AI use, data privacy, spotting inaccuracies, and practical integration into daily tasks.
- **Role Dependent:** Advanced modules focusing on verifying AI outputs, overseeing AI-assisted processes, and ensuring compliance across sites.

**Neurodiversity and Inclusive Workspaces:** AI can unlock unique strengths within a neurodiverse workforce by providing tailored support, such as:

- **Personalised workspaces** that accommodate individual preferences.

- **Real-time transcription, summarisation, and accessibility tools** to enhance productivity and participation.
- Supporting an **inclusive and empowering work environment** that benefits all colleagues.

**Feedback and Continuous Improvement:** We will establish **feedback mechanisms** to capture staff experiences with AI, enabling ongoing refinement of tools, policies, and training. Key practices include:

- Encouraging colleagues to **share successes, challenges, and improvement suggestions**.
- Conducting **lessons learned reviews** whenever AI-related errors or issues occur.
- Documenting outcomes and sharing insights with **decision-makers** to promote accountability, service quality, and professional development.

**Key Outcomes:** Through effective learning and development, AI adoption will:

- Enhance **colleague confidence and competence**.
- Support **person-centred care and education** by freeing staff to focus on meaningful interactions.
- Promote a **culture of continuous improvement, inclusivity, and innovation**.
- Ensure compliance with **data protection, safeguarding, and ethical standards**.

## 9. Associated Documents

The following documents and policies support, complement, or provide additional context to the **Safe Use of AI Policy**:

- **Data Protection Policy** – Outlines organisational requirements for processing personal and sensitive data in compliance with GDPR and the UK Data Protection Act 2018.
- **Information Governance Policy** – Provides guidance on data security, confidentiality, and safe information handling across all services.
- **Safeguarding Children and Adults Policy** – Defines procedures for protecting children, adults, and vulnerable individuals, including reporting and escalation pathways.
- **Mental Capacity Act Policy** – Guidance on decision-making for individuals who may lack capacity, ensuring compliance when using AI in care planning.
- **Residential Care and Support Planning Policies** – Frameworks for drafting and reviewing support plans, risk assessments, and personal plans.
- **Incident Reporting and Whistleblowing Policy** – Procedures for reporting errors, AI misuse, or data breaches safely and transparently.
- **Information Technology and Systems Use Policy** – Rules and guidance for using IT systems, including AI platforms, safely and securely.

- **Equality, Diversity, and Inclusion Policy** – Supports inclusive practice and guides bias prevention in AI-generated outputs.
- **Training and Development Policy** – Outlines mandatory training, competency development, and continuous professional development, including AI-related training.
- **Clinical and Medication Policies** – Provide guidance for colleagues on safe administration of medicines and clinical interventions where AI may support documentation or scheduling.
- **Quality Assurance and Audit Policies** – Ensure monitoring, auditing, and continuous improvement of processes, including AI-assisted documentation and reporting.
- **Approved Vendor and Procurement Policy** – Sets out requirements for sourcing and approving AI vendors in line with regulatory, ethical, and security standards.

## 9. Useful Links

- **Ask Emma (Approved AI Platform)** – [Internal access link or portal]
- **Co-Pilot (Approved AI Platform)** – [Internal access link or portal]
- **NHS AI and Digital Regulations Service** – Guidance for safe and compliant AI use in health and social care: <https://www.digitalregulations.innovation.nhs.uk/>
- **Information Commissioner’s Office (ICO)** – Guidance on GDPR, Data Protection Act, and DPIAs: <https://ico.org.uk/>
- **Digital Social Care Data Security and Protection Toolkit (DSPT)** – <https://www.dsptoolkit.nhs.uk/>
- **Care Quality Commission (CQC)** – Regulatory standards for adult social care and health services in England: <https://www.cqc.org.uk/>
- **Ofsted** – Inspection and regulatory guidance for schools and educational settings: <https://www.gov.uk/government/organisations/ofsted>
- **Estyn** – Inspection framework for schools and education in Wales: <https://www.estyn.gov.wales/>
- **Care Inspectorate Wales (CIW)** – Regulatory guidance for social care and education services in Wales: <https://careinspectorate.wales/>
- **Mental Capacity Act 2005 Guidance** – Guidance on decision-making for individuals lacking capacity: <https://www.gov.uk/government/publications/mental-capacity-act-code-of-practice>
- **Working Together to Safeguard Children (2023)** – Statutory guidance for safeguarding children: <https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>
- **ISO/IEC 27001:2013 Information Security Management** – Guidance on information security for digital and AI systems: <https://www.iso.org/isoiec-27001-information-security.html>

## 10. References

- **UK Data Protection Act 2018** – Legal framework governing the processing of personal data in the UK, aligned with GDPR.
- **General Data Protection Regulation (GDPR) (EU) 2016/679** – European data protection regulation retained in UK law, governing processing, storage, and protection of personal data.
- **Digital Social Care Data Security and Protection Toolkit (DSPT)** – NHS framework assessing digital health and social care technologies for data security, privacy, and usability.
- **Data Protection Impact Assessment (DPIA) Guidance** – ICO guidance on assessing and mitigating risks when processing personal or sensitive data.
- **NHS AI and Digital Regulations Service** – AI regulatory framework for healthcare and social care digital technologies, provided by NICE, MHRA, HRA, and CQC.  
<https://www.digitalregulations.innovation.nhs.uk/>
- **Care Quality Commission (CQC) Regulations** – Regulatory standards for health and social care services in England, including digital record keeping and safeguarding.
- **Ofsted Inspection Framework** – Standards and guidance for education providers, including digital and technological compliance.
- **Estyn Inspection Framework (Wales)** – Regulatory framework for education providers in Wales.
- **Care Inspectorate Wales (CIW) Regulations** – Standards for social care and education services in Wales.
- **Mental Capacity Act 2005** – Legal framework for decision-making for individuals who lack capacity, including safeguards when using digital tools or AI in care planning.
- **Working Together to Safeguard Children (2023)** – Statutory guidance for safeguarding and promoting the welfare of children.
- **NHSX AI Guidance for Health and Social Care** – Guidance on safe, ethical, and effective use of AI technologies in healthcare and social care settings.
- **ISO/IEC 27001:2013 – Information Security Management** – International standard for managing information security risks, relevant for AI and data protection.
- **Top Employer & Disability Confident Guidance** – Best practice in workforce governance, inclusion, and compliance when adopting new technologies

## 11. Version Control

This is a controlled document. As a controlled document, any printed copies of this document, or saved onto local or network drives should be actively monitored to ensure the latest version is always available.

Version Number	Date	Status	Changes
V1	October 2025	Draft	New policy
V2	November 2025	Reviewed	Changes throughout
V2.1	March 2026	Addendum	Added – Family and Representative Notification Process