

The Papworth Trust

Candidate Privacy Notice

Issued: 14 February 2023

Version: 1.1

Review History

Date	Version	Amendments and Comments	Owner(s)
14/02/2023	1.1	Initial draft.	

PAPWORTH TRUST CANDIDATE PRIVACY NOTICE

Who we are

When we say 'we' or 'us' in this notice, we are referring to The Papworth Trust, also referred to as, 'the Trust'. We are registered with Companies House under company number 00148906. We are also a charity with registered charity number 211234. Our registered office is at Saxongate Bradbury Place, Hartford Road, Huntington, Cambridgeshire PE29 3RR.

This notice is applicable to all candidates, both those applying for permanent and fixed term roles. It applies to agents and contractors, as well as other roles such as interns, trainees and graduates who work on projects for the Trust.

We are committed to protecting your rights and freedoms with regards to your personal data. This notice explains how we collect, store, use, and share personal information of our employees and those individuals going through a recruitment process to become employees. It also explains the rights you have in relation to the personal information that we hold about you.

This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time. Updates to this notice shall be made to this page and, where appropriate, notified to you either in writing, by email or other notification, but please check back to see any updates or changes.

When appropriate we will provide a 'just in time' notice to cover any additional processing activities not mentioned in this notice.

What kinds of data do we collect about you and why?

Throughout the Trust's recruitment processes, we may process personal data about you and your dependents, beneficiaries, and other individuals whose personal data has been provided to us.

The Trust collects and uses your personal data primarily for the purpose of assessing your suitability for employment. You don't have to provide what we ask for, but it may affect your application if you do not provide it.

The below are examples of the data we collect and the purposes for collection.

Application Stage

If you use our online application system, your details will be collected by our recruitment team. Your data will be held on our recruitment portal as well as being held on our internal servers and systems.

To access a copy of your completed application form you can email us at hr.administration@papworthtrust.org.uk

During the recruitment process we will ask you for your personal details including name and contact details. We will also ask you about previous experience, education, referees and for answers to questions relevant to the role. Our recruitment team will have access to all this information.

You will also be asked to provide equal opportunities information. This is not mandatory – if you do not provide it, it will not affect your application. We will not make the information available to any staff outside our recruitment team, including hiring managers, in a way that can identify you. Any information you provide will be used to produce and monitor equal opportunities statistics.

Shortlisting

Our hiring managers shortlist applications for interview. They will not be provided with your equal opportunities information if you have provided it.

Assessments

We may ask you to participate in an assessment; complete tests or occupational personality profile questionnaires; attend an interview; or a combination of these. Information will be generated by you and by us. For example, you might complete a written test, or we might take interview notes. This information is held by us. If you are unsuccessful after assessment for the role, we may ask if you would like your details retained in our talent pool. If you say yes, we will proactively contact you should any further suitable vacancies arise.

Interview

Prior to interview we ask you for details of qualifications and working history. This will be discussed at interview. We will also ask you for a record of any criminal convictions. We require this to ensure a safe environment for staff and service users. You must successfully complete pre-employment checks to progress to a final offer. We must confirm the identity of our staff and their right to work in the United Kingdom, and seek assurance as to their trustworthiness, integrity, and reliability.

You may be asked to provide:

- proof of your identity – you may be asked to attend our office with original documents; we will take copies. We may ask you to provide these electronically through Vetting.com our pre-employment checks partner.
- proof of your qualifications – you will be asked to attend our office with original documents; we will take copies. We may ask you to provide these electronically; in this case we will provide a secure transfer mechanism.
- a criminal records declaration to declare any unspent convictions.
- your email address, Vetting.com which will contact you to:
 - complete an application for a Basic or Enhanced Criminal Record check via the Disclosure and Barring Service which will verify your declaration of unspent convictions.
 - contact your referees, using the details you provide in your application or provided directly to Vetting.com to obtain confidential references.
- We may also ask you to complete a questionnaire about your health to establish your fitness to work.
- We may also ask you about any reasonable adjustments you may require under the Equality Act 2010. This information will be shared with relevant staff to ensure these are in place for when you start your employment.

If we make a final offer, we'll also ask you for the following:

- bank details – to process salary payments.
- emergency contact details – so we know who to contact in case you have an emergency at work.

After your start date

Information provided during the recruitment process will form part of your employment record and used to carry out the contract we have with you, provide you access to appropriate services required for your role and manage our human resources processes. We may need to confirm with our regulatory partners that you have commenced employment with us. We may share this information with the Charity Commission, Homes England and the Care Quality Commission. Information on these processing activities will be made available in our Employee Privacy Notice.

Other purposes

We may also be required to process your personal data where it is necessary for complying with laws and regulations, including collecting and disclosing employee personal information as required by law (e.g., for tax, health and safety, anti-discrimination laws), under judicial authorisation, or to exercise or defend the legal rights of the Trust.

We may also collect and use personal information when it is necessary for other legitimate purposes, such as to help us conduct our business more effectively and efficiently – for example, for IT security/management, accounting purposes, or financial planning. We may also process your personal data to investigate breaches of law or of our own internal policies.

Lawful basis for processing your personal data

Depending on the processing activity, we rely on the following lawful bases for processing your personal data under the GDPR:

- Article 6(1)(a) which relates to having your freely given consent.
- Article 6(1)(b) which relates to processing necessary for the performance of a contract.
- Article 6(1)(c) so we can comply with our legal obligations.
- Article 6(1)(d) to protect your vital interests or those of another person.
- Article 6(1)(f) for the purposes of our legitimate interest.

The primary lawful basis we rely on for processing your personal data is article 6(1)(b) of the UK-GDPR, which relates to processing necessary to perform a contract or to take steps at your request, before entering into a contract of employment with you.

If you provide us with any information about reasonable adjustments, you require under the Equality Act 2010 the lawful basis we rely on for processing this information is article 6(1)(c) to comply with our legal obligations.

Please note, while consent is listed as a lawful basis it is unlikely that the Trust will rely upon this lawful basis unless it can be shown that you were able to freely give such consent. Where consent is used as a lawful basis, you have the right to withdraw such consent at any time. The use of consent will be made clear to you at the point of collection, alongside the purposes for processing this data. Should you wish to withdraw your consent, please contact our Data Protection Officer at info@papworthtrust.org.uk or write to us at:

1 Saxongate,
Bradbury Place,
Huntingdon,
Cambridgeshire, PE29 3RR.
01480 357200

Special category data

Some data is sensitive and must be further protected. The UK GDPR describes some such data as special category data, these are set out at Article 9:

- (a) race;
- (b) ethnic origin;
- (c) political opinions;
- (d) religious or philosophical beliefs;
- (e) trade union membership;
- (f) genetic data;
- (g) biometrics (when used for ID purposes);
- (h) health;
- (i) sex life;
- (j) sexual orientation.

Where the information we process is special category data, for example your health data, the additional bases for processing that we rely on are:

- Article 9(2)(a) which relates you providing explicit consent.
- Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.
- Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent.
- Article 9(2)(h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee.
- Article 9(2)(f) for the establishment, exercise, or defence of legal claims.

In addition, where we are required to identify a condition under the DPA we rely on processing conditions at Schedule 1 part 1 paragraph 1 and Schedule 1 part 1 paragraph 2(2)(a) and (b) DPA. These provisions relate to the processing of special category data for employment purposes, preventative or occupational medicine and the assessment of your working capacity as an employee.

Criminal convictions and offences

We may need to process information about candidate criminal convictions and offences e.g. in a Disclosure and Barring Service (DBS) check. The lawful basis we rely on to process this data is:

- Article 6(1)(b) UK GDPR for the performance of a contract of employment.

The relevant condition for the processing is that at Schedule 1 paragraph 1 DPA which relates to employment, social security and social protection. It may be that during the course of your employment we discover that you have committed a criminal offence and will require to process that data by disclosing it to the police and process it to use it in the course of disciplinary proceedings. We will, in such circumstances, rely upon the conditions at Schedule 1 Part 2 paragraphs 11 and 12 – preventing unlawful acts and protecting the public from dishonesty.

Appropriate Policy Document

In processing your personal data we undertake to do so in a manner which complies with the data protection principles listed under Article 5 UK GDPR. These require that personal data be:

1. Processed lawfully, fairly and transparently (lawfulness, transparency and fairness) .
2. Collected for specified, explicit and legitimate purposes, and not further processed in a way which is incompatible with those purposes (purpose limitation).
3. Adequate, relevant and not excessive in relation to the purposes for which it is processed (data minimisation).
4. Accurate and where necessary kept up to date (accuracy).
5. Kept for no longer than is necessary for the purposes for which it is processed (storage limitation).
6. Processed in a way that ensures appropriate security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (security - integrity and confidentiality).
7. We will undertake to be responsible for complying with the above principles (accountability).

Lawfulness

We undertake to only process your personal data where we have a lawful basis under the UK GDPR to do so and where that information is required for a particular purpose. We will publish this policy on our website and update it regularly. We have set out above the legal bases we will rely upon to process your personal data. As we have also stated where we process candidate special category data about you we do so for the purposes of us fulfilling our employment contract and other employment obligations, in going through the recruitment process it is necessary for us to process this special category data too. We do so in line with an appropriate condition under the UK GDPR and DPA as identified above. Sometimes this processing is inadvertent in that the nature of the personal data that we process will allow special category data to be inferred but that does not detract from the purpose of the original processing. We will require to process criminal conviction data during the employment recruitment process for the purposes of DBS checks.

Purpose Limitation

Processing of special category data will be restricted to only that which is necessary for the relevant purpose and it will not be used for another purpose unless that use is otherwise authorised. We will outline the purposes identified in this document.

Data Minimisation

We will limit the amount of data (including special category and criminal conviction data) that is collected and ensure that it is collected only for the purpose identified. We will adhere to the terms of our retention schedules so that we will delete that data which we do not need.

Accuracy

We will ensure as far as possible that the data we hold is accurate and kept up to date and will record the source of the data. In some circumstances we may need to keep factually inaccurate information e.g. if a grievance is raised during the recruitment process. Checks are carried out on the accuracy of data during audits and line manager checks. Personal data found to be inaccurate will be rectified or erased whenever possible. Where this is not possible, there will be an addendum to that personal data advising of the inaccuracy. If inaccurate personal data has been disclosed, the recipient will be advised of this as soon as practicable.

Storage Limitation

We have considered the length of time we should keep personal data (including special category and criminal conviction data) we maintain a retention schedule which dictates the length of time personal data should be kept in certain circumstances. All processing of special category and criminal conviction data will be dealt with under the schedule. When an individual withdraws consent to the processing of special category data (in the unusual circumstances where consent has been previously requested and provided by the individual), that data will be destroyed in line with requirements under the UK GDPR (see below regarding your right to object).

In the event of a candidate being unsuccessful we will delete their personal data after six months.

Security

We have developed and implemented certain technical and organisational measures to protect against unauthorised or unlawful processing and also against accidental loss, destruction or damage. We employ such security measures as encryption, firewalls, anti-virus software, IT health checks, vulnerability assessment and penetration process, user authentication, role based and password-controlled access, technical assurance and technical audits. All staff are required to undertake mandatory data protection training.

Accountability

We will review this document regularly and at least every two years to ensure we adhere to the above principles. We have set out below your rights and how to exercise them.

Sources of personal data

Usually, you will have provided the information we hold about you directly but there may be situations where we collect personal data from other sources. The following are the types of personal data we may collect about you and the source of this data:

- Confidential references from nominated third party referees, including previous employers.
- Details of any psychometric tests taken by a third-party provider.
- Details of employee pre-employment screening.
- Feedback from colleagues including managers and peers collected during the recruitment process.
- Feedback from clients or other third parties collected during and following client engagements.
- Referrals for roles from referees, either external or internal, or by recruitment agencies.
- Details relating to your employment history, education and qualification listed on social media platforms, such as LinkedIn.
- CCTV images.
- IT related data e.g., computer ID, user ID, IP addresses, service access logs, software and hardware inventory, cookies.

How long we keep your personal data

We will only retain your personal information for as long as necessary to fulfil the purposes for which we collect it, including for the purposes of satisfying any legal, insurance, accounting or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk or harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, insurance and compliance requirements. We tend only to retain candidate data, for unsuccessful candidate for around six months.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. We will retain and securely destroy your personal information in accordance with our data retention policy, considering applicable laws and regulations, where we no longer have a legitimate reason for retaining it.

We will also base any retention decisions on criteria, including:

- Any legal or regulatory requirements to delete or retain the data for a specific timeframe.
- Our legitimate business reasons for keeping the data, such as to analyse and assess our activities. This includes assessing the fairness of our recruitment practices.
- The likelihood of a claim arising where we would need to defend our conduct.
- Whether the data is likely to remain up to date.

Data sharing

In some circumstances, such as under a court order, we are legally obliged to share information. We may also share information about you with third parties including government agencies and external auditors.

We may have to share your data with other third parties, including third-party service providers. We require third parties to respect the security of your data and treat it in accordance with data protection laws. If we do share data, you are entitled to expect that third party to apply a similar level of protection in respect of your personal information.

The Trust, or its service providers, share your personal data with third parties when:

- required by law;
- requested by a regulator;
- necessary to manage its working relationship with you;
- it is in the public interest to do so;
- necessary for the performance of its services;
- contacted by a new or prospective employer for a confidential employment reference; or
- necessary for fraud and data error investigations.

The third parties include service providers, contractors, agents, and other government bodies.

Third party	Purpose
Pre-employment screening	Pre-employment checks for ID, referees etc.
Disclosure and Barring Service	Security vetting
Charity Commission, Homes England and the Care and Qualities Commission.	Regulatory requirements
External auditors	Variety of audit checks to assure compliance with process/policy
Travel providers	Travel and accommodation arrangements
Offsite document storage providers	Storage of your HR, pay and pension records

All our third-party service providers are required to take appropriate security measures to protect your personal information. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the Trust or where we are under a duty to disclose or share your personal data to comply with any legal obligation; or to protect the rights, property, or safety of the Trust, our customers, or others.

Security of your Data

The Trust has implemented specific measures such as admission controls, system access controls, data access controls, transmission controls, input controls, job controls, availability controls, and segregation controls to ensure adequate protection of personal data. This includes specific measures such as the use of anti-virus applications, proper training protocols, systematic access management, and DDoS mitigation technologies].

The Company's approach to protect the integrity of the data includes, but is not limited to, technical and organisational measures such as proper system administration, regular backup procedures, the use of authentication codes, signature procedures, network controls, and proper training of employees and relevant third parties

How we make decisions about recruitment

Final recruitment decisions are made by hiring managers and members of our recruitment team. We take account of all the information gathered during the application process. Any online testing is marked, and a result is generated automatically. However, if you wish to challenge the mark you have received, the result can be checked manually.

You can ask about decisions on your application by speaking to your contact in our recruitment team or by emailing recruitment@papworthtrust.org.uk

Your rights

There are several rights available to people under the UK GDPR. These include:

- Access to your data and information about what data we hold, its source and the purposes of processing your data.
- Rectification of your data where it is inaccurate.
- The right to be forgotten / to request that data is deleted.
- The right to restrict the processing of data.
- Data portability.
- The right to object.
- Rights relating to automated decision-making.
- You can find more information on these rights below. If you wish to exercise one of your rights, please contact our Data Protection Officer at info@papworthtrust.org.uk or write to us at:

1 Saxongate,
Bradbury Place,
Huntingdon,
Cambridgeshire, PE29 3RR.
01480 357200

1. Access to your data

You have the right to ask us to confirm that we process your personal data, as well as to have access to and receive copies of the data we hold about you. This right also include being provided information on the categories of data held, the sources of any data we process and information on who this is shared with or sold to – for ease we have included most of this information within this privacy policy.

We will provide the information you request as soon as possible and in any event within one calendar month of receiving your request unless we require to extend it in line with the provisions under the UK GDPR. If we need more information to comply with your request, we will let you know.

2. Rectification (correction) of your data

If you believe personal data, we hold about you is inaccurate or incomplete, you can ask us to rectify it. We will make the correction within one month, unless we do not feel the change is appropriate for us to make, in that case, we will let you know why. We will also let you know if we need more time to comply with your request.

3. Right to be forgotten (erasure)

In some circumstances, you have the right to ask us to delete the personal data we hold about you when:

- We no longer need your personal data for the purpose for which we collected it.
- We have collected your personal data on the grounds of consent (or the condition of explicit consent) and you withdraw that consent.
- You object to the processing, and we do not have any overriding legitimate interests to continue processing the data about you.
- We have unlawfully processed your personal data (i.e., we have failed to comply with the UK-GDPR).
- The personal data must be deleted to comply with a legal obligation.

There are certain situations in which we are entitled to refuse to comply with a request. If any of those apply, we will let you know.

4. Right to restrict processing

In some circumstances, you are entitled to ask us to stop processing your personal data. But, while this means we must stop actively processing your personal data, we do not have to delete it. This right is available if:

- You believe the personal data we hold is not accurate – we will cease processing it until we can verify its accuracy.
- You have objected to us processing the data – we will stop processing it until we have determined whether our legitimate interests override your objection.
- If the processing is unlawful.
- If we no longer need the data but you would like us to keep it because you need it to establish, exercise, or defend a legal claim.

5. Data portability

Where the Trust acts as a data controller, you have the right to ask us to provide your personal data in a structured, commonly- used and machine-readable format so that you can transfer the personal data to another data controller. This right only applies:

- To personal data you provide to us.
- When processing is based on your consent or for performance of a contract (i.e., the right does not apply if we process your personal data on the grounds of legitimate interests).
- If the processing is automated.

We will respond to your request as soon as possible and in any event within one calendar month. If we need more time, we will let you know.

6. Right to object

You are entitled to officially object to us processing your personal data:

- If the processing is based on legitimate interests or performance of a task in the public interest or exercise of official authority.
- For direct marketing purposes (including profiling).
- For the purposes of scientific or historical research and statistics.

We will stop processing your data if you have grounds for objecting unless we can show that there are legitimate compelling grounds that override your interests, rights, and freedoms or the processing is for the establishment, exercise, or defence of legal claims.

7. Rights related to automated decision-making including profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects you.

For something to be solely automated there must be no human involvement in the decision-making process. The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. A legal effect is something that affects your legal rights. In these cases, you can request that human intervention or human involvement be used as part of the decision-making process. Furthermore, you can request information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences of any decisions made. We do not envisage that this type of decision-making will take place.

Changes to this Privacy Notice

We may update this notice at any time. This notice shall be made available on our website. Updates to this notice shall be made to this page and, where appropriate, notified to you.

Please check back frequently to see any updates or changes.

Contact

Questions, comments and requests regarding this privacy notice and your individual rights are welcomed. To contact us on these matters, or for any other data protection concerns or issues, please use the following details:

- by email:
info@papworthtrust.org.uk
- in writing to:
1 Saxongate,
Bradbury Place,

Huntingdon,
Cambridgeshire, PE29 3RR.
01480 357200

Complaints and Concerns

If you have any concerns about the ways in which we process your personal data, you have a right to complain to the Information Commissioner's Office. We would encourage you to contact us first, so we can address your concerns.

The Information Commissioner's Office can be reached using the following details:

- through their website: <https://ico.org.uk/>
- by telephone: 0303 123 1113
- in writing: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF