# Data Protection Policy

| | |
|---|---|
| Policy implemented: | Sep 2019 |
| Last reviewed: | Dec 2020 |
| Next review due: | Dec 2022 |

## 1. Summary

There are a number of “information laws” which set out how organisations may process information about people, including the Data Protection Act 2018 (DPA), Digital Economy Act 2017, and the General Data Protection Regulation (GDPR).

Salutem  collects and looks after personal information about the people we support, relatives, staff and other people whom we work with in order to operate and provide our services. Salutem recognises that handling this information with care and confidentially is essential to delivering quality services and to maintaining trust between the organisation and the people whom it serves.

This policy provides a guide to the key elements of the legal framework governing information handling, outlines the responsibilities for managers and staff in relation to data protection and confidential information, and provides guidance for staff on all aspects of information handling.

The main objectives of this policy are:

- To demonstrate the ways in which Salutem ensure that personal data is handled effectively and securely
- To promote best practice in the processing of personal data
- To ensure all staff understand their responsibilities and Salutem’s obligations when handling personal data
- Comply with relevant legislation

# 2. Document Control

| | |
|---|---|
| **Initial purpose and scope of the new policy/procedure agreed by:** | Director of Quality and Goverance , (July 2019) |
| **Technical review carried out:** | Data Protection Officer, Aug 2019) |
| **Final quality check carried out:** | Group Head of Policy and Performance, Aug 2019 |
| **Date implemented:** | Sep 2019 |
| **Version Number:** | 3.0 |
| **Date of the next review:** | Dec 2022 |
| **Department responsible:** | Quality and Governance |
| **Job Title of Lead Person:** | Data Protection Officer |
| **Author / Main Contact, including their job title (if different from above):** | - |

Box below not relevant for HR Policies

In addition to this policy, local authorities and other commissioners may have their own policies, procedures and guidance which Services 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 Salutem's policies and procedures without corporate approval but, where needed, local procedures should be developed to accompany these.

**EQUALITY AND DIVERSITY STATEMENT**

The Salutem Group is 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



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

The controlled version of this policy and its associated documents are available on the P: drive, the T:/ drive and the eLFY bookshelf. Printed or downloaded copies are uncontrolled and may not be up to date.

# 4. Definitions

## Key Language

| | |
|---|---|
| Personal data | Any information about an identifiable living individual |
| Special category data | Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation |
| Data subject | The subject of the personal data, or the individual to whom it relates |
| Processing | Any action performed on or using personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction |
| Fair processing | What a reasonable person should expect an organisation to do with their personal data |
| Transparent | Concise, intelligible and easily accessible, using clear and plain language, in particular for any information addressed specifically to a child |
| Purposes | The reason(s) for which personal data are processed, which must be communicated to the data subject where personal data are processed with their consent or in the legitimate interests of the controller |
| Information governance | All the aspects of management of information within an organisation, including data protection, records management, and security |
| Records management | The supervision and administration of digital or paper records, including creation, receipt, maintenance, use and disposal |
| Data subject rights | The rights of the data subject to control aspects of how their personal data is used, and to gain access to the data |
| Subject access | The right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and information regarding its use |
| Restriction request | The marking of stored personal data with the aim of limiting their processing in the future |
| Rectification request | The right to obtain from the controller the rectification of inaccurate personal data concerning him or her or have incomplete information completed |
| Erasure request | Otherwise known as "the right to be forgotten", the data subject has the right (under certain circumstances) to have personal data concerning them erased |
| The right to object | The right to object, on grounds relating to his or her particular situation, at any time to processing of their personal data |
| Data portability | The right to receive personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided |
| Incidents | Any event of activity which does not comply with information law or documented organisational policies and procedures |

| | |
|---|---|
| Breaches | 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 |
| Data controller | The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data |
| Joint controller | Where two or more organisations determine the purposes and means of processing personal data, they become joint controllers |
| Data processor | A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller |
| Confidential information | All business or technical information, such as marketing and business plans, databases, specifications, formulations, prototypes, models, specifications, procurement requirements, engineering information, samples, computer software (source and object codes), forecasts, identity of or details about actual or potential customers or projects, techniques, inventions, discoveries, know-how and trade secrets |
| Legal base | The legal condition the data controller relies upon in order to process personal data |
| Consent | Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data |
| Vital interests | Processing necessary to protect the life, or, in extreme circumstances, the property, of an individual where they are incapable of giving consent to the processing |
| Legitimate interests | The legitimate interests of an organisation or third party, including processing in their commercial interests, which must be balanced against the interests, rights and freedoms of the data subject |
| Profiling | Processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements |

# 5. Principles

## Registration

The Digital Economy Act 2017 requires every data controller in the UK to register with a supervisory authority. In the UK, the supervisory authority is the Information Commissioner's Office (ICO), and the registration must include business contact information, outline the categories of data they hold about people, and what they do with it.

Details of Salutem's registrations can be found in the ICO Registrations spreadsheet held by the Data Protection Officer.

## Data Subject Rights

### Transparency

Article 12 of the GDPR states that 'The controller shall take appropriate measures to provide any information… relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language... The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.'

Salutem provides transparency information in the manner most appropriate to the purposes for processing the personal data.

- Service users are provided with transparency information when they enter a service, in accessible form if required
- A printed service user Privacy Notice and other associated printed materials are available at all services, including in accessible form
- Staff are provided with the Staff Privacy Notice upon commencing employment and the Notice is available to them on eLFY thereafter
- Salutem websites have a Privacy Notice & Cookie Policy, as well as Cookie Notice pop-up

All privacy and cookie notices are reviewed annually by the Data Protection Officer and updated where necessary.

### Data Subject Rights Requests

Salutem has a process for handling data subject rights requests, whether acting in their capacity as data processor or data controller.

For more information about each type of data subject right, please see the Definitions above or Data Subject Rights Processes.

Where a staff member is asked to routinely facilitate in some way the provision of information or process for handling data subject rights requests, they will be provided with suitable training by the Data Protection Officer.

## Data Sharing

Where Salutem acts as data processor, they may share personal data with sub-contractors to the extent specified in any contractual agreement with the data controller. However, in the majority of cases, Salutem will be the data controller.

Where Salutem is the data controller, they may share data with sub-processors, contractors and third parties in line with the original or a related purpose for processing, with a valid legal base upon which to rely, and where there are appropriate security safeguards in place. More information about secure mechanisms for data sharing can be found in the Information Security Policy.

Prior to any new data sharing activity, the Data Protection Officer should be consulted. Data sharing must be documented in contracts, through a Data Protection Impact Assessment process, or on the Data Sharing Checklist.

Where a sub-processor is required for a task involving the processing personal data, a contract must be in place prior to the activity taking place. The External Parties Information Security Questionnaire (due diligence check) must be conducted in cooperation with information technology staff and the Data Protection Officer.

**International Data Transfers**

International data transfers include not only the sharing of personal or confidential data with a person or organisation based outside of the European Economic Area (EEA), but also with companies whose servers are based outside of the EEA, organisations who may transfer the data outside of the EEA for their own purposes, and multinational companies who may share that data with, or allow access by, their global branches.

Salutem does not routinely transfer personal data outside of the EEA or to countries besides those which the European Commission has designated as having adequacy status. Should a one-off international data transfer (outside of the EEA and countries with adequacy) be proposed, the Data Protection Officer must be consulted prior to data being shared.

There is an International Transfers Checklist to be consulted and all international transfers shall be documented by the Data Protection Officer, including the appropriate security measures enacted to protect personal data.

**Post-Brexit**

Personal data relating to EEA citizens may not be transferred outside of the EEA without appropriate safeguards. Should the UK leave the EU with No Deal, we will be considered a “third country” outside the EEA – and therefore, under the GDPR, transfers involving the data of EEA citizens restricted. Although the UK will likely eventually be granted adequacy status by the European Commission, this process may take some time to complete.

Salutem processes data of UK citizens, but not of EEA citizens generally. Therefore, post-Brexit, as GDPR only applies to the data of EEA citizens, it is the organisation’s stance that Salutem will continue to be able to make business-as-usual data transfers.

In some cases, where a data processor’s servers are based in the EEA, it is deemed acceptable post-Brexit to transfer data into the EEA and return the same data to its place of origin in the UK. This decision has been made based on a judgement about the UK’s adequacy status (as we will continue to rely on the same data protection laws as the EEA), and as the data relates to UK citizen’s and was collected and otherwise processed in the UK. It will not be transferred, in the organisation’s opinion, to a region whose data protection and privacy laws vary in any way from those required in the EEA. Nor will it involve the processing of citizens of, or those who are resident in, the EEA.

However, post-Brexit, for the sake of ease the organisation will prefer, and seek to ensure that, all data processors appointed going forwards are based in the UK where possible.

## CCTV

Salutem uses CCTV systems at a number of sites for the purposes of the prevention and detection of crime.

Where services and offices utilise CCTV systems to cover a public area, and that CCTV is directed at viewing and/or recording the activities of individuals, we must ensure that it's use complies with the requirements of the GDPR and DPA.

The Service Manager must ensure that any CCTV system in place at their service is appropriately secured, for example that devices are stored in a locked room or cabinet. Any CCTV device used must encrypt wireless communication links and storage devices / recordings to a suitable level. In addition, the CCTV system must be of a standard capable of producing clear images.

Access to CCTV systems is restricted to senior management and service managers, and only permissible to be accessed in any case where a crime is suspected for the purposes of providing the relevant section of the footage to the appropriate authorities.

Where a new CCTV system has been commissioned, a Data Protection Impact Assessment must be completed.

Where a CCTV system is in place, that service shall prominently display a CCTV notice.

CCTV systems shall delete all images, recordings and back-ups in line with Departmental Retention Policy guidelines.

*For more information, please see CCTV Guidance.*

## Data Protection by Design

Recital (78) of the GDPR states that:

*When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.*

In practise, Data Protection by Design is a requirement to embed data protection in all areas of the business where personal data are processed. Salutem ensures we meet this requirement through the Data Protection Impact Assessment (DPIA) Process. The DPIA Process is only applicable where Salutem acts as data controller.

Where a DPIA is to be conducted the Data Protection Officer must be consulted. For more information, see the DPIA Process and associated guidance.

**Data Protection Impact Assessments**

Article 35 of the GDPR states that a Data Protection Impact Assessment is particularly required where:

1. Processing involves in particular the use of new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons
2. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
    a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
    b. processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences; or
    c. a systematic monitoring of a publicly accessible area on a large scale.

Where Salutem intends to conduct any activity involving a new technology, special category data, profiling activities, monitoring of a publicly accessible area, or which is likely to result in a risk to the rights and freedoms of the data subject, they must therefore consult the Data Protection Officer in order to conduct a DPIA. This consultation must take place at the planning stages of any new initiative.

A Data Protection Impact Assessment must consider at least the following aspects of Data Protection by Design, as set out by Article 25 and recital (78) of the GDPR:

- appropriate technical and organisational measures, such as pseudonymisation and data minimisation, which are designed to implement data protection Principles
- security measures to ensure that accessibility of the personal data is limited to authorised persons
- transparency with regard to the functions and processing of personal data
- measures where applicable enabling the data subject to monitor the data processing
- measures enabling the data controller to create and improve security features

*For more information, see the Data Protection Impact Assessment Process and Guidance.*

## Legal Bases

In order for processing to meet the requirements of **Error! Reference source not found.** a), the Data controller must be able to rely on one of the **Error! Reference source not found.** for processing as set out by the GDPR and Data Protection Act. This is a key component of any new or ongoing project, and

the Legal base must be identified in the Information Asset Register, as well as in any **Error! Reference source not found.**.

If the Processing involves Personal data, the legal base must be selected from those listed in Article 6 of the GDPR; if it involves Special category data, the Legal base must be selected from those listed in Article 9.

| Personal Data<br>*Article 6* | Special Category Data<br>*Article 9* |
|---|---|
| Consent | Explicit Consent |
| The performance of a contract | Employment and social security and social protection law |
| Compliance with a legal obligation | Vital interests, where the data subject is physically or legally incapable of giving consent |
| Vital interests | Membership activities of a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim |
| The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller | Manifestly made public by the Data subject |
| Legitimate interests | The establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity |
| | Substantial public interest |
| | Preventive or occupational medicine |
| | Public interest in the area of public health |
| | Archiving in the public interest, scientific or historical research or statistical purposes |

Where the Data controller wishes to rely on legitimate interests for processing, they must consult the Data Protection Officer in order to conduct a Legitimate Interests Assessment. You cannot rely on legitimate interests where the data concerned is special category or the data subject is a child.

The legal bases on which Salutem relies for the processing of personal and special category data are set out in the Article 30 Records, Information Asset Register, and applicable privacy notices.

Even where consent is not the legal basis for processing personal data, Salutem will give individuals as much control as possible over their own data. This includes asking permission to process and share their personal data.

As a social care and education provider, Salutem will take particular care in obtaining consent from the people we support. Salutem makes every effort with younger and more vulnerable service users to assist them in providing fully informed consent.

*For more information, see Legal Base Guidance.*

## Risk Management

### Incidents & Breaches

Where a staff member becomes aware of an Incident involving personal data or confidential information, they must immediately report the incident to the Data Protection Officer.

All incidents shall be recorded on c360 and the Non Conformance Register maintained by the Data Protection Officer.

Where an incident involves personal data, the Data Protection Officer shall follow the Incident Management Process and complete an Incident Management Form.

Where an incident rises to the level of a reportable breach, the Data Protection Officer shall follow the Breach Reporting Process.

The Data Protection Officer shall make a quarterly report of all incidents and breaches, for review by senior management.

### Risk Assessment

The Data Protection Officer shall conduct an annual information compliance internal risk assessment.

In addition, annual cyber security penetration testing shall be conducted by information technology providers. Ad hoc physical and social penetration testing shall be coordinated by the Data Protection Officer and conducted by a reputable and suitably experienced firm.

## Criminal Records Data

Salutem processes criminal records data in line with the Safeguarding Vulnerable Groups Act (SVGA) 2006 which requires enhanced DBS background checks to be conducted on all staff who work with children and vulnerable adults.

Access to this information is strictly controlled.

*For more information, please see the Criminal Records Data Guidance.*

## Children's Data

Salutem processes data about persons under the age of 13 in order to provide them with support and educational services.

*For more information, please see the Children's Data Guidance.*

## Accountability

Article 5(2) of the GDPR states that "The controller shall be responsible for, and be able to demonstrate compliance with, [the Principles]'. This is achieved through the Information Governance Self-

Assessment, against which the Data Protection Officer evidences compliance at the end of each compliance year (June – May). The results of this internal audit are shared with senior management and, where appropriate, all staff.

In addition, Salutem is required to complete the NHS' Data Security Protection Toolkit.

## Article 30 Records

Article 30(1) and (2) states that "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility", and "Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller".

Article 30 records must be maintained in writing and made available to the Information Commissioner's Officer on request.

The Data Protection Officer shall maintain Article 30 Records.

## Data Processor Obligations

Where Salutem acts as a data processor, they are bound by certain obligations. These include:

- Assisting the data controller with audits, responding to data subject rights requests, and liaison with the supervisory authority on request; as specified in any Data Protection Addendum of their contract
- Notifying the data controller if they believe that any aspect of processing may breach relevant law
- Providing adequate guarantees to the data controller of their ability to comply with relevant law
- Not acting in any manner contrary to the data controller's instructions when processing personal data
- Notifying the data controller within 24-hours of any breach
- Ensuring adequate contractual protections and data processing assurances from any sub-processors, conducting due diligence checks prior to onboarding, and audits to assure themselves of the sub-processor's ability to comply with relevant law
- Notifying the data controller of the intention to introduce or replace a sub-processor to process personal data, and giving them the opportunity to object
- Notifying the data controller in a timely manner in regards to any data handling complaints and assisting them with their response and investigation
- Providing the data controller with access to facilities or information regarding their data handling processes on request
- Complying with instructions regarding returning or erasing data

Any data controller requests for audit, access, or data protection information should be directed to the Data Protection Officer.

Where Salutem acts as the data processor, individual processes or internal instructions are in place to facilitate compliance with these obligations.

**Data Processor Audit**

Routine reviews of an organisation's data processors provide assurance that information is being treated in accordance with GDPR requirements in practise.

Salutem conducts annual audits of 25% of their data processors. For those large data processors, where a personal audit is impossible, Salutem will conduct a due diligence review. For data processors with whom there is a personal relationship with Salutem, an in-person review of the due diligence questionnaire will be conducted and data processors asked to provide appropriate evidence of practise.

## 6. Areas of Governance

This policy has been written with expert contribution from appropriate stakeholders. The Quality Assurance and Risk Management Group (QARM) will monitor, reflect on and gain organisational learning from the implementation of this policy. This policy will be reviewed and updated two years from implementation by QARM unless legal changes demand a more timely amendment.

The application of this policy and its associated documents is mandatory for all services staff, volunteers, agency staff and all other Salutem representatives. Staff understanding of this policy and associated documents will be assured through training, assessment of competency and supervision.

Staff understanding of this policy will be assured through training and the delivery of awareness raising workshops as deemed necessary by QARM. The people we support will be involved in the review to ensure it captures the important issues for them.

## 7. Areas of Responsibility

*The Data Protection Policy applies to all business areas where Salutem handles personal data, and to all staff.*

*Data Protection and Confidentiality is a component of information governance and as such this policy and associated procedures form part of Salutem's overall Information Governance Framework.*

*Further details of individual responsibility by role can be found in the Information Governance Framework document.*

## 8. Learning and Development

Salutem is committed to ensuring that all staff are aware of what is expected of them so that everyone is appropriately supported. Staff should speak to their line manager in relation to their learning needs using supervision and through the appraisal process.

The Education and Awareness Raising Plan sets out how Salutem ensures that all staff receive appropriate data protection training and how awareness raising activities are undertaken to further this training and support engagement with the Information Governance Programme.

## 9. Associated Documents

The GDPR sets out six data protection Principles, which all organisations processing personal data must follow:

1. Personal data shall be:
    a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
    b. collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes;
    c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
    d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
    e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
    f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('Accountability')

This Policy sets out how Salutem will comply with Principles a), b), c) and f) and other requirements of the GDPR, Digital Economy Act and DPA, such as Data Protection by Design and maintaining records under Article 30.

The Records Management Policy sets out particularly how Salutem will comply with Principles d) and e), concerning data minimisation measures, accuracy and integrity of information, and storage limitation. The Information Security Policy contains further information, in particular, for example, more detailed systems security information, which is of relevance when considering how Salutem complies with Principle f) and should be read in conjunction with this Policy.

Additional information regarding Salutem's compliance with these Principles can be found in supplementary policy and procedural documentation, such as the data subject rights processes.

The key documents for the Information Governance Programme are set out in the Information Governance Policy Suite Map.

# 10. 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 |
|---|---|---|---|
| V2.0 | Aug 2019 | Draft | New policy |
| V3.0 | Dec 2020 | Reviewed | Minor changes |
| | | | |
| | | | |
| | | | |

Please see the Equality Impact Statement for all Information Governance Policies.