

This policy applies to information held on behalf of:

- ✘ All Centura Group Companies
- ✘ All Centura Group employees
- ✘ All Centura Group supply chain partners
- ✘ All Centura Group sub-contract or agency workers
- ✘ All Centura Group web-site visitors
- ✘ All Centura Group business partners
- ✘ All third parties whose information may be held by a Centura Group Company

The purpose of this policy is to enable CENTURA GROUP LTD to:

- ✘ Comply with our legal, regulatory and corporate governance obligations and good practice
- ✘ Gather information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- ✘ Ensure business policies are adhered to (such as policies covering email and internet use)
- ✘ Fulfill operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
- ✘ Investigate complaints
- ✘ Check references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- ✘ Monitor staff conduct, disciplinary matters
- ✘ Market our business
- ✘ Improve services

This policy applies to information relating to identifiable individuals e.g. staff, applicants, former staff, clients, suppliers and other third party contacts.

CENTURA GROUP LTD will:

- ✘ Comply with both the law and good practice
- ✘ Respect individuals' rights

- ✘ Be open and honest with individuals whose data is held
- ✘ Provide training and support for staff who handle personal data, so that they can act confidently and consistently

CENTURA GROUP recognises that its priority under the GDPR protection is to avoid causing harm to individuals. In the main this means:

- ✘ Complying with your rights,
- ✘ Keeping you informed about the data we hold, why we hold it and what we are doing with it,
- ✘ Keeping information securely in the right hands, and
- ✘ Holding good quality information.

GDPR aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, CENTURA GROUP LTD will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used. This includes the right to erasure where data is no longer necessary and the right to rectification where the data is incorrect. Full details are available in the Privacy Notice issued at the point of gathering the data.

CENTURA GROUP LTD has identified the following potential key risks, which this policy is designed to address:

- ✘ Breach of confidentiality (information being given out inappropriately)
- ✘ Insufficient clarity about the range of uses to which data will be put — leading to Data Subjects being insufficiently informed
- ✘ Failure to offer choice about data use when appropriate
- ✘ Breach of security by allowing unauthorised access
- ✘ Failure to establish efficient systems of managing changes, leading to personal data being not up to date
- ✘ Harm to individuals if personal data is not up to date
- ✘ Insufficient clarity about the way personal data is being used e.g. given out to general public
- ✘ Failure to offer choices about use of contact details for staff, clients workers or employees.

In order to address these concerns, to accompany this policy, we have an accompanying Information Security Policy and we will issue Privacy Notices to explain what data we have, why we have it and what we will do with it. The Privacy Notice will also explain the data subject's rights. We will offer training to staff where this is necessary and appropriate in the circumstances to ensure compliance with GDPR. Such training will vary according to the role, responsibilities and seniority of those being trained.

We aim to keep data only for so long as is necessary which will vary according to the circumstances.

We have no intention to transfer data internationally.

All Group managers, departmental managers and processors are responsible for their own department's data as follows:

- ✂ Reporting breaches to the Information Commissioners Office and the relevant Data Subject(s)
- ✂ Briefing the board on Data Protection responsibilities
- ✂ Approving contracts with Data Processors
- ✂ Ensuring all Data is stored securely
- ✂ Maintain a Data Audit and keep this up to date
- ✂ Ensuring that Data Protection induction and training takes place
- ✂ Ensuring department Data is stored securely
- ✂ Notification to all suppliers, clients/customers/staff
- ✂ Ensuring Data is stored securely

In addition, the Group HR department are responsible for:

- ✂ Handling subject access requests
- ✂ Approving unusual or controversial disclosures of personal data

Significant breaches of this policy will be handled under CENTURA GROUP LTD disciplinary procedures which may amount to gross misconduct.

Subject Access Request

Subject access requests must be in writing. All staff are required to pass on anything, which might be a subject access request without delay. The applicant will be given their data within 1 month unless there are complexities in the case which justify extending this to 2 months. You will be notified of any extensions to the deadline for response and the reasons as soon as possible.

We have the right to refuse a subject access request where data is requested at unreasonable intervals, manifestly unfounded or excessive. You will be notified of the reasons as soon as possible.

Where the individual making a subject access request is not personally known to The HR Team their identity will be verified before handing over any information.

The required information will be provided in a permanent and portable form unless the applicant makes a specific request to be given supervised access in person.

You have the right to request the information we hold is rectified if it is inaccurate or incomplete. You should contact the relevant named staff and provide them with the details of any inaccurate or incomplete data. We will then ensure that this is amended within one month. We may, in complex cases, extend this period to two months.

You have the right to erasure in the form of deletion or removal of personal data where there is no compelling reason for its continued processing. We have the right to refuse to erase data where this is necessary in the right of freedom of expression and information, to comply with a legal obligation for the performance of a public interest task, exercise of an official authority, for public health purposes in the public interest, for archiving purposes in the public interest, scientific research, historical research, statistical purposes or the exercise or defence of legal claims. You will be advised of the grounds of our refusal should any such request be refused.

Employee Privacy Notice

This notice is provided with the intention to comply with your right to be informed under the General Data Protection Regulation.

We will hold and process the following information:

1. Your personal and contact details including your name, address, telephone numbers, emails
2. Particulars of your employment including your job title, salary, benefits

3. Financial information including your bank details, N.I No; tax statements, payslips
4. Particulars of your right to work in the UK
5. Particulars of your qualifications and skills including references, licences, certificates and training
6. Emergency contact information
7. Particulars of your performance including tasks, attendance
8. Sensitive information including protected characteristics under the Equality Act 2010 for Equal Opportunities Monitoring and Compliance
9. IT usage information including email addresses, log-ins, passwords
10. Particulars of processes e.g. disciplinary, grievance, performance management processes undertaken with you
11. Copies of letters and communications between us and you.
12. Occupational Health personal information including Health Assessment Certificates

We are the controller of this information and we are also the processor of this information. This data has been gathered with your consent and in the legitimate interest of assisting us in fulfilling the contractual requirements to supply hours and pay in the course of your employment. It will also be necessary for us to hold and process this data in the interests of your health, safety and welfare in work.

This is done on the basis of your consent and the legitimate interests to safeguard your health, safety and welfare and the health, safety and welfare of your colleagues, clients and third parties in the workplace. Your data is also processed in accordance with a contractual requirement between us and your employer. The failure to provide us with the data or to withdraw your consent may impact upon your recruitment, employment or tasks, duties and responsibilities with your role and/or assignment. You should discuss the further impact of this with your manager.

The recipients of your data are us and we anticipate that we may need to share personal data with the HMRC (e.g. your Name and National Insurance Number), HSE (e.g. your Name and Employment Details where there has been a reportable accident or investigation), Legal Advisers and professional advisers (e.g. your name and employment details where we need advice), Tribunals and Courts (e.g. your name, employment details and other personal data which is necessary for the determination of claims where litigation is commenced). It is not anticipated that there will be any other recipients nor any transfers of data to a third country. Accordingly, it is considered that safeguards for the transfer of data to a third country are not necessary. Should this change you will be notified.

Your employment data will be kept for the duration of your employment and for a further period thereafter of 12 months. This period has been set for the protection of our organisation throughout your employment and for a period thereafter in the event of any employment tribunal claims. If such a claim has been filed, the data will be retained for a period of 6 years following resolution of that claim and for 6 years following the resolution of any further claims. This period has been determined for the protection of the organisation in the event any professional negligence or breach of contract claims in the event we use representation to defend any claims.

Your financial data will be kept for the duration of your employment and for a further period thereafter of 6 years. This period has been set for the protection of our organisation throughout your employment and for a period thereafter in the event of any employment tribunal or breach of contract claims. If such a claim has been filed, the data will be retained for a period of 6 years following resolution of that claim and for 6 years following the resolution of any further claims. This period has been determined for the protection of the organisation under HMRC requirements and in the event any professional negligence or breach of contract claims in the event we use representation to defend any claims.

You have the right;

- ✂ to be informed of fair processing information with a view to transparency of data. This statement is intended to fulfil that right
- ✂ to access the information we hold. You should make such a request in writing to Sharon O'Sullivan, Group HR Executive
- ✂ to request the information we hold is rectified if it is inaccurate or incomplete. You should contact Sharon O'Sullivan using the above contact information and provide her with the details of any inaccurate or incomplete data. We will then ensure that this is amended within one month. We may, in complex cases, extend this period to two months
- ✂ to erasure in the form of deletion or removal of personal data where there is no compelling reason for its continued processing. We have the right to refuse to erase data where this is necessary in the right of freedom of expression and information, to comply with a legal obligation for the performance of a public interest task, exercise of an official authority, for public health purposes in the public interest, for archiving purposes in the public interest, scientific research, historical research, statistical purposes

or the exercise or defence of legal claims. You will be advised of the grounds of our refusal should any such request be refused

- ✂ to restrict our processing of your data where contest the accuracy of the data until the accuracy is verified
- ✂ to restrict our processing of your data where you object to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our organisation's legitimate grounds override your interests
- ✂ to restrict our processing of your data when processing is unlawful, and you oppose erasure and request restriction instead
- ✂ to restrict our processing of your data where we no longer need the data and you require the data to establish, exercise or defend a legal claim. You will be advised when we lift a restriction on processing
- ✂ to data portability in that you may obtain and reuse your data for your own purposes across different services, from one IT environment to another in a safe and secure way, without hindrance to usability. The exact method will change from time to time. You will be informed of the mechanism that may be in place should you choose to exercise this right

You have the right to object to the following:

- ✂ processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- ✂ direct marketing (including profiling); and
- ✂ processing for purposes of scientific/historical research and statistics (the data collected is not anticipated to fall within the above categories)

You have the right to withdraw your consent at any time.

You have the right to lodge a complaint with a supervisory authority such as the Information Commissioner's Office or any other of our regulators or accreditors that may regulate or provide accreditations to us from time to time.

Website Data Management

All Centura Group businesses protect and make use of the information you give them when you correspond with or use their website. It also covers all data provided by our material suppliers and sub-contractors.

The data gathered will only be used in the way described in this policy in compliance with the General Data Protection Regulation 2018.

This policy is updated from time to time. The latest version can be found on the Centura Group website – www.centuragroup.co.uk

If you have any questions about this policy, please contact the individual group business via the privacy link on the website.

What data we gather

We may collect the following information:

- ✂ Name and job title
- ✂ Contact information including email address
- ✂ Demographic information such as postcode, preferences and business sector interests
- ✂ Correspondence
- ✂ Other information relevant to client enquiries
- ✂ Project history with Centura Group companies
- ✂ Project feedback

How we use the data

Collecting the data helps us understand what business sectors you are interested in. For our suppliers and sub-contractors, it allows us to send out tender enquiries to specific companies and individuals

Specifically, we may use data:

- ✂ For our own internal records
- ✂ To comply with all current legislation and contractual obligations
- ✂ To improve the products and services we provide
- ✂ To contact you in response to a specific enquiry
- ✂ To send promotional emails about products, services and other things we think might be relevant to you
- ✂ To correspond with you via email, telephone or mail

Controlling information about you

When you are included in correspondence with us through email, telephone, meetings, exhibitions, website or any other means we will assume you consent for us to retain your contacts details.

If do not wish to remain on our database, you can request the information to be deleted via one of three methods:

- ✂ When you receive an email newsletter there will be an opt out button for all future correspondence
- ✂ You will find a privacy settings button on the individual group company websites where you may opt out
- ✂ Write to the individual group company requesting that your details are deleted.

We will never lease, distribute or sell your personal information to third parties unless we have your permission, or the law requires us to.

Any personal information we hold about you is stored on our servers located in the UK and processed under our data protection policy in compliance with the General Data protection regulation.

Security

We always hold your information securely.

To prevent unauthorised disclosure or access to your information, we have secure IT data management systems in place. Our IT services are managed in-house for the Group businesses and the data is stored on our own servers with password protection. Please refer to our 'GDPR – Information Security Policy'

In Centura the employees responsible for the protection of your data are:

- ✂ Personnel, payroll, training and HR data - Group HR Executive
- ✂ Finance and supply chain data - Group Systems & Management Accountant
- ✂ Website, CRM Database and B2B data - Sales and Marketing Director

Your data will be used to assign you work, provide you with hours of work, pay you, monitor your performance, write to you with important documents, check your skills, qualifications and experience, appraise your performance and safeguard your health, safety and wellbeing in the workplace.

A P Rimoldi

Group Chief Executive

March 2020