EMPLOYEE PRIVACY NOTICE

This statement is needed because of new data protection requirements arising from the UK General Data Protection Regulation ("UK GDPR"), which came into effect on 31st January 2020.

The Abbey DLD Group ("the organisation") collects and processes personal data relating to its employees to manage the employment relationship. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the organisation collect?

The organisation collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to benefits such as pensions or private medical cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

The organisation collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments. Personal data about you will also be created throughout your employment, such as during the appraisal process.

Data is stored in a range of different places, including in your personnel file, in the organisation's HR management systems and in other IT systems (including the organisation's email system and network folders). Some information about you is also stored on the Group's Single Central Register.

Why does the Abbey DLD Group process personal data?

The organisation needs to process data about you for a variety of reasons, which are explained below, along with the legal basis on which we are relying in order to process your information.

Necessary for the performance of your employment contract

Much of what we will do with your data will be linked to your employment contract, and is necessary for us to fulfil our obligations to you under that contract. For example, we need to process your bank details in order to make a payment of salary to you, we may need to provide your personal data to a pension provider that you can benefit from your pension entitlement, and we may need to use your data to provide you with any contractual benefits to which you are entitled.

The organisation has a legal obligation to use your personal data in a particular way

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. The organisation also has to comply with our legal duty to safeguard pupils, which may mean that we have to investigate complaints, and make referrals to other agencies such as the Local Authority, or the DBS. It is also necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question and to comply with safeguarding requirements.

The processing is necessary for the performance of a task carried out in the public interest

The education of pupils is a task carried out in the public interest, and it will be necessary for the organisation to use your personal data to carry out this task. For example, we will provide training and support to you to carry out your role effectively. We will use your data in the course of providing education and support to the pupils, and we may need to use you information to fulfil our safeguarding requirements, where this does not amount to a legal obligation, but the use is nonetheless in the public interest.

The use is a legitimate interest of the organisation

In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- Undertake effective personnel management:
    - run recruitment and promotion processes;
    - maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
    - operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
    - operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;

  - operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
  - obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, and meet its obligations under health and safety law,
  - operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
  - ensure effective general HR and business administration;
  - provide references on request for current or former employees;
- obtain relevant professional advice where required in relation to legal claims, and financial matters;
- obtain and maintain relevant insurance;
- deal with parental and other complaints;
- comply with any relevant requirements linked to the inspection regime.

Where the organisation relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Protection of vital interests

Information may be used in an emergency to protect your vital interests or those of another.

Special category data

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring.

Who has access to data?

Your information will be shared internally, including with members of the HR team (including payroll), your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

The organisation shares your data with third parties in order to obtain pre-employment references from other employers, and obtain necessary criminal records checks from the Disclosure and Barring Service. The organisation may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The organisation also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits, compliance with safeguarding and right to work

and for the provision of occupational health services. These third parties will be directly responsible under data protection law for protecting the personal data as controllers, the organisations we share your data with are;

- The Access Group (HR & Recruitment system supplier);
- Capita (SIMS Supplier);
- Paycircle (Payroll Provider);
- Scottish Widows;
- AXA Healthcare (Private Medical)
- Health Assured (Online health checks & Occupational health referrals);
- Benefex (Pension Administrator);
- Unum (Life Assurance provider);
- Mercer March (Benefits Administrator – Private Medical);
- Back Office Admin Solutions (DBS checks), and
- Veristat (Assistance with eligibility to work compliance and Visa advice)

We may also share your personal data with third parties in the following circumstances:

- Where the sharing is necessary for us to obtain advice from professional advisers and/or consultants;
- Where necessary in order to comply with any inspection - this may involving sharing with the Independent Schools Inspectorate and the Department for Education;
- When making or investigating the possibility of an insurance claim, we may need to share information with our insurance company;
- Where an individual is exercising their right of Subject Access under the UK GDPR, and it would be reasonable for the organisation to release your personal data;
- In relation to any health and safety incident, it may be necessary to share data with the Health and Safety Executive;
- Where a complaint is made by you or about you, we may need to share your personal data with the other parties involved;
- When allegations of misconduct are alleged, it may be necessary to share information with a relevant statutory agency;
- In the course of any safeguarding investigation it may be necessary to share your personal data with the Local Authority Designated Officer (or equivalent);
- Where staff lists, policies or documentation are published on a company website, personal data such as your name, role and work contact details may be shared;
- In some circumstances it may be necessary to share information with the police;
- With parents and pupils in relation to your professional duties - such as telling a pupil that you will be a class teacher, or what your extracurricular remit is;
- In an emergency, we may need to disclose your details to protect you, or others;
- Where we are a Tier 2 sponsor, we may need to share information with UK Visa and Immigration;

The organisation will not transfer your data to countries outside the European Economic Area unless necessary; for example, for communications with Abbey DLD Group staff or contractors.

How does the organisation protect data?

The organisation takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does the organisation keep data?

Retention periods are outlined in the Group *Data Retention Policy*, which employees can access on the Portal.

Your rights under UK GDPR

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing; and
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

If you would like to exercise any of these rights or make a subject access request, please contact dpo@abbeydld.co.uk.

If you are dissatisfied with any aspect of the Group's handling of your personal data you have a right to lodge a complaint with the Information Commissioner's Office (https://ico.org.uk).

What if you do not provide personal data?

You have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making.

Contact

If you have any questions concerning this statement or the policies or procedures referred to above, please contact dpo@abbeydld.co.uk or in writing to: Abbey DLD Colleges Limited, Homerton Gardens, Cambridge, CB2 8EB.