Policy Reference:		Org 4
Issue Number:		02
Date of Issue:		May 2022
Review date:		May 2023
Title:		Data Protection Policy
Policy Owner		Karen Thomas
Other Relevant Policies: Archiving and Retention policy, IT policy, Confidentiality policy, Professional Code of Conduct for Employees and Shared Lives Carers; Privacy Notice		

Everyone has rights with regard to how their personal information is handled and data protection is about ensuring people can trust you to use their data fairly and responsibly.

This policy aims to respect those rights and provides a framework for ensuring that ategi meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). It aims to prevent harm to those individuals we process data about by creating a responsibility for keeping the information as safe as possible.

Safety and providing quality services is at the heart of everything we do. It is very important to us that we keep all personal information that we hold safe and only use it in line with the data subject's wishes. We want everyone to be in control of their own data. There are no secrets when it comes to how we use data and we only process the information we need to support the work we do.

At ategi we require that personal data is:

- Processed fairly, lawfully and in a transparent manner;
- Used only for limited, specified and stated purposes as outlined in our privacy statement;
- Adequate, relevant and limited to what is necessary;
- Accurate and, where necessary, kept up to date;
- Not kept for longer than is necessary; and
- Kept safe and secure.

The types of personal data we are required to handle relates to:

- Employees (including agency staff)
- Volunteers (including trustees)
- The people we support and their relatives, next of kin or advocates
- People who are looking for support
- Carers, family linked carers and the people who live with them
- People who complain about our services
- Customers, suppliers and business contacts
- People who are interested in our work
- Visitors to our website

Any person in one of these categories is known and referred to as a data subject.

The information that belongs to them, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in Data Protection Law which is in force at any given time ('the Law') and other regulations. The Law imposes restrictions on how we may use that information.

Non-compliance

Non-compliance with the Law could result in damage to the data subject and to ategi's reputation. It could also result in financial sanctions imposed by the regulator – the Information Commissioners Office (ICO).

This policy applies to all the processing of personal data carried out by ategi including processing carried out by employees (including those working casual hours, temporary, agency, volunteers or work experience), joint controllers, contractors and processors.

This policy does not form part of any employee contract of employment and it may be amended at any time.

Any breach of this policy will be taken seriously and may result in disciplinary action.

To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law.

Our staff have access to a number of policies, operational procedures and guidance to give them appropriate direction on the application of the data protection legislation.

Information covered by Data Protection Legislation

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.

Some personal data is more sensitive and is afforded more protection, this is information related to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric ID data;
- Health data;
- Sexual life and/or sexual orientation; and
- Criminal data (convictions and offences)

Our Commitment

ategi is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about customers, staff or those who work or interact with us.

• ***Information Asset Owners*** – we assign an Information Asset Owner (IAO) to each information asset throughout the organisation, who together with a network of teams and staff with information management responsibilities aid the ICO in managing personal data and its associated risks.

• ***Privacy Notices*** - we publish a privacy notice on our website and provide timely notices where this is required. We track and make available any changes in our privacy notice.

• ***Training*** - we require all staff to undertake mandatory training on information governance and security which they re-take every year. In addition, all staff are required to attend a more detailed data protection training module as part of their induction.

• ***Breaches*** - we consider personal data breach incidents and have a reporting mechanism that is communicated to all staff. The DPO will assess whether we need to report breaches to the ICO as the Regulator of DPA. We take appropriate action to make data subjects aware if needed.

• ***Information Rights*** - we have a Data Protection Officer and clear processes to handle subject access requests and other information rights requests.

• ***Data Protection by Design and Default*** - we have a procedure to assess processing of personal data perceived to be high risk, that needs a Data Protection Impact Assessment (DPIA) carried out, and processes to assist staff in ensuring compliance and privacy by design is integral part to any product, project or service we offer.

• ***Policies and Procedures*** - we produce policies and guidance on information management and compliance that we communicate to staff.

• ***Communications*** - We have a clear communication plan which seeks to embed a culture of privacy and risk orientation.

• ***Contracts*** - Our Data Protection Officer oversees that our contracts are compliant with UK GDPR.

Individual Rights

Individuals have the right to be informed about the collection and use of their personal data.

All data subjects have the right to:

- ***Be Informed*** about how we use their data. We do this by providing a privacy notice on our website and at the point of collecting your data.
- ***Have personal data corrected if it is inaccurate.*** Any individual can make a request verbally or in writing and we have one calendar month to respond. We can refuse to comply with a request for rectification if the request is excessive, taking into account whether the request is repetitive in nature.

- ***Object to the processing of personal data.*** This right only applies in certain circumstances and all requests should be made directly to our data protection officer.

- ***Have personal data erased.*** This is also known as the 'right to be forgotten'. An individual can make a request verbally or in writing and we have one calendar month to respond. This right only applies in certain circumstances and all requests should be made directly to our data protection officer.

- ***Restrict the processing of personal data.*** An individual can make a request verbally or in writing and we have one calendar month to respond. This right only applies in certain circumstances and all requests should be made directly to our data protection officer.

- ***Request access to their personal data and information.*** An individual may exercise their legal right to access information by making a 'Subject Access Request' (SAR) at any time.

  An individual wishing to make a SAR should do so using a Subject Access Rest Form, sending the form to our Data Protection Officer. If you are requesting information on behalf of another individual we will require proof that you are acting with the authorisation of the data subject which includes a signed authorisation confirming the data subject's consent and evidence of the identity of the data subject.

  Responses to SARS must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject will be informed.

  All SARS received shall be handled by our Data Protection Officer.

We do not charge a fee for the handling of normal SARs but reserve the right to charge reasonable fess for additional copies of information that have already been supplied and for requests that are manifestly unfounded or excessive, particularly if requests are repetitive.

Data Protection by Design and Default

Data Protection Law requires us to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights.

This is 'data protection by design and by default'.

Identifying data protection risks at an early stage, and taking subsequent measure to address those risks, will help ategi to comply with the requirements of Data Protection Law.

Ategi is committed to considering data protection issues when designing and implementing systems, services, products and business practices. We will do this by asking project leads to follow our internal data protection procedures.

In doing so, we will make sure that data protection is considered at the earliest possible stage helping us to:

- Anticipate risks events before they occur, and take steps to prevent harm to individuals;
- Only process the personal data that we need to;
- Ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy;
- Adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data;
- Provide individuals with tools so they can determine how we are using their personal data;
- Offer strong privacy defaults, user-friendly options and controls, and respect user preferences;
- Only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design;
- Make sure that we only use designers and manufacturers who take data protection issues into account when using other systems, services or products in our processing activities; and

- Use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

Roles and Responsibilities

- The **Board** has overall responsibility for ensuring that the organisation complies with its legal obligations.

- The **Data Protection Officer (DPO)** is primarily responsible for advising on and assessing our compliance with the DPA and UK GDPR and making recommendations to improve compliance. Other responsibilities include:
  - Briefing the board on the organisation's legal obligations;
  - Reviewing data protection practices across ategi;
  - Reviewing and updating policies and procedures;
  - Advising employees on data protection issues;
  - Ensuring that data protection training takes place;
  - Ensuring notifications to the ICO;
  - Handing subject access requests;
  - Reporting data breaches;
  - Approving unusual or controversial disclosures of personal data;
  - Approving data protection clauses in organisational contracts;
  - Approving Data Protection Impact Assessments.

  The DPO is Lauren Osman at Modern Governance Solutions Limited, and she can be contacted at lauren.osman@moderngovernancesolutions.co.uk.

- The **Senior Information Asset Owner (SIRO)** owns the overall risk arising from the processing personal data by ategi.

  Our SIRO is our Chief Executive Officer, Kate Allen, and she can be contacted at KateA@ategi.co.uk.

- **Department Heads** are responsible for monitoring their own compliance with ategi policies and procedures and reporting back to the DPO if they have any queries or concerns. Additional key responsibilities are outlined in our procedures.

- **Employees and Volunteers** are required to read, understand, accept and follow our policies and procedures relating to data protection and account for them when handling personal data in the course of their work.

Monitoring Compliance with this policy will be monitored via the DPO and the responsible teams reporting to the board.

Definitions

'Consent' means the consent of the data subject which must be a freely given, specific, informed and unambiguous indication of the data subject's wishes by which they (by a statement or by a clear affirmative action) signify their agreement to the processing of the personal data relating to them.

'Data Controller' means the organisation (or individual) which, either alone or jointly with another organisation (or individual) decides why and how to process personal data.

The Controller is responsible for compliance with the DPA and GDPR.

'Data Processor' means a person or organisation which processes personal data on behalf of a data controller.

'Data Protection Legislation' means all applicable data protection and privacy laws including, but not limited to, the retained EU law version of the General Data Protection Regulation (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended and any successor legislation.

'Data Subject' means a living, identified or identifiable individual about whom the Data Controller holds personal data.

'EEA' means the European Economic Area consisting of all EU member states.

'Personal data' means any information relating to an identifiable living individual who can be identified from that data or from that data and other data.

This includes not just being identified by name but also by any other identifier such as ID number, location data or online identifier, or being singled out by any factors specific to the physical, physiological, genetic, mental, cultural or social identity of the individual.

'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored, or otherwise processed.

'Processing' means anything that is done with personal data, including collection, storage, use, disclosure, and deletion.

‘Pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

‘Special category personal data’ means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual’s sex life or sexual orientation.