DN COLLEGES GROUP

This notice explains how DN Colleges Group ("the College", "we", "us", or "our") handles your personal data when you apply for a job or vacancy with us. It outlines our commitment to protecting your privacy and your rights under the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR).

WHO WE ARE

We are DN Colleges Group, based at The Hub, Chappell Drive, Doncaster, DN1 2RF (ICO Registration: ZA341759). For any queries regarding your data, contact our Data Protection team at dataprotection@dncolleges.ac.uk.

WHAT DATA WE COLLECT AND WHY

We collect and process your personal data to evaluate your application, manage our recruitment processes, and fulfil our legal obligations as a potential employer.

Information Collected During Recruitment:

- **Contact and Biographical Details:** Name, email address, telephone number, postal address, and date of birth.
- **Social Sign-In and Authentication Details:** If you choose to register or sign in to our application portal via third-party Single Sign-On (SSO) providers (such as Google or LinkedIn) we collect your name, email address, and profile identifier as permitted by your privacy settings on those platforms.
- **Application and Employment History:** CVs, cover letters, application forms, employment history, qualifications, professional memberships, and references.
- **Vetting and Right to Work:** Proof of identity, right to work in the UK documentation, and pre-employment screening data.
- **Special Category Data:** With your consent or where legally required, we process sensitive data such as health or disability information (to provide reasonable adjustments during the interview process).
- **Equality Monitoring**: We collect data on gender, nationality, and ethnicity to monitor diversity and meet statutory reporting duties.

WHY WE USE YOUR DATA (LAWFUL BASIS)

We process your information using the following legal bases:

- **Contract / Pre-Contractual Steps:** To evaluate your application, verify your information, and take steps at your request prior to entering into an employment contract.
- **Legal Obligation:** To meet statutory duties such as verifying your right to work in the UK and carrying out necessary safeguarding checks.
- **Legitimate Interests:** For the effective administration and management of our recruitment and selection processes, including security and fraud prevention on our portal.

- **Consent:** Where you choose to sign in via third-party single sign-on services (such as Google or LinkedIn) or where special category data is voluntarily provided for diversity monitoring or candidate adjustments.

HOW WE SHARE YOUR DATA

We only share your recruitment data when there is a justified purpose:

- **Recruitment Platform Providers**

We use networx Recruitment (and their candidate portal platform) to host, receive, and manage job applications on our behalf.

- **Authentication Service Providers** If you select the option to sign in using Google or LinkedIn, limited account information is securely exchanged with these providers to authenticate your identity.
- **Government and Regulatory Bodies** HMRC, DfE, and local authorities where statutory obligations apply.
- **Disclosure and Barring Service (DBS)** To carry out necessary background and safeguarding checks for successful applicants.

HOW LONG WE KEEP YOUR DATA

We retain applicant records in line with our Records Management Policy.

- **Unsuccessful Applicants:** Personal data collected during the recruitment process will typically be retained for up to 12 months following the completion of the vacancy campaign for legal, auditing, and feedback purposes.
- **Successful Applicants:** If your application is successful, the information gathered during recruitment will be transferred to your employee personnel record and retained in line with our Staff Privacy Notice.

DATA SECURITY

We take a robust approach to security. Our systems are protected by firewalls and intrusion detection. We have achieved Cyber Essentials Plus, ensuring we are protected against hacking and phishing attacks. All candidate data processed via our external partners and recruitment platform providers is securely stored and encrypted in transit and at rest.

YOUR RIGHTS AND PRIVILEGES

Privacy rights

You can exercise the following rights:

- The right to access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to object to processing;

- The right to data portability;

To exercise these rights, please contact dataprotection@dncolleges.ac.uk.

Update your information and withdraw your consent

If you believe that the information we hold about you is inaccurate or request its rectification, deletion, or object to legitimate interest processing, please do so by contacting us.

Access Request

In the event you want to make a Data Subject Access Request, please contact us. We will respond to requests regarding access and correction as soon as reasonably possible. Should we not be able to respond to your request within thirty (30) days, we will tell you why and when we will be able to respond to your request. If we are unable to provide you with any Personal Data or to make a correction requested by you, we will tell you why.

Complaints

The Information Commissioner's Office (ICO) is the UK's independent supervisory authority for data protection matters. Under the Data (Use and Access) Act, you have the statutory right to lodge a complaint with the ICO if you believe your personal data has been processed unlawfully or your data rights have been infringed. However, you are required to raise your complaint directly with us as the data controller in the first instance to give us an opportunity to resolve the matter.

The ICO will typically only intervene if you have exhausted our internal data protection complaints procedure, if we fail to formally acknowledge your complaint within 30 days of receipt, or if you remain dissatisfied with our final substantive outcome response. For further details or to report a concern to the regulator, please visit the ICO website (www.ico.org.uk).

Data Breaches and Notification

Databases or records containing Personal Data may be breached accidentally or through unlawful intrusion. As soon as we become aware of a data breach, we will notify all affected individuals whose Personal Data may have been compromised, and the notification will be accompanied by a description of the measures that will be taken to repair the damage caused by the data breach. Notifications will be sent as soon as possible after the violation is discovered.

What we do not do

- We do not sell your Personal Data;
- We do not process Special Category Data without obtaining prior specific consent; and
- We do not use automated decision-making, including profiling.

CHANGES

This notice is the current version as of November 2026. If we make significant changes, we will update the effective date and notify you via our website.