YMCA TRINITY GROUP

Employee and Self-Employed Contractors Privacy Statement

Contents

YMCA Trinity Group is aware of its obligations under the Data Protection Act 2018 and is committed to processing your data securely and transparently. This privacy statement sets out, in line with the Data Protection Act, the types of data that we hold on you as an employee of YMCA Trinity Group. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

This statement applies to current and former employees, workers, agency workers and contractors. This statement does not form part of any contract of employment or other contract to provide services, and we may update this statement at any time.

Data controller details

YMCA Trinity Group is a data controller, meaning that it determines the purposes for which we collect and use your personal data, and the processes to be used when using your personal data. Our contact details are as follows:

YMCA Trinity Group

Queen Anne House
Gonville Place
Cambridge
Cambridgeshire
CB1 1ND

Data protection principles

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your employment, and in ways that have been explained to you
- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- process it in a way that ensures it will not be used for anything that you are not aware of or have not consented to (as appropriate), lost or destroyed

Types of data we process

We can hold many types of data about you, including:

- your personal details including your name, address, date of birth, personal email address, phone numbers
- your photograph
- gender
- marital status
- next of kin and their contact numbers
- medical or health information including whether or not you have a disability
- information used for equal opportunities monitoring about your nationality, marital status, religion or belief and ethnic origin
- information included on your application form including references, education history and employment history
- documentation relating to your right to work in the UK
- driving licence & vehicle insurance
- bank details
- tax codes/tax reference number for self-employed contractors
- National Insurance number
- Professional Membership Details (where applicable)
- Public liability insurance details for self-employed contractors
- current and previous job titles, job descriptions, pay grades, pension entitlement, hours of work and other terms and conditions relating to your employment with us
- letters of concern, formal warnings and other documentation with regard to any disciplinary proceedings

- internal performance information including measurements against targets, formal warnings and related documentation with regard to capability procedures, appraisal forms
- leave records including annual leave, family leave, sickness absence etc
- details of your criminal record
- training details and copies of training certificates
- CCTV footage
- building entry card records.

How we collect your data

We collect data about you in a variety of ways and this will usually start when we undertake a recruitment exercise where we will collect the data from you directly. This includes the information you include in your application form or a recruitment cover letter, or notes made by our managers during a recruitment interview. Further information will be collected directly from you when you complete forms at the start of your employment, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in personnel files or within YMCA Trinity Group's HR and IT systems.

Why we process your data

The law on data protection allows us to process your data for certain reasons only:

- in order to perform the employment contract that we are party to
- in order to carry out legally required duties
- in order for us to carry out our legitimate interests
- to protect your interests and
- where something is done in the public interest.

All of the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data. For example, we need to collect your personal data in order to:

- carry out the employment contract that we have entered into with you and
- ensure you are paid.

We also need to collect your data to ensure we are complying with legal requirements such as:

- ensuring tax and National Insurance is paid
- carrying out checks in relation to your right to work in the UK and
- making reasonable adjustments for disabled employees.

We also collect data so that we can carry out activities which are in the legitimate interests of YMCA Trinity Group. We have set these out below:

- making decisions about who to offer initial employment to, and subsequent internal appointments, promotions etc
- making decisions about salary and other benefits
- providing contractual benefits to you
- maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained
- effectively monitoring both your conduct and your performance and to undertake procedures with regard to both of these if the need arises
- offering a method of recourse for you against decisions made about you via a grievance procedure
- assessing training needs
- implementing an effective attendance management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments
- gaining expert medical opinion when making decisions about your fitness for work
- managing statutory leave and pay systems such as maternity leave and pay etc
- business planning and restructuring exercises
- dealing with legal claims made against us
- preventing fraud
- ensuring our administrative and IT systems are secure and robust against unauthorised access

Special categories of data

Special categories of data are data relating to your:

- health
- sex life
- sexual orientation
- race
- ethnic origin
- political opinion
- religion
- trade union membership
- genetic and biometric data.

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations in the field of employment, social security and social protection law
- we must process data for reasons of substantial public interest
- you have already made the data public.

We will use your special category data:

- for the purposes of equal opportunities monitoring
- in our attendance management procedures
- to determine reasonable adjustments
- to monitor and record COVID-19 infections *see appendix page 8*

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

Criminal conviction data

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment. We use criminal conviction data in the following ways:

- To allow information to be discussed and considered before a formal Disclosure and Barring Service (DBS) check is submitted
- To confirm whether you are recorded on the relevant Barred list, if your role is a Regulated Activity (as defined by DBS)
- To manage our safeguarding requirements

We rely on the lawful basis of section 122(2) of the Police Act and the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 to process this data.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out our duties in line with your contract of employment. If you do not provide us with the data needed to do this, we will be unable to perform those duties, eg ensuring you are paid correctly. We may also be prevented from confirming, or continuing

with, your employment with us in relation to our legal obligations if you do not provide us with this information eg confirming your right to work in the UK or, where appropriate, confirming your legal status for carrying out your work via a criminal records check.

Sharing your data

Your data will be shared with colleagues within YMCA Trinity Group where it is necessary for them to undertake their duties. This includes, for example, your line manager for their management of you, the HR department for maintaining personnel records and the payroll department for administering payment under your contract of employment.

We share your data with third parties as follows:

- obtaining references as part of the recruitment process – as given by you on your application form
- Sage Payroll - To process your salary payments
- Rotageek – to process timesheets and attendance records
- Pension providers, depending on your contract either NEST, Scottish Widows or People's Pension – to pay your pension contributions
- Pyramid - to process your expense payments
- HMRC - To ensure the correct tax and National Insurance payments are made on your behalf
- Auditors – to ensure legal compliance and rule out any financial malpractice
- IRIS Cascade HR & Payroll – To process your electronic Personnel file and process your salary payments
- Inform – Members of the Accommodation Team, in order to carry out your day to day duties
- MyConcern – To enable reporting and management of safeguarding concerns
- Training providers (various) – To register you for courses
- Hive – name, DOB and work email. To participate in work related surveys, all data is processed & reported anonymously
- Health & Safety Executive – in RIDDOR situations
- LoneAlert – Those using loneworker devices only
- Simply Health or Health Assured, as relevant – to provide Employee Benefits package
- Grant funders – To demonstrate compliance with funding applications
- Occupational Health – After gaining signed consent from you
- National Council of YMCA (YMCA England and Wales) – To provide the Death in Service benefit.
- Charity Commission – Board of Trustees & Chief Executive only
- Companies House – Board of Trustees only

We may share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us.

We share data outside of the EEA in very limited circumstances, relevant to CCTV log in details only. Please see the CCTV Verkada Privacy Statement for more details here .

Medical Emergencies

In a medical emergency, including mental health emergencies, YMCA Trinity Group may deem it necessary to share people's information with the emergency services or other health professionals.

In all cases any information shared will be proportionate to the incident and the professional involved.

The Next of Kin (as per individual Cascade records) may also be contacted. The details of any health emergency would be shared proportionately and a more limited account of the situation shared with the nominated NOK than with the emergency services.

Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such:

- Secure storage of paper HR files – lockable, fire proof cabinets
- Comprehensive ICT policy and procedures
- Limiting access to your data on Cascade via hierarchy profiles
- Records and Retention policy and procedure

Where we share your data with third parties, we request copies of their policies to ensure that your data is held securely and in line with Data Protection requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data. Copies of these policies are available here

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 documented instructions.

How long we keep your data for

In line with data protection principles, we only keep your data for as long as we need it for, which will be at least for the duration of your employment with us though in some cases we will keep your data for a period after your employment has ended. Retention periods can vary depending on why we need your data, as set out in our Retention Schedule. Details available on request.

Automated decision making

No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

Your rights in relation to your data

The law on data protection gives you certain rights in relation to the data we hold on you. These are:

- the right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy statement
- the right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request. You can read more about this in our Subject Access Request policy which is available from HR.
- the right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it
- the right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it
- the right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we may stop processing the data (whilst still holding it) until we have ensured that the data is correct
- the right to portability. You may ask that we transfer the data that we hold on you to a third party, for your own purposes
- the right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests
- the right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.
If you wish to exercise any of the rights explained above, please contact a member of the HR team.

Making a complaint

The supervisory authority in the UK for data protection matters is the Information Commissioner (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO.

Changes to this Privacy statement

We reserve the right to update this statement at any time, and we will provide you with a new privacy statement when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

Appendix: Covid-19

YMCA Trinity Group aims to provide a safe working environment for our staff and clients.

YMCA Trinity Group has a legitimate interest to record and process absence and testing data related to COVID-19. This data falls under 'special category data' as it is medical data.

COVID-19 data processing will be for the conditions of health and social care and for public health; specifically of infection control (including 'track & trace' + RIDDOR reporting) and workforce planning.

Should a member of staff believe they, or a member of their family, is infected with or absent due to COVID-19/ Corona Virus, they should inform their line manager as soon as possible as per the usual absence reporting procedure (see Staff Handbook for more details).

If a member of staff, either through workplace referral or self-referral has a positive PCR COVID-19 test, we request that they inform us of their test date and the outcome as soon as it is received. Failing to report a suspected Covid-19 infection or test outcome may result in disciplinary action being taken.

COVID-19 related absence records are securely recorded on Cascade and processed by the HR department. Sight of these records is limited to the individual and their departmental line managers as per the organisational hierarchy (line manager's supervisor up to relevant Executive). All Childcare testing details are retained as requested by the DfE. For more details, see the Mass Testing (COVID) Policy and Procedure.

In order to fulfil our 'track & trace' responsibilities, data on positive COVID-19 test results will be shared anonymously with relevant colleagues. To fulfil our RIDDOR reporting responsibilities we would have to disclose, confidentially, further details of the individual affected as a legal requirement.

COVID-19 Retention schedule
Medical records related to COVID-19, including test outcomes, are planned to be permanently deleted after 3 years. This retention schedule for this data will be under constant review and may be shortened or extended without notice.

This appendix to the Employee Privacy Notice can change at any time and without notice. The most up to date version can be located via Cascade> documents> Employee.