The Kite Trust.

Gender and sexuality
Supporting young people

DATA PROTECTION AND CONFIDENTIALITY POLICY

Last reviewed and approved by trustees: August 2020
Next due for review: December 2022

Our Vision

We envisage an inclusive society where LGBTQ+ young people are healthy, successful and celebrated.

Our Purpose

We support the wellbeing and creativity of LGBTQ+ young people in Cambridgeshire, Peterborough and surrounding areas through information, support and groups. We build inclusive communities to tackle inequalities through consultancy, training and education to all sectors.

Our Values

Relevant – Our learning and development is continuous.
Engaging – We are warm and welcoming.
Accessible – We create inclusive communities and safe spaces.
Community Led – We are motivated by the voices of LGBTQ+ young people.
High Quality – Our support and guidance are of the highest quality.

The Kite Trust
Registered Charity: 1189936
26 St Thomas Place, Ely, CB7 4EX
info@thekitetrust.org.uk
01223 369508

Introduction

The security and privacy of your data and your confidentiality is taken seriously by us, but we need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We are committed to complying with all the Data Protection legal obligations.

This policy applies to current and former employees, contractors, volunteers and service users. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy.

The Kite Trust has taken steps to protect the security of your data in accordance with our this policy and will train staff about their data protection responsibilities as part of the induction process. We will only hold data for as long as necessary for the purposes for which we collected it.

The Company is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how The Kite Trust will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, The Kite Trust.

Data Protection Principles

Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and

- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

How we define personal data

'**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or another agency), or it could be created by us. It could be provided or created before, during or after your involvement with The Kite Trust.

The types of personal data we collect and use about you is included in the Privacy Notice that is issued with your contract of employment.

How we define special categories of personal data

'**Special categories of personal data**' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your health;
- your sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data,

as detailed in the Privacy Notice, in accordance with the law.

How we define processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

How will we process your personal data

The Kite Trust will process your personal data (including special categories of personal data). We will use your personal data for:

- performing the contract of employment (or services) between us, or delivering services to you;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

Examples of when we might process your personal data can be found in the Privacy Notice. We will only process special categories of your personal data

in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the person for responsible for Data in the Company.

We do not need your consent to process **special categories** of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.
- Where processing is necessary to carry out a DBS form. If a post is exempt from the Rehabilitation of Offenders Act 1974, applicants are required to declare any convictions, cautions, reprimands and final warnings that are not protected (i.e. that are not filtered out) as defined by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended in 2013).

We might process special categories of your personal data for the purposes stated in the Privacy Notice, in particular, we may use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.
- DBS requirements

We do not take automated decisions about you using your personal data or use profiling in relation to you.

Data will be retained for a period dependent on the document type. The length of time data is retained for is set out in Appendix A.

We might collect any or all of the following types of information from staff or volunteers depending on the nature of your role with us:

1. Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
2. Date of birth.
3. Gender.
4. Next of kin and emergency contact information.
5. National Insurance number.
6. Bank account details, payroll records, travel logs and expenses and tax status information.
7. Salary, annual leave, pension and benefits information.
8. Start date.
9. Location of employment or workplace.
10. Access to your DVLA portal.
11. Recruitment information (including copies of right to work documentation, passport, references and other information included in a CV or cover letter or as part of the application process).
12. Employment records (including job titles, work history, working hours, training records and professional memberships).
13. Compensation history.
14. Performance information.
15. Disciplinary and grievance information.
16. Information about your use of our information and communications systems.
17. Photographs.

We may also collect, store and use “special categories” of more sensitive personal data which require a higher level of protection about staff and volunteers:

18. Information about your health, including any medical condition, health and sickness records (including Occupational Health records).

19. Absence notes
20. Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
21. Trade union membership.
22. Information about criminal convictions and offences.

We need all the categories of information identified above primarily to allow us to perform our contract with you[*] and to enable us to comply with legal obligations[**]. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties[***] (provided your interests and fundamental rights do not override those interests). We will process your personal information as follows, the asterisks show the purpose for processing:

Purpose	Type of data	Lawful basis
Making a decision about your recruitment or appointment.	1, 11, 12, 22	***
Determining the terms on which you work for us.	7, 8, 9, 11, 12	***
Checking you are legally entitled to work in the UK.	1, 2, 5, 10	**
Paying you and, if you are an employee, deducting tax and National Insurance contributions.	1, 5, 6, 7	** *
Liaising with your pension provider.	1, 2, 5, 7, 8	*
Administering the contract we have entered into with you.	1, 4, 5, 6, 7, 8, 9, , 14, 15, 20	*** *
Business management and planning, including accounting and auditing.	1, 2, 3, 5, 6, 7, 8, 9, 14, 15, 16, 18, 20, 21	***
Conducting performance reviews, managing performance and determining performance requirements.	1, 7, 8, 9, 14, 15, , , 16, 20	*** *
Making decisions about salary reviews and compensation.	1, 6, 7, 8, 9, 11, 12, 14, 15, 16	*** *

Assessing qualifications for a particular job or task, including decisions about promotions.	1, 11, 12, 14, 15, 20	*** *
Gathering evidence for possible grievance or disciplinary hearings. Making decisions about your continued employment or engagement.	1, 14, 15, , 16, 20 1, 14, 15, , 16, 20	*** *
Making arrangements for the termination of our working relationship.	1, 5, 6, 7, 14, 15, 20	*** *
Education, training and development requirements.	1, 12, 14, 15, 20	*** *
Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.	1, 6, 7, 13, 14, 15, 16, 17, 18, 19, 20, 22	***
Ascertaining your fitness to work and managing sickness absence.	1, 2, 3, , 4, 9, 14,15, , 16, 17, 18, 20	*** *
Complying with health and safety obligations.	1, 4, 9, 20	** *
To prevent fraud.	1, 5, 6, 10, 11, 12, 22	***
To monitor your use of our information and communication systems to ensure compliance with our IT policies.	1, , 16	***
To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.	1, , 16	***
To conduct data analytics studies to review and better understand employee retention and attrition rates.	1, 2, 3, , 18, 20	***
Equal opportunities monitoring.	1, 2, 3, , 18, 20	***

Sharing your personal data

Sometimes we might share your personal data with other agencies to carry out our obligations under our contract with you, in line with our safeguarding duty or for our legitimate interests.

We require those agencies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We use the following contractors to carry out our business and therefore share personal data of employees with them:

- Dartnell Lynn Ltd to store and manage your personal data with regard to your payroll

We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

How should you process personal data for The Kite Trust

Everyone who works for, or on behalf of, The Kite Trust has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy.

The Kite Trust's Data Protection Officer is responsible for reviewing this policy The Kite Trust's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person and address any written requests to them.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of The Kite Trust and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

- You should not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.

- You should regularly review and update personal data. This includes telling us if your own contact details change.
- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords.
- Staff and volunteers should lock computer screens when not at your desk.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Do not save personal data to your own personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the person for responsible for Data in your Company.
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- You should not take personal data away from The Kite Trust's premises without authorisation from your line manager or from the Data Protection Officer.
- Personal data should be shredded and disposed of securely when you have finished with it.
- You should ask for help from the Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
- Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.
- It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact the person for responsible for Data immediately and keep any evidence you have in relation to the breach.

Subject Access request

Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to the Data Protection Officer who will coordinate a response.

If you would like to make a SAR in relation to your own personal data, you should make this in writing to the Data Protection Officer. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

Your data subject rights

- You have the right to information about what personal data we process, how and on what basis as set out in this policy.
- You have the right to access your own personal data by way of a subject access request (see above).
- You can correct any inaccuracies in your personal data. To do you should contact of the Data Protection Officer.
- You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer

necessary to process it for the purpose it was collected. To do so you should contact the Data Protection Officer.

- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Data Protection Officer.
- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- You have the right to object if we process your personal data for the purposes of direct marketing.
- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- With some exceptions, you have the right not to be subjected to automated decision-making.
- You have the right to be notified of a data security breach concerning your personal data.
- In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Data Protection Officer.
- You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

SERVICE USERS CONFIDENTIALITY

A service user has the right to reveal information to The Kite Trust in the knowledge that the information is privileged and will not be passed on outside the organisation without consent. In the early stages of working with

service users, other professionals and agencies, formal explanation about confidentiality should be given in line with this policy.

A service user has the right to use the services of The Kite Trust without being identified as a service user to anyone outside the organisation without that individual's permission.

Information is not passed to other agencies, the media, service users, the service user's family, or other users of the service, without the service user's consent. The exception to this is if we believe there is a risk to the service user or others based on the information shared. Confidentiality cannot be assured where the following situations apply:

- If The Kite Trust is compelled to divulge confidential information by a court order.
- If a service user gives us information concerning abuse of a child or vulnerable adult *(see* The Kite Trust *Safeguarding Policy)*
- If, by keeping confidentiality, a service user might suffer severe injury or abuse
- If, by keeping confidentiality, someone else might suffer severe abuse (including death or serious injury through violence or rape and sexual assault.)

In any situation, where a volunteer or staff member believes that information has been disclosed that may require confidentiality to be broken this should be discussed with the service user if possible and appropriate and with the appointed person (see below). The views of the service user should always be taken into account, however it may be that the service user does not wish action to be taken; does not wish to become involved in an investigation and/or does not want confidential information to be shared with other individuals and agencies. In such a situation the staff service user or volunteer should inform the service user that they have a duty to discuss the disclosure with an appointed person within The Kite Trust.

The matter must then be referred, if any way possible, to an appointed person to make a decision as to whether The Kite Trust will breach the confidentiality of the service user. The appointed persons are:

Pip Gardner, Chief Executive
Rosie Woolgar, Programme Manager (Youth Work)

Bethan Rees, Programme Manager (Schools and Training)

The Kite Trust will only breach confidentiality without service user consent or contrary to the wishes of a service user in the circumstances of serious abuse or serious risk of self harm or abuse to a service user as outlined. If appropriate without causing prejudice to the protection of individuals at risk, or to a subsequent investigation the consent of the service user will be sought and in any event full support will be offered. Only an appointed person can authorise a disclosure where consent has not been given or has been refused, and the disclosure would only be made to relevant agencies.

Nothing in this section should prevent volunteers covered by inter-agency child protection procedures from complying with their statutory professional duties.

VOLUNTEER CONFIDENTIALITY

It is down to the discretion of individual The Kite Trust volunteers whether or not they identify themselves as a The Kite Trust volunteer to anyone outside of The Kite Trust.

An individual's involvement with The Kite Trust should never be disclosed by anyone within the organisation to anyone outside the organisation without that individual's permission.

Volunteers should not give out their home contact details to service users in the course of their volunteering, nor should they give out the home contact details of other The Kite Trust volunteers to third parties.

Each service user agrees to abide by the The Kite Trust Data Protection and Confidentiality Policy by signing the The Kite Trust volunteer agreement.

STAFF AND CONFIDENTIALITY

It is a contractual requirement for staff to be familiar with and adhere to the The Kite Trust Data Protection and Confidentiality Policy.

Any confidential information must be kept securely, and any information shared and used in line with our Data Protection policy.

INTER-AGENCY CONFIDENTIALITY

The guidelines set out under "Service user confidentiality" above should be followed when dealing with other agencies.

With written authorisation The Kite Trust may liaise with other agencies on behalf of the service user. Consent giving The Kite Trust permission to do this must be obtained from the service user and documented in their CharityLog record. Only information agreed by the service user prior to involving other agencies may be given. Information obtained in this way is subject to this confidentiality policy.

An agreement on use of information given to other agencies should be made at the time of giving them that information. If we are asked to abide by another organisation's confidentiality rules, we should do so as long as they do not lead to a contravention of our own. If this is the case, we should inform the other organisation.

BUSINESS CONFIDENTIALITY

The Kite Trust is dependant on the generation of income through fundraising, grant applications and corporate support. Business information is defined as any files, information, documents, or any copies relating to The Kite Trust except for materials published for public dissemination. Such material and/or information may not be used or retained by employees, service users or volunteers for their own purposes or conveyed to another organisation / body without the explicit permission of the Chief Executive or where required within the normal duties of their post/role. In any event information that identifies or relates to individual service users will not be passed on without their consent except in the circumstances described in this policy.

DISCIPLINARY ACTION

Any breach of this confidentiality policy may result in disciplinary action being taken. This could mean expulsion from The Kite Trust, or a limitation or withdrawal of the right to access services. In the case of staff, a breach of this policy could be considered to be gross misconduct and would be dealt with through the staff disciplinary procedure.

Appendix A – Document Retention Schedule

DOCUMENT TYPE	RETENTION PERIOD
FINANCIAL	
Payments cash book or record of payments made	6 years
Invoice – revenue	6 years
Petty Cash records	6 years
Invoice – capital item	10 years
Bank paying in slips	6 years
Bank statements	6 years
Remittance advices	6 years
Correspondence re donations	6 years
Bank reconciliations	6 years
PAYROLL DOCUMENTATION	
P45s	6 yrs plus current year
P6 (notice to employer of tax code)	6 yrs plus current year
P11D (annual return of employees expenses)	6 yrs plus current year
P60 (certificate of pay and tax deducted)	6 yrs plus current year
Notice of tax code change	6 yrs plus current year
Annual tax returns	6 yrs plus current year
Records of tax deduction	6 yrs plus current year
Payroll records	6 yrs plus current year
Pay advice	1 yr plus current year
EMPLOYEE/PERSONNEL RECORDS	
Accident book/reports	3 yrs after the last entry or conclusion of investigation
Wages and salary records	6 yrs plus current year
Expense accounts/records	6 yrs plus current year
Redundancy records	6 yrs after employment has ceased
Job applications for unsuccessful candidates	6 months after notifying the candidate
Maternity pay records	3 yrs after the tax yr in which maternity period ends
Sickness records	3 yrs after the end of the tax year
CRB checks	6 months after recruitment. Thereafter just keep details.

Personnel files and training records	6 years after employment ceases
BUILDING/PLANT	
Leases	15 years after expiry
PENSION RECORDS	
Pension scheme expression of wish forms	6 yrs after date of death
Pension contribution records	Permanently
INSURANCE RECORDS	
Policies	3 yrs after lapse
Claims correspondence	3 yrs after settlement
Employers Liability Certificate	40 years
Accident reports and relevant correspondence	3 yrs after settlement
OTHER	
Trustee meeting minutes	Permanently
Annual accounts and annual review	Permanently
Major agreements of historical significance	Permanently
Health & Safety records	Permanently
Contracts; licensing, rental, and HP agreements	6 years after expiry
Records relating to children	3 years after last engagement
Email Communications of Staff Members	3 years for current employees, 1 year after end of employment for former employees