



Organisation: Unmask Your Potential Ltd

Policy owner: Helen Kent

Designated Safeguarding Lead: Helen Kent

Deputy Designated Safeguarding Lead: N/A

Online Safety Lead: Helen Kent

Version: 1.0

Date approved: 01/09/2025

Review date: 31/08/2026

10. Data Protection and Confidentiality Policy

10.1 Purpose

Unmask Your Potential Ltd is committed to protecting personal data, special category data and confidential information. This policy explains how Unmask Your Potential Ltd will comply with its obligations under the UK General Data Protection Regulation, the Data Protection Act 2018, safeguarding requirements and any contractual or data processing requirements agreed with Suffolk County Council.

This policy applies where Unmask Your Potential Ltd processes personal data in its own right and where it processes personal data on behalf of Suffolk County Council as part of contracted or commissioned services.

10.2 Scope

This policy applies to all directors, employees, associates, contractors, agency staff, sessional workers, volunteers and anyone acting on behalf of Unmask Your Potential Ltd.

It applies to all personal data and confidential information handled by the organisation, including information about:

- Children and young people
- Parents, carers and family members
- Staff, associates, contractors and volunteers
- Schools, commissioners and professionals
- Referrals, assessments and suitability information
- Attendance, engagement and progress records
- Risk assessments and support plans
- Safeguarding and child protection information
- Health, SEND, neurodiversity or wellbeing information
- Incident, concern and complaint records
- Communication with Suffolk County Council, schools or other agencies

10.3 Data protection principles

Unmask Your Potential Ltd will handle personal data in line with the data protection principles. Personal data will be:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date where required
- Kept only for as long as necessary
- Processed securely using appropriate technical and organisational measures
- Managed in a way that demonstrates accountability

10.4 Roles and responsibilities

The Director is responsible for overseeing data protection and confidentiality arrangements within Unmask Your Potential Ltd.

Data Protection Lead: Helen Kent

Telephone: 07944927395

Email: support@unmaskyourpotential.com

The Data Protection Lead is responsible for:

- Ensuring this policy is implemented and reviewed
- Responding to data protection queries
- Managing data protection risks and incidents
- Ensuring staff understand information handling responsibilities
- Liaising with Suffolk County Council where required
- Supporting responses to data subject rights requests
- Ensuring personal data is stored, shared, retained and destroyed securely

All staff, associates, contractors and volunteers must:

- Handle personal data lawfully, securely and confidentially
- Access only the information needed for their role
- Share information only where there is a legitimate reason
- Follow secure storage and transfer procedures
- Report data breaches, near misses or concerns immediately
- Follow safeguarding procedures where information indicates risk of harm

10.5 Controller and processor arrangements

Where Unmask Your Potential Ltd receives and processes personal data on behalf of Suffolk County Council as part of contracted services, Unmask Your Potential Ltd will act in accordance with the agreed contract, data processing agreement, information sharing agreement or commissioner instructions.

Unmask Your Potential Ltd will only process Suffolk County Council data for the agreed purpose of delivering, managing, safeguarding, reviewing and reporting on the commissioned service, unless there is a legal or safeguarding reason to do otherwise.

Where Unmask Your Potential Ltd determines the purpose and means of processing for its own business, legal, safeguarding or service records, it may act as a data controller for those records. Where roles and responsibilities are set out by Suffolk County Council, those arrangements will be followed.

10.6 Types of data processed

Unmask Your Potential Ltd may process:

Personal data

This may include names, dates of birth, addresses, contact details, school or education information, attendance information, referral information, family information and professional contact details.

Special category data

This may include information about health, mental health, SEND, neurodiversity, ethnicity, religion or belief, sexual orientation where relevant and lawfully shared, and other sensitive information required to support or safeguard the young person.

Criminal offence or risk-related information

Where relevant to safe delivery and lawful to process, Unmask Your Potential Ltd may receive or record information about offending, alleged offending, harmful behaviour, exploitation risks, police involvement or youth justice involvement.

Safeguarding information

This may include concerns, disclosures, referrals, risk assessments, child protection information, professional advice, agency communication and records of action taken.

10.7 Lawful basis and purpose of processing

Unmask Your Potential Ltd will process personal data only where there is a lawful basis. Depending on the circumstances, this may include:

- Performance of a contract or commissioned service
- Compliance with a legal obligation
- Protection of vital interests
- Performance of a task carried out in the public interest, where applicable through the commissioner's functions
- Legitimate interests, where appropriate and balanced against individual rights
- Consent, where this is appropriate and valid

Special category data will only be processed where an additional lawful condition applies, such as safeguarding children and individuals at risk, provision of support services, substantial public interest, health or social care purposes, or explicit consent where appropriate.

The main purposes for processing SCC data are:

- To assess suitability for provision
- To deliver commissioned services
- To safeguard children and young people
- To manage attendance, engagement and progress
- To complete risk assessments and support planning
- To communicate with SCC, schools, parents/carers and professionals
- To meet contractual monitoring and reporting requirements
- To manage incidents, concerns, complaints and safeguarding referrals
- To comply with legal, insurance and audit requirements

10.8 Privacy notice

Unmask Your Potential Ltd maintains a privacy notice explaining how personal information is collected, used, stored, shared and protected.

Privacy notice location: <https://unmaskyourpotential.com/privacy-policy/>

Where required, service users, parents/carers, staff and stakeholders will be directed to the privacy notice. Additional privacy information may be provided where a specific service, commissioner or data sharing arrangement requires this.

10.9 Confidentiality

All personal, sensitive and safeguarding information must be treated as confidential. Staff must not share confidential information unless there is a legitimate reason to do so.

Confidentiality may be overridden where necessary to:

- Safeguard a child or young person
- Prevent serious harm
- Comply with a legal obligation
- Support statutory agencies
- Fulfil contract or commissioner requirements
- Respond to a valid data subject rights request or regulatory requirement

Staff must never promise absolute confidentiality to children, young people, parents, carers or stakeholders. Where safeguarding concerns arise, information may need to be shared with the DSL, Suffolk County Council, children's social care, police or other appropriate agencies.

10.10 Access permissions

Access to personal, sensitive and safeguarding information will be managed on a strict need-to-know basis. Only authorised people who require access for delivery, safeguarding, management, administration, reporting or contractual purposes will be able to access relevant information.

Access permissions will be managed by the Director. Safeguarding records will be restricted to the Designated Safeguarding Lead, Deputy DSL and authorised personnel where access is necessary to protect a child or fulfil statutory duties.

Access will be reviewed regularly and whenever there is a change in staffing, role, contract, service involvement or provision. Access will be removed promptly when no longer required.

Access will be managed and audited by:

- Maintaining a record of authorised users and access levels
- Reviewing permissions periodically
- Checking that users only have access to information required for their role
- Reviewing safeguarding and service user record access where appropriate
- Monitoring information-sharing decisions and data handling practice
- Reviewing any data protection incidents, near misses or suspected unauthorised access

10.11 Secure storage of digital data

Where data is held digitally, Unmask Your Potential Ltd will use appropriate security controls to protect personal, sensitive and safeguarding information.

Controls may include:

- Password-protected devices and systems
- Access restricted to authorised users
- Need-to-know access permissions
- Multi-factor authentication where available
- Secure cloud-based or encrypted storage where appropriate
- Up-to-date antivirus and security software where applicable
- Screen locks and automatic locking where available
- Secure Wi-Fi use and avoidance of unsecured public networks when accessing sensitive data
- Secure deletion when records are no longer required
- Prompt removal of access when staff or contractors no longer require it

Safeguarding records will be stored separately from general service records where possible and appropriate.

10.12 Physical location of electronic data

Unmask Your Potential Ltd aims to ensure that electronic data is held within the United Kingdom wherever possible.

Electronic data may be held on secure password-protected devices and/or external cloud-based systems used for record keeping, communication, administration and service delivery. Where cloud-based systems are used, Unmask Your Potential Ltd will seek to ensure that data is stored in UK-based data centres or that appropriate UK GDPR safeguards are in place.

If any personal data is stored or processed outside the UK, this will only take place where there is a lawful basis and appropriate safeguards are in place, such as adequacy regulations, standard contractual clauses or equivalent contractual and security protections.

10.13 Paper records

Unmask Your Potential Ltd aims to keep paper records to a minimum. Where information supplied by Suffolk County Council is held in paper format, this will only be where necessary for delivery, safeguarding, risk management, attendance, emergency contact information or commissioner requirements.

Paper records will be:

- Accessed only by authorised staff on a need-to-know basis
- Stored securely in a lockable cabinet, drawer or locked location when not in use
- Kept under the control of the authorised staff member during sessions
- Not left unattended in public or shared spaces
- Not copied unnecessarily
- Kept secure during transport where transport is necessary
- Not stored in vehicles overnight
- Securely destroyed when no longer required

Safeguarding paper records will be stored separately from general service records where applicable.

10.14 Secure transfer of personal data with SCC

Personal data and special category data will only be transferred between Suffolk County Council and Unmask Your Potential Ltd where there is a legitimate reason and using secure, approved methods.

This may include secure email, encrypted attachments, password-protected documents, secure portals or other systems agreed with Suffolk County Council. Passwords for protected documents will be shared separately from the document itself.

Personal or special category data must not be transferred using personal email accounts, personal messaging apps, social media or informal channels.

Information will only be sent to named authorised recipients and checked before sending to reduce the risk of misdirection.

10.15 Information handling guidance

Unmask Your Potential Ltd will provide information handling guidance to staff, associates, contractors, volunteers and relevant stakeholders as part of induction, service set-up and ongoing working arrangements.

Guidance will cover:

- Sharing information securely
- Storing information securely
- Accessing information only where authorised
- Retaining information only for as long as necessary
- Destroying information securely
- Reporting data breaches or concerns
- Maintaining confidentiality
- Safeguarding information-sharing responsibilities

10.16 Data minimisation and accuracy

Unmask Your Potential Ltd will only collect and record information that is necessary, relevant and proportionate for the agreed purpose.

Records will be factual, accurate, respectful and kept up to date where required. Staff must avoid recording unnecessary personal opinions, excessive detail or irrelevant information.

Where inaccurate information is identified, it will be corrected or updated where appropriate.

10.17 Retention

Unmask Your Potential Ltd will retain information received from Suffolk County Council only for as long as necessary for the purpose for which it was shared, or where there is a legal, safeguarding, contractual, insurance or audit reason to keep it.

Where Suffolk County Council specifies a retention period within the contract, data sharing agreement or commissioning terms, this will be followed. Where no specific period is stated, Unmask Your Potential Ltd will apply a proportionate retention period based on the type of information held, the purpose of processing and safeguarding or legal requirements.

Information will not be kept for longer than necessary.

10.18 Secure destruction

At the end of the agreed retention period, personal data, special category data and safeguarding information will be securely destroyed unless there is a continuing legal, safeguarding, contractual, insurance or audit reason to retain it.

Digital records will be securely deleted from electronic systems, folders, devices and storage locations where appropriate. Where cloud-based systems are used, deletion will be completed in line with the system's secure deletion process.

Paper records will be shredded using a cross-cut shredder or disposed of through confidential waste arrangements. Paper records will not be placed in general waste or recycling.

Duplicate or working copies, including downloads, email attachments, printed notes or temporary files, will also be deleted or destroyed where they are no longer required.

A record of destruction may be kept where appropriate, including the type of information destroyed, date, authorisation and method used.

10.19 Data subject rights

Individuals have rights under data protection law, which may include the right to:

- Be informed about how their data is used
- Access their personal data
- Request correction of inaccurate data
- Request erasure in certain circumstances
- Restrict processing in certain circumstances
- Object to processing in certain circumstances
- Data portability, where applicable
- Not be subject to solely automated decisions with legal or similarly significant effects, where applicable

Any request relating to personal data must be passed to the Data Protection Lead promptly. Where the request relates to Suffolk County Council data or commissioned services, SCC will be informed or consulted where required by the contract or data processing agreement.

10.20 Data breaches and incidents

A data breach may include loss, theft, unauthorised access, misdirected email, accidental disclosure, cyber incident, loss of paper records, inappropriate sharing, unauthorised deletion or alteration of personal data.

Any actual or suspected data breach must be reported immediately to the Director /Data Protection Lead.

The Data Protection Lead will:

- Take immediate steps to contain the breach
- Assess what data is involved and who may be affected
- Consider the risk to individuals
- Inform Suffolk County Council where SCC data is involved
- Decide whether the Information Commissioner's Office must be notified
- Decide whether affected individuals must be informed
- Record the incident, decisions and actions taken
- Review learning and reduce the risk of recurrence

Where a breach may also indicate safeguarding risk, safeguarding procedures will be followed.

10.21 Use of IT suppliers and processors

Where Unmask Your Potential Ltd uses external IT suppliers, cloud service providers or other processors, appropriate supplier terms, contracts, service agreements or data processing terms will be in place.

Unmask Your Potential Ltd will only use suppliers that provide suitable assurances around data protection, confidentiality, access controls, security and compliance with UK GDPR and the Data Protection Act 2018.

10.22 Training and awareness

Staff, associates, contractors and volunteers will receive data protection and confidentiality guidance appropriate to their role. This may include:

- Secure handling of personal data
- Confidentiality and safeguarding
- Access permissions
- Secure storage and transfer
- Data minimisation
- Record keeping standards
- Breach reporting
- Subject access and individual rights
- Retention and secure destruction

10.23 Monitoring and audit

Compliance with this policy will be monitored through:

- Periodic review of access permissions
- Review of data handling and sharing arrangements
- Review of safeguarding and service user records where appropriate
- Review of data breaches, incidents and near misses
- Staff supervision and training records

- Contract review and commissioner monitoring where applicable
- Annual policy review

10.24 Review

This policy will be reviewed annually, or sooner if there are changes to legislation, statutory guidance, Suffolk safeguarding procedures or organisational practice.

This policy will be reviewed annually or sooner if:

- Statutory guidance changes
- Suffolk safeguarding procedures change
- There is a safeguarding incident or serious concern
- Provision changes significantly
- Commissioning requirements change

Approved by: Helen Kent

Role: Director

Signature:



Date: 01/09/2025