Personnel Privacy Notice

Keeping your data is important to us at Anglia Care Trust and we take the security of your personal data seriously as it must be protected. Our Privacy Notice informs you of how we take care of the safety and security of your personal information.

The Data Protection Act

The General Data Protection Regulation 2016 (GDPR) requires us to manage personal information in accordance with Data Protection Principles. In particular the Law requires us to process your personal information fairly and lawfully. This means you are entitled to know how we intend to use any information you provide. You can then decide whether you want to give it to us in order that we may provide the product or service that you require. All our employees are personally responsible for maintaining confidentiality and will do their utmost to keep all data accurate, timely and secure. We provide training and education to all employees to remind them of their legal obligations.

What is personal data?

Personal data is any information about a living individual which allows them to be identified from that data (for example a name, photograph, video, email address, or address). Identification can be direct, using the data itself or by combining it with other information which helps to identify a living individual. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by Anglia Care Trust (ACT). We are the Data Controller for your data.

Other Data Controllers ACT works with and Information Sharing

- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers

We may need to share personal data we hold with them so that they can carry out their responsibilities. The organisations referred to above will sometimes be “joint data controllers”. This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration then the data controllers will be independent and will be individually responsible to you.

ACT will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

What data do we process?

- Names, titles, and aliases, photographs.
- Start date / leaving date
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in an application form, CV or cover letter or as part of the application process and referral source.
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

We use your personal data for some or all of the following purposes:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you

- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records.
- To seek your views or comments.
- To process a job application.
- To provide a reference.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest.

How we use sensitive personal data

- We may process sensitive personal data relating to staff and volunteers including, as appropriate:
    - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
    - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;

- in order to comply with legal requirements and obligations to third parties.

- These types of data are described in the GDPR as “Special categories of data” and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
  - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
  - Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it so that you can carefully consider whether you wish to consent.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public.
- We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect personal data about criminal convictions as part of the recruitment process or we may be notified of such personal data directly by you in the course of you working for us.

What is the legal basis for processing your personal data?

Some of our processing is necessary for compliance with a legal obligation.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

We will also process your data in order to assist you in fulfilling your role including administrative support or if processing is necessary for compliance with a legal obligation.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of our tasks or where you first give us your prior consent. It is likely that we will need to share your data with:

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions , or to maintain our database software;
- Other persons or organisations operating within local community.
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Credit reference agencies
- Professional advisors
- Trade unions or employee representatives
- Training providers

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We are permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims. We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

We use the Professional Standards Authority as a guide to the retention of data. More information can be found at https://www.professionalstandards.org.uk/home

Your responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with personal data

You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. **The right to access personal data we hold on you**

At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from.

Once we have received your request we will respond within one month. There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2. **The right to correct and update the personal data we hold on you**

If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. **The right to have your personal data erased**

If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.

When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4. **The right to object to processing of your personal data or to restrict it to certain purposes only**

You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5. **The right to data portability**

You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. **The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained**

You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. **The right to lodge a complaint with the Information Commissioner's Office.**

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and

whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on www.angliacaretrust.org.uk and also on our internal G drive.

This Notice was last updated in May 2018.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

Head of Business Support, Anglia Care Trust, Unit 8 The Square, Martlesham Heath, Ipswich, IP5 3SL

Email: Email: GDPR@angliacaretrust.org.uk

Telephone no: 01473 622888

Access to personal data (Subject access requests)

Under GDPR, individuals have the right to access personal data held about them. Requests should be made in writing to the Head of Business Support using the above contact details and detailing the information required.

The Head 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.