Clarity Independent School

Privacy Notice for Employees

In accordance with the General Data Protection Regulation (GDPR), we have implemented this privacy notice to inform you, our employees, of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

This notice applies to current and former employees and workers.

A) Data Protection Principles

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing is fair, lawful and transparent
b) data is collected for specific, explicit, and legitimate purposes
c) data collected is adequate, relevant and limited to what is necessary for the purposes of processing
d) data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we comply with the relevant GDPR procedures for international transferring of personal data

B) Types Of Data Held

We keep several categories of personal data on our employees to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data, as appropriate to your status:

a) personal details such as name, address, phone numbers
b) name and contact details of your next of kin
c) your photograph
d) your gender, marital status, information of any disability you have or other medical information
e) right to work documentation
f) information on your race and religion for equality monitoring purposes
g) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter

h) references from former employers
i) details on your education, qualifications and employment history etc
j) National Insurance numbers
k) bank account details
l) tax codes
m) driving licence
n) criminal convictions
o) information relating to your employment with us, including:

   i) job title and job descriptions
   ii) your salary
   iii) your wider terms and conditions of employment
   iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
   v) internal and external training modules undertaken
   vi) information on time off from work including sickness absence, family related leave etc

p) CCTV footage
q) building access attendance records
r) IT equipment use including telephones and internet access.

C) Collecting your Data

You provide several pieces of data to us directly during the recruitment period and subsequently upon the start of your employment.

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 files or within the Company's HR and IT systems.

Workforce data is essential for the school's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with UK GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

D) Lawful Basis for Processing

The law on data protection allows us to process your data for certain reasons only. In the main, we process your data in order to comply with a legal requirement or in order to effectively manage the employment contract we have with you, including ensuring you are paid correctly.

The information below categorises the types of data processing, appropriate to your status, we undertake and the lawful basis we rely on.

Activity requiring your data	Lawful basis
Carry out the employment contract that we have entered into with you e.g. using your name, contact details, education history, information on any disciplinary, grievance procedures involving you	Performance of the contract
Ensuring you are paid	Performance of the contract
Ensuring tax and National Insurance is paid	Legal obligation
Carrying out checks in relation to your right to work in the UK	Legal obligation
Making reasonable adjustments for disabled employees	Legal obligation
Making recruitment decisions in relation to both initial and subsequent employment e.g. promotion	Our legitimate interests
Making decisions about salary and other benefits	Our legitimate interests
Ensuring efficient administration of contractual benefits to you	Our legitimate interests
Effectively monitoring both your conduct, including timekeeping and attendance, and your performance and to undertake procedures where necessary	Our legitimate interests
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	Our legitimate interests
Implementing grievance procedures	Our legitimate interests
Assessing training needs	Our legitimate interests
Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments	Our legitimate interests
Gaining expert medical opinion when making decisions about your fitness for work	Our legitimate interests
Managing statutory leave and pay systems such as maternity leave and pay etc.	Our legitimate interests
Business planning and restructuring exercises	Our legitimate interests
Dealing with legal claims made against us	Our legitimate interests
Preventing fraud	Our legitimate interests
Ensuring our administrative and IT systems are secure and robust against unauthorised access	Our legitimate interests
Providing employment references to prospective employers, when our name has been put forward by the employee/ex-employee, to assist with their effective recruitment decisions	Legitimate interest of the prospective employer

E) Special Categories of Data

Special categories of data are data relating to your:

a) health
b) sex life
c) sexual orientation
d) race
e) ethnic origin
f) political opinion
g) religion
h) trade union membership
i) genetic and biometric data.

We carry out processing activities using special category data:

a) for the purposes of equal opportunities monitoring
b) in our sickness absence management procedures
c) to determine reasonable adjustments

Most commonly, we will process special categories of data when the following applies:

a) you have given explicit consent to the processing
b) we must process the data in order to carry out our legal obligations
c) we must process data for reasons of substantial public interest
d) you have already made the data public.

F) Failure to Provide Data

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract of employment with you. This could include being unable to offer you employment or administer contractual benefits.

G) 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 to determine your suitability, or your continued suitability for the role. We rely on the lawful bases of legal obligation and contractual obligations to process this data.

H) Who we Share your Data With

Employees within our company who have responsibility for recruitment, administration of payment and contractual benefits and the carrying out performance related procedures will have access to your data which is relevant to their function. All employees with such responsibility have been trained in ensuring data is processing in line with GDPR.

Data is shared with third parties for the following reasons:

- The administration of payroll and pensions
- Disclosure and barring (DBS) checks
- Occupational Health appointments (with your prior permission)

- Reference checks with previous employers
- Training courses
- Privileged legal advice
- Purchasing ID cards for lanyards
- Staff within this school
- Parents and clients using the service
- Relevant staff from other schools which a child you have worked with / are working with, may have attended / are about to attend
- Ofsted/Independent Schools Inspectorate (ISI) for the purposes of regulation of the school
- Contracted-in professionals such as Speech and Language Therapist, Occupational Therapist, Well-being Coach, Forest Schools Teacher etc.

We may also 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 have a data processing agreement in place with such third parties to ensure data is not compromised. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

We do not share your data with bodies outside of the European Economic Area.

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

I) 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.

J) Retention Periods

We only keep your data for as long as we need it, 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. Some data retention periods are set by the law. We determine the retention period of other data based on our legal obligations and the necessity of its retention for our business needs. Our retention periods are:

- Regulatory data – case closed no action taken 2 years
  - case closed action taken 6 years
- Data protection and complaints (physical items which cannot be scanned or returned) – 6 months
- Breach report – no action taken case closed 2 years, breach report action taken case closed 6 years
- Communication data – 5 years
- Internal Regulatory Activities (including policies, guidelines, research, decision making) – 6 years
- Data privacy impact assessments – 6 years
- Corporate Governance – internal committee and groups minutes – 6 years, plans, business continuity, policies, business management and strategies – 3 years
- Corporate functions – Health and safety, property management and asset records – 6 years
- IT system running and long-term use – 12 months
- Records and information management – 3 years
- Information requests – 2 years
- IT back-ups – 6 months

- Performance Management Information – 2 years
- CCTV – 1 month
- Reception sign in book – 2 years
- Finance information and payroll reports – 2 years, payroll sheets 6 years
- Human Resources – Personnel Development Records and Employee Files - 6 years, Disciplinary and grievance, accident and ill health, assessment and testing – 6 years, Job Descriptions, training material and Terms and Conditions – 6 years, annual leave (general) 3 years, maternity, paternity adoption and sick leave – 3 years, successful recruitment candidate information (including third party referee details provided by applicant) – 6 months from end of employment, unsuccessful recruitment candidate information (including third party referee details provided by applicant) – 6 months from last action, staff pension, pay history and termination reasons – 100 years from DOB, health surveillance – 40 years from last action, third party emergency contact details provided by the staff member – immediately upon end of employment, equality and diversity published information – 6 years from last action, marriage certificate and documents relating to civil registration – 100 years from DOB, Medical / self-certificates unrelated to industrial injury – 4 years from end of absence
- Corporate communications and marketing – press releases – 3 years, staff events (marketed) – 3 years, conference delegate lists – 400 days from conference, webinar registration – 1 month, communications with journalists – 12 months
- Legal advice – 6 years from last action, enforcement legal cases – 6 years, contracts – 6 years, unsuccessful tenders – 400 days from last action, buildings contracts and leases – 12 years from end of contract, non-disclosure agreements – 2 years from last action, case summaries and background documents – 6 years from last action.
- Communication activities – staff mailboxes and outlook, internal, external and customer mailboxes – 12 months from creation, physical correspondence once scanned – 6 months
- Organisation wide – drafts (e.g. versions of policies) – significant 3 years, less significant – 12 months, internal audits 3 years, templates and procedures – 3 years, annually renewed documents – 3 years

K) Automated Decision Making

Automated decision-making means making decision about you using no human involvement e.g. using computerised filtering equipment. 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.

L) Requesting Access to your Personal Data

The UK-GDPR gives you certain rights about how your information is collected and used. To make a request for your personal information, contact our Data Protection Officer.

You also have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you. More information on this can be found in our separate policy on Subject Access Requests;

c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information;
h) the right to regulate any automated decision-making and profiling of personal data.
i) the right to withdraw consent at any time (where relevant).
j) The right to complain to the Information Commissioner if you feel we have not used your information in the right way

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it. For example, some rights will not apply:

a) right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
b) right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
c) right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent.

M) Consent

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

N) Making a Complaint

If you have a concern about the way we are collecting or using your personal data, or think your data rights have been breached, you can contact us in the first instance. Alternatively, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

O) Data Protection Compliance

Our Data Protection Officer (DPO) is:

Grace Hanson
Tel: 01245 408 606

Email: Businessmanager@clarity.essex.sch.uk