DATA PROTECTION, STORAGE AND RETENTION POLICY

All reference to personnel includes both paid employees and volunteers. This policy applies to all Anglia Care Trust activities irrespective of location, all staff and direct contractors.

Keeping data is important to us at Anglia Care Trust and we take the security of personal data seriously as it must be protected.

General Data Protection Regulation and Data Protection Act 1998

From 25 May 2018, existing data protection duties have been tightened up under the EU General Data Protection Regulation (GDPR) and this has transformed the way in which personal data (including personal sensitive data) is collected, shared and used. It aims to strengthen the rights of individuals, particularly with regard to consent. The GDPR will see organisations held to higher standards than ever before in terms of their use of personal data, with severe penalties for non-compliance.

Anglia Care Trust must be compliant with the EU General Data Protection Regulation (GDPR). It protects personnel against the misuse of personal data and covers both manual and electronic records.

Why do we hold personal data?

We hold personal data and sensitive personal data to enable us to manage our personnel, to deliver a service to our service users and to manage the health and safety of our personnel and service users.

The GDPR applies to both personal and sensitive personal data:

Personal data

This is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

Sensitive personal data

The GDPR refers to sensitive personal data as “special categories of personal data.” The special categories specifically include genetic data and biometric data where processed to uniquely identify an individual.

Sensitive personal data includes information relating to the following matters:

- the member of personnel’s racial or ethnic origin
- his or her political opinions;
- his or her religious beliefs

- his or her trade union membership his or her physical or mental health or condition
- his or her physical or mental health or condition,
- his or her sex life; or
- the commissions or alleged commission of any offence by the member of personnel.

We will not hold or process sensitive personal information unless the security and management arrangements of the GDPR higher standards have been met.

The member of personnel's written consent will be sought at the point at which sensitive personal data is collected.

Holding personal data

GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- 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.

Purposes for which personal data may be held

Personal data relating to personnel may be collected primarily for the purposes of:

- recruitment, promotion, training, redeployment and/or career development;
- administration and payment of wages and expenses;
- calculation of certain benefits including pensions;
- disciplinary or performance management purposes;
- performance review;
- recording of communication with employees and their representatives;
- compliance with legislation;
- provision of references for financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers; and
- staffing levels and career planning.

Anglia Care Trust considers that the following personal data falls within the categories set out above with respect to personnel:

- personal details including name, address, age, status and qualifications. Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant;
- references and CVs;
- emergency contact details;
- notes on discussions between management and the employee;
- appraisals and documents relating to grievance, discipline, promotion, demotion or termination of employment;

- training records
- salary benefits and bank/building society details; and
- absence and sickness information

With respect to Service Users, Anglia Care Trust considers that the following personal data falls within these categories:

- personal details including but not limited to name, address, age and family members where appropriate to the service. Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant;
- notes on discussions between staff and Service Users include support plans and risk assessments;
- file notes and correspondence detailing communications from third parties relevant to the service being provided.

Privacy Notices

We will be open, accurate, and clear in explaining how personal data will be used. Individuals will be advised by Anglia Care Trust of the personal data which has been obtained or retained, its source, and the purposes for which the personal data may be used or to whom it will be disclosed through the relevant Privacy Notice.

We will make privacy notices available to personnel and service users and will ensure these can be accessed through our website www.angliacaretrust.org.uk

Anglia Care Trust will review the nature of the information being collected and held on an annual basis to ensure there is a sound business reason for requiring the information to be retained.

Lawful bases for processing personal data

In order to process personal data, there must be a lawful basis which requires that processing is 'necessary'. It must be a targeted and proportionate way of achieving the purpose. If you can reasonably achieve the same purpose without the processing, there is no lawful basis. The lawful bases are:

- Consent - the individual has given clear consent for you to process their personal data for a specific purpose
- Contract - the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legal obligation - the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests - the processing is necessary to protect someone's life.
- Public task - the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- Legitimate interests - the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Therefore, to ensure compliance with GDPR and in the interests of privacy, personnel confidence and good personnel relations, the disclosure and use of information held by Anglia Care Trust is governed by the following conditions:

- personal data must only be used for one or more of the purposes specified in this Policy or the relevant Privacy Notice;
- Anglia Care Trust documents may only be used in accordance with the statement within each document stating its intended use; and provided that the identification of individual personnel is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external requests for data (e.g. surveys, staffing level figures); and
- personal data must not be disclosed, either within or outside Anglia Care Trust, to any unauthorised recipient.

Rights of the Individual

GDPR is more specific in the rights it provides for individuals. It specifies the following rights for any individual for which personal data is held by Anglia Care Trust:

- Individuals have the right to be informed about the collection and use of their personal data. It emphasises the need for transparency over how their personal data is used.
- Individuals have the right to access their personal data and supplementary information
- Individuals have a right to have inaccurate personal data rectified if inaccurate, or completed if it is incomplete
- Individuals have a right to have personal data erased and to prevent the processing of this data. The right to erasure does not provide an absolute 'right to be forgotten'.
- Individuals have the right to request the restriction or suppression of processing their personal data.
- Individuals have the right to data portability to obtain and reuse their personal data for their own purposes across different services.
- Individuals have the right to object to processing of their data based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.
- Individuals have rights in relation to automated decision making and profiling. GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual).

Access to personal data (Subject access requests)

Under GDPR, individuals have the right to access personal data held about them so that they can verify the lawfulness of the processing of their data. Requests should be made in writing to the Director of Business Support using the below contact details and detailing the information required:

Email: admin@angliacaretrust.org.uk (for the attention of the Director of Business Support)
Via post: Director of Business Support, Anglia Care Trust, Unit 8 The Square, Martlesham Heath, Ipswich, IP5 3SL

The Director of Business Support will take suitable measures to verify their identity and will provide the information in a commonly used electronic format. Data will be provided free of charge within 1 month from the written request. However, should the request be deemed unfounded or excessive (eg repetitive requests to provide data or requests for further copies of data), a £10 administration fee will be charged.

Anglia Care Trust will extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, they will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Anglia Care Trust reserves the right to refuse to respond to a request that is considered unfounded or excessive and will the reason to the individual, informing them of their right to complain to the supervisory authority.

To make a request for deletion or rectification of data, a written request should be sent to the above address detailing the information that is believed to be inaccurate and evidence of why it needs correcting. Receipt of requests will be confirmed in writing.

Management of data

Anglia Care Trust will adhere to the following actions when managing data and expects all personnel to do the same:

- We will hold the minimum amount of data that is necessary for the function of our services
- We will keep information up to date and correct any inaccurate data that is identified (as outlined below)
- We will not hold data longer than is necessary for our business purposes (see retention information below)
- We will not export your data overseas without ensuring appropriate data protection arrangements are in place
- We will not use automated decision making solely when making a decision which will have a direct impact on an individual.

Disclosure of personal data

Personal data may only be disclosed outside Anglia Care Trust without the individual's written consent, where disclosure is required by laws, where there is immediate danger to the employee's health or where the risk of danger of harm to the individual or another person or property is suspected.

Accuracy of personal data

Anglia Care trust will review personal data regularly to ensure that it complies with the conditions outlined in the policy to date.

With respect to personnel, in order to ensure Anglia Care Trust's files are accurate and up to date, and so that Anglia Care trust is able to contact the member of personnel or, in the case of an emergency, another designated person, the member of personnel must notify Anglia Care Trust as soon as possible of any change in their personal details (e.g. change of name, address, next of kin details etc)

Data Protection Audit

With respect to personnel, standard reports of personal records will be issued to all personnel on an annual basis for the purpose of ensuring the data is up to date and accurate. Personnel will be entitled to amend any incorrect details and these corrections will be made to all files held on Anglia Care Trust's information systems. In some cases, documentary evident e.g. qualification certificate, will be requested before any changes are made.

Once complete, these records will be stored in the member of personnel's personnel file.

With respect to Service Users, Operational Managers will be responsible for ensuring that all records are audited annually to ensure that they comply with the aforementioned criteria.

Data Storage Policy Statement

Anglia Care Trust stores data in two ways, hard and computerised. It is important that Anglia Care Trust builds a relationship of trust with its Service Users, other agencies and its personnel in relation to the storage of data.

Therefore Anglia Care Trust has the responsibility to ensure that all data relating to its business activities is stored in a safe, secure and confidential way. In order to ensure that the organisation not only complies with GDPR and that privacy and confidentiality are ensured, the following guideline will be followed:

All personnel have the responsibility for ensuring that information they store relating to the business of Anglia Care Trust is stored safely, securely and confidentially in line with GDPR requirements whether this is computerised data or hard data.

Security

To enable personnel to carry out their responsibilities the following security measures have been adopted:

- Mobile phones will be kept secure at all times with a 4 digit PIN. If lost or mislaid personnel should inform their line manager as soon as possible.
- Computer systems are password protected and all data on the server requires 2 forms of authentication to be accessed.
- Personnel should ensure that their own password and mobile phone PIN is not shared with others
- Information stored on the network system is stored on five levels. Level zero and one can be accessed by all salaried personnel, level two by co-ordinators, managers and the Directors. Level three can be accessed by managers and the Directors. Level four can be accessed by the Directors only.
- Data should only be saved on the G drive and not on the hard drive of either a laptop or desktop.
- Lockable filing cabinets are provided for the storage of hard data and should be used for all personal data
- Service Users' and personnel information, together with hard data relating to the business of Anglia Care Trust, should be locked away at all times if not being used
- Keys to filing cabinets should be stored in a safe place
- Hard data that is no longer required must be shredded or placed in white security bags to be shredded
- Contact details and messages on mobile phones should be limited only to those relevant to current casework.
- Accounting data is stored for seven years in a locked filing cabinet or suitable secure storage facility
- Service User data is stored for five years in a locked filing cabinet or suitable secure storage facility

- Data relating to unsuccessful job applications is shredded within six months of interviews having taken place to allow time for feedback and any follow up queries
- Data relating to the work of Anglia Care Trust may at times need to be shared with other personnel. This must be dealt with in a confidential manner
- Photocopied/printed data should not be left on top of the photocopier. Any unnecessary copies should be shredded
- Open access data should not contain information that is confidential.
- A clear desk policy will be adopted and at the end of each working day, all papers will be cleared away and secured.
- Hard copies of sensitive personal data should only be kept if necessary and should be kept in a locked cabinet when not in use.
- Personnel will only use memory devices and IT equipment authorised by Anglia Care Trust.
- Personnel will adhere to the guidelines outlined in the Fair Use of Internet Policy.

Responsibilities for storage of hard data and computerised data

- Personnel files are kept in a locked cabinet
- Legal documentation, Service Level Agreements and contracts are kept in a locked filing cabinet
- All personnel have the responsibility of ensuring that the data and records that they store are kept safe and secure
- The Director of Business Support has the responsibility of ensuring that all financial documentation, information, chequebooks and such like are kept secure; this relates to both hard and computerised data
- The Director of Business Support has the responsibility of ensuring that data relating to the finances of the organisation are kept secure for seven years. For all other data see Data Retention
- Personnel transporting hard or computerised data must ensure that this is kept safe at all times and not left in vehicles unattended at any time
- There should be no need for data to be kept at personnel's homes. If this need occurs, arrangements for storage will be agreed with the Director of Business Support on an individual basis
- It is the responsibility of the Business Support Team to ensure that all correspondence delivered to Anglia Care Trust's registered office is dealt with in the strictest confidence and that it reaches the person for whom it is intended.

Third parties we work with

Depending on the type of organisation, Anglia Care Trust will undertake one of the following actions:

- Review their terms and conditions to ensure they protect data in accordance with GDPR requirements
- Provide details of the information we hold and process, ensure they understand their responsibilities in helping us secure it and formally agree the arrangements

Data Retention and destruction of data

Data will be retained in line with the guidance set out by the Professional Standards Authority. More information can be found at https://www.professionalstandards.org.uk/home
Once the retention period has elapsed, we will ensure that any information is immediately and suitably destroyed by secure means i.e. by shredding. While awaiting destruction, information will not be kept in any insecure receptacle.

Data Protection Breach

Anglia Care Trust has a duty to report a personal data breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, where feasible.

Any member of personnel that becomes aware of a potential breach must report this to the Director of Business Support immediately. It is the responsibility of the Director of Business Support to investigate whether a breach has taken place and if so, to report the details of the breach to the ICO.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must also be informed without undue delay.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:

- access to personal data by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data

Records of processing activities

Anglia Care Trust will hold an internal record of all processing activities. This record will include the following:

- Name and details of the organisation (and where applicable, of other controllers, representative and data protection officer)
- Purposes of the processing
- Description of the categories of individuals and categories of personal data
- Categories of recipients of personal data
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

Compliance

Failure to comply with this policy by personnel will be dealt with under our disciplinary procedure.

Date of next review – October 2019