DATA PROTECTION POLICY

Introduction

At Kids Can Achieve (KCA) we collect and process personal information, or personal data, relating to our service users, staff, workers, consultants and contractors to manage support and working relationships. This personal information may be held by us on paper or in electronic format. This policy does not form part of your contract of employment and may be amended or departed from at any time.

We are committed to being transparent about how we handle personal information, to protecting the privacy and security of personal information and to meeting our data protection obligations under the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018.

The aims of this policy are to provide:

- a framework for us to meet our legal obligations
- staff with guidance for the appropriate use and storage of personal data
- privacy notices for staff, service users and others who may provide us with their data
- procedures for people to exercise their rights in relation to their personal data.

Scope

This policy applies to:

- all employees
- workers engaged on a contract for services (sessional workers)
- agency workers
- self-employed individuals
- volunteers
- trustees.

Key responsibilities – staff

- Keep data secure
- Follow all relevant procedures
- Report any potential data protection breaches as soon as you become aware of them

Key responsibilities – managers

- Ensure personal data processed in your area conforms to the requirements of this policy
- Ensure new and existing staff who are likely to process personal data are aware of their responsibilities and are provided with adequate training and support

1 Data protection principles

1.1 We recognise the data protection principles established by GDPR and the Data Protection Act 2018, which provide that personal information we hold must be:

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

1.2 We are responsible for, and must be able to demonstrate compliance with, these principles.

2 Bases for collecting, storing and using personal data

2.1 The lawful bases we use for collecting, storing and using personal data are outlined in relevant privacy notices for:

- Staff
- service users and their families
- website, marketing and fundraising.

3 Staff responsibilities

3.1 You should always collect and process personal information about people in accordance with the data protection principles, in particular:

- personal data must be kept securely and not disclosed orally or in writing, by accident or otherwise, to unauthorised third parties
- if you get data from someone you must inform them appropriately of their rights (i.e. orally or by signposting to a privacy notice)
- adhere to our policies regulating the use of Information Systems and email

- report the loss of any personal or special category data (paper or electronic) or equipment containing such data immediately to your manager and Human Resources
- only dispose of personal data by secure destruction and in accordance with the retention schedule
- if you work offsite – ensure that you use Citrix and do not download personal data to other machines or unencrypted storage devices
- store all paper documents containing service user or staff details in closed files kept in locked stores or cabinets to which only authorised staff have access
- emails should not be used to transfer personal and special category data unless it is password protected or encrypted
- take care when discussing staff or service users on phones when others may hear

4 Individual rights and how to exercise them

4.1 Individuals have the right to be informed about the collection and use of their personal data.

4.2 We use our privacy notices to provide individuals with information, including our purposes for processing personal data, retention periods for that data, and who it will be shared with.

4.3 The information contained in privacy notices must be provided to individuals at the time the data is collected from them in a manner appropriate to the data collected and individuals.

4.4 If we obtain personal data from other sources, privacy information must be provided within a reasonable period of obtaining the data and no later than one month after.

4.5 Other subject rights and how to exercise them are outlined in the relevant privacy notices; these rights relate to:

- requesting access to data
- requesting rectification of errors to data
- requesting the erasure of data
- restricting the processing of data
- objecting to the processing data
- data portability
- automated decision making.

4.6 When a request is made we have a legal duty to fulfil the request within one month. If you receive a formal request or something that could be interpreted as a request you must contact the following immediately:

- Human Resources if the request is in relation to staff data
- Marketing if the request is in relation to marketing or fundraising data
- Director of Services if the request is in relation to a service user.

4.7 The lead manager is responsible for appropriately fulfilling the request within the timescale. S/he may liaise with the Data Protection Officer if necessary.

5 Data security

5.1 Standards for the secure storage and transfer of electronic data are outlined in our IT policy.

5.2 The use of paper records should be minimised, with data scanned and stored electronically whenever possible.

5.3 Paper records should be held securely when not is use and only accessible to those who need to access them.

6 Data retention

6.1 Our approach to data retention is outlined in our Data retention schedule.

7 Data breaches

7.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It can be accidental or deliberate causes. A breach will have occurred if:

- any personal data is lost, destroyed, corrupted or disclosed
- someone accesses data or passes it on without proper authorisation
- data is made unavailable, for example, if it has been encrypted by ransomware, or accidentally lost or destroyed
- it is accessed by an unauthorised third party
- personal data is sent to an incorrect and unauthorised recipient
- devices containing personal data are lost or stolen
- personal data is altered without permission.

7.2 We have an obligation to report most personal data breaches to the Information Commissioners Office (ICO) within 72 hours of becoming aware of that breach. Additionally, if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform individuals affected without undue delay.

7.3 If you become aware of a potential data breach you must report it to your manager and Human Resources immediately.

8 Data protection officer

8.1 Our Data Protection Officer's contact details are at the end of this policy.

9 International data transfers

9.1 There are no international data transfers.

10 Data protection by design and data impact assessments

10.1 We are required to implement privacy-by-design measures as we develop our processes for collecting, storing and processing personal data, by implementing appropriate technical and organisational measures.

10.2 Under the circumstances outlined below we will undertake a data protection impact assessment (DPIA) before that processing is undertaken:

- the use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes)
- automated processing including profiling
- large scale processing of sensitive (special category) data
- large scale, systematic monitoring of a publicly accessible area.

10.3 A DPIA should systematically analyse proposed processing and help identify and minimise data protection risks. A DPIA should consider compliance and broader risks to the rights and freedoms of individuals. ADPIA must consider both the likelihood and the severity of any impact on individuals. It does not have to indicate that all risks have been eradicated, but it should assess whether or not any remaining risks are justified.

Data Protection Officer

Michael Griffin
07849 973 493
mjgconsulting@aol.com

Appendix 1 – Privacy notice for staff

1 What types of personal information do we collect about you?

1.1 Personal information is any information about you from which you can be directly or indirectly identified. It doesn't include anonymised data, i.e. where all identifying particulars have been removed.

1.2 There are also "special categories" of personal information and personal information on criminal convictions and offences that we collect and require a higher level of protection because it is of a more sensitive nature. The special categories of personal information comprise information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

1.3 We collect, use, and process a range of personal information about you, including:

- your contact details, including your name, address, telephone number and personal e-mail address
- your emergency contact details/next of kin
- your date of birth
- your sex
- the start and end dates of your employment or engagement
- recruitment records, including personal information included in a CV, any application form, cover letter, interview notes, references, copies of proof of right to work in the UK documentation, copies of documents that you present to enable us to undertake a Disclosure and Barring Check, copies of qualification certificates, a copy of driving licence (if you are required to drive as part of your job role or you present it as identification) and other background check documentation
- the terms and conditions of your employment or engagement (including your job title and working hours), as set out in a job offer letter
- any contracts and changes to that contract
- your National Insurance number
- your bank account details, payroll records, tax code and tax status information
- record of your performance at work, e.g. rotas, disciplinary, grievance, capability and sickness absence management records
- appraisals records
- training records
- leave and absence records

- information about your use of our IT systems, including usage of telephones, e-mail and the Internet
- photographs
- any other correspondence about your work with us.

1.4 We may also collect, use and process the following special categories of your personal information:

- information about your health, including any medical condition(s)
- if you disclose a disability, including reasonable adjustments made as a result of a disability or health condition
- sickness absence records (including details of the reasons for sickness absence being taken), medical reports and related correspondence
- your diversity profile, for example, ethnic origin, sexual orientation, marital status etc. to enable us to monitor its workforce and ensure that it is reflective of the people we work with (where we collect this for monitoring purposes you can choose not to disclose)
- trade union membership
- information about any criminal convictions, offences and cautions to meet our safeguarding obligations.

2 How do we collect your personal information?

2.1 We may collect personal information about you in a variety of ways. It is collected during the recruitment process, either directly from you or sometimes from a third party such as an employment agency. We may also collect personal information from other external third parties, e.g. references from former employers, information from background check providers, and criminal record checks from the Disclosure and Barring Service (DBS).

2.2 We may also collect additional personal information throughout the period of your employment or working relationship. This may be collected in the course of your work-related activities.

2.3 Whilst some of the personal information you provide to us is mandatory and/or is a statutory or contractual requirement, some of it you may be asked to provide to us on a voluntary basis. We will inform you whether you are required to provide certain personal information to us or if you have a choice in this.

3 Storing and maintain your personal data

3.1 Your personal information may be stored in different places, including in your personnel file, in our Human Resources and Payroll databases and related systems and in other IT systems, such as the e-mail system.

3.2 Your data is stored in:

- Human Resources - electronic database and shared folder accessed by Human Resources; a physical paper file only exists if you joined us before January 2015
- Payroll – electronic database and shared folder accessible by authorised Finance staff
- Managers – electronic folders accessible as necessary for the operation of the business.

4 Why and how do we use your personal information?

4.1 We collect and use information about you to:

- make decisions about your recruitment and confirm suitability for engagement and promotion
- determine and review your terms and conditions
- administer your contract and employment
- ensure you are legally entitled to work for us
- check employment history and criminal convictions in relation to working with children and/or vulnerable adults (where permitted)
- pay you and make the correct adjustments for tax, National Insurance, pension etc.
- manage development, performance, conduct, attendance etc.
- manage termination of employment
- undertake diversity monitoring
- comply with legislation, including tax, employment, health and safety, equality and diversity and safeguarding.

4.2 If you fail to provide certain personal information when requested or required, we may not be able to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations. You may also be unable to exercise your statutory or contractual rights.

4.3 We will only collect and use your sensitive personal information, which includes special categories of personal information and information about criminal convictions and offences, when the law allows us to.

4.4 Some special categories of personal information, i.e. information about your health or medical conditions and trade union membership, and information about criminal convictions and offences, is processed so that we can perform or exercise our obligations or rights under employment law.

4.5 Information about health or medical conditions may also be processed for the purposes of assessing the working capacity of an employee or medical diagnosis, provided this is done under the responsibility of a medical

professional subject to the obligation of professional secrecy, e.g. an occupational health adviser or a doctor.

4.6 We will also process these special categories of personal information, and information about any criminal convictions and offences, where we have your explicit written consent. Your consent can be withdrawn at any time. It is important to note that by withdrawing your consent it may prevent you and us from meeting our contractual obligations.

4.7 If we process other special categories of personal information, i.e. information about your ethnic origin, religious beliefs or sexual orientation, this is done only for the purpose of diversity monitoring. Personal information used for these purposes is anonymised; however you may decline to disclose this information.

4.8 We may also occasionally use your special categories of personal information, and information about any criminal convictions and offences, where it is needed for the establishment, exercise or defence of legal claims.

5 Changes of purpose

5.1 We will only use your personal information for the purposes for which we collected it. If we need to use your personal information for a purpose other than that for which it was collected, we will provide you, prior to that further processing, with information about the new purpose, we will explain the legal basis which allows us to process your personal information for the new purpose and we will provide you with any relevant further information.

6 The lawful basis on which we process information about you

6.1 We will use your personal information in one or more of the following circumstances:

- to perform the contract we have entered into with you
- to comply with a legal obligation
- where it is necessary for our legitimate interests (or those of a third party), and your interests or your fundamental rights and freedoms do not override our interests
- where we need to protect your (or someone else's) vital interests.

6.2 We will only use your special category personal data in one or more of the following circumstances:

- you have given explicit consent (e.g. to your union to make membership deductions)

- it is necessary for the purposes of carrying out our or your rights in the field of employment and social security
- it is necessary to protect your vital interests
- you have made the data manifestly public
- processing is necessary for the establishment, exercise or defence of legal claims.

7 Who has access to your personal information?

7.1 Your personal information may be shared internally, including with members of the HR and Finance teams, your manager, other managers in the department in which you work and IT staff if access to your personal information is necessary for the performance of their roles.

7.2 We may also share your personal information with third-party service providers (and their designated agents), including:

- external organisation for the purposes of conducting pre-employment reference and employment background checks
- human resources and payroll database suppliers
- benefits providers and benefits administration, including insurers
- pension scheme providers and pension administrators
- occupational health providers
- external IT services
- external auditors
- HM Revenue and Customs
- professional advisers, such as lawyers and accountants, Health and Safety, IT or HR Consultants.

7.3 We may also share your personal information with other third parties in the context of a potential sale, transfer or restructuring of some or all of its business. In those circumstances, your personal information will be subject to confidentiality undertakings.

7.4 Your personal information may also be shared in the following circumstances:

- public disclosure under Freedom of Information - e.g. requested names or contact details of senior managers or those in public-facing roles;
- disclosure to CQC / Ofsted inspectors – e.g. DBS number and expiry date;
- disclosure to POVA / POCA – e.g. to report a safeguarding incident following a formal investigation;
- disclosure to training providers – e.g. your contact details and any other information is subject to your explicit consent;

- disclosure to the Office of National Statistics which is a legal requirement;
- disclosure to comply with the law.

7.5 We may share your personal information with third parties where it is necessary to administer the contract we have entered into with you, where we need to comply with a legal obligation, or where it is necessary for our legitimate interests (or those of a third party).

8 How do we protect your personal information?

8.1 We have measures to protect the security of your personal information, including policies, procedures and controls to prevent your personal information from being accidentally lost or destroyed, altered, disclosed or used or accessed in an unauthorised way.

8.2 In addition, we limit access to your personal information to those employees, workers, agents, contractors and other third parties who have a business need to know in order to perform their job duties and responsibilities.

8.3 Where your personal information is shared with third-party service providers, we require all third parties to take appropriate technical and organisational security measures to protect your personal information and to treat it subject to a duty of confidentiality and in accordance with data protection law. We only allow them to process your personal information for specified purposes and in accordance with our written instructions and we do not allow them to use your personal information for their own purposes.

8.4 We have procedures to deal with a suspected data security breach and we will notify the Information Commissioner's Office (or any other applicable supervisory authority or regulator) and you of a suspected breach where we are legally required to do so.

9 For how long do we keep your personal information?

9.1 We will only retain your personal information for as long as is necessary to fulfil the purposes for which it was collected and processed, including for the purposes of satisfying any legal, tax, health and safety, reporting or accounting requirements.

9.2 We will generally hold your personal information for the duration of your employment or engagement. The exceptions are:

- personal information about criminal convictions and offences collected in the course of the recruitment process will be deleted once it has been verified through a DBS criminal record check,

unless, in exceptional circumstances, the information has been assessed by us as relevant to the ongoing working relationship

- it will only be recorded whether a DBS criminal record check has yielded a satisfactory or unsatisfactory result, unless, in exceptional circumstances, the information in the criminal record check has been assessed by us as relevant to the ongoing working relationship.

9.3 Once you have left our employment or your engagement has been terminated, we will generally hold your personal information for 6 years after the termination of your employment or engagement, but this is subject to:

- any minimum statutory or other legal, safeguarding, tax, health and safety, reporting or accounting requirements for particular data or records, and
- protection against legal risk, e.g. if potentially relevant to a possible legal claim in a tribunal, County Court or High Court.

9.4 In the event that you bring a claim of any sort against us following the termination of your employment your personal information may be retained for a longer period in order that it may be referred to by all parties in relation to that claim and any subsequent appeal.

9.5 In some circumstances we may anonymise your personal information so that it no longer permits your identification. In this case, we may retain such information for a longer period.

10 Your rights in connection with your personal information

10.1 It is important that the personal information we hold about you is accurate and up to date, so please keep us informed if your personal information changes, e.g. you change your home address, so that our records can be updated. We cannot be held responsible for any errors in your personal information in this regard unless you have notified us of the relevant change.

10.2 As a data subject, you have a number of statutory rights. Subject to certain conditions, and in certain circumstances, you have the right to:

- be informed about the data we hold on you – this privacy notice fulfils this right
- request access to your personal information - this is usually known as making a data subject access request and it enables you to receive a copy of the personal information we hold about you
- request rectification of your personal information - this enables you to have any inaccurate or incomplete personal information we hold about you corrected

- request the erasure of your personal information - this enables you to ask us to delete or remove your personal information where there's no compelling reason for its continued processing, e.g. it's no longer necessary in relation to the purpose for which it was originally collected;
- restrict the processing of your personal information - this enables you to ask us to suspend the processing of your personal information, e.g. if you contest its accuracy and so want us to verify its accuracy
- object to the processing of your personal information - this enables you to ask us to stop processing your personal information where we are relying on the legitimate interests of the business as our legal basis for processing and there is something relating to your particular situation which makes you decide to object to processing on this ground
- data portability - this gives you the right to request the transfer of your personal information to another party so that you can reuse it across different services for your own purposes.

10.3 In the event that you wish to exercise any of these rights, please contact Human Resources. To assist us please make it clear which right you wish to exercise. We may need to request specific information from you in order to verify your identity and check your right to access the personal information or to exercise any of your other rights. This is a security measure to ensure that your personal information is not disclosed to any person who has no right to receive it.

10.4 If you believe that we have not complied with your data protection rights, you have the right to make a complaint to the Information Commissioner's Office (ICO) at any time. The ICO is the UK supervisory authority for data protection issues. You can find their contact details on their website – www.ico.org.uk.

11 Automated decision making

11.1 Automated decision making occurs when an electronic system uses your personal information to make a decision without human intervention.

11.2 We do not make any automated decisions; we will notify you in writing if this position changes.

12 Changes to this privacy notice

12.1 We reserve the right to update or amend this privacy notice at any time, including where we intend to further process your personal information for a purpose other than that for which the personal information was collected

or where we intend to process new types of personal information. We will issue you with a new privacy notice when we make significant updates or amendments. We may also notify you about the processing of your personal information in other ways.

13 Contact

13.1 Contact Human Resources if you have any questions about this privacy notice or how we handle your personal information.

14 Acknowledgement

I acknowledge receipt of this privacy notice and confirm that I have read and understood it:

Name: ……

Signature……

Date……

Appendix 2 – Website Privacy Notice

Information that we collect from you

When you visit our website or complete our enquiry you will be asked to provide certain information about yourself including name and contact details. We may also collect information about your usage of our website as well as information about you from emails you send us.

Use of your information

Your information will enable us to contact you to provide the information you have requested. We may also use and analyse the information we collect so that we can administer, support, improve, and develop our services.

The information you provide us will be held on our computers in the UK and may be accessed by or given to our staff and third parties who act on our behalf for the sole purpose of providing the services.

If you have given your explicit consent, we may use your information to contact you by post, telephone, email, or text message for your views on our services; to notify you of important changes or developments to the site and our services; and to let you know about other products and services which we offer which may be interest to you. You may withdraw your consent at any time by contacting us.

If you have given your explicit consent, we may allow carefully selected third parties to contact you occasionally by email about products or services which may be of interest to you. You may withdraw your consent at any time by contacting us.
We may also pass aggregated information on the usage of our site to third parties for analysis purposes, but this will not include information that can be used to identify you. Unless required to do so by law we will not otherwise share, sell, or distribute any of the information you provide to us without your explicit consent.

Security and data retention

We employ industry standard security measures to protect your information from, unauthorised access; unlawful processing; accidental loss, destruction, or damage. We will retain your information for a reasonable period or as long as the law requires.

Access and updating

In accordance with the Data Protection Act 2018 you are entitled to see all the information held about you, and you may request changes to ensure the information is accurate, up to date, and relevant.