



INSPIRE EDUCATION GROUP PRIVACY POLICY

References in this statement to “IEG” “Group” “College”, “we”, “our”, and “us”, etc. are references to us, Inspire Education Group, operating as Peterborough College and Stamford College.

Purpose

The General Data Protection Regulation (GDPR) came into force on the 25 May 2018. IEG has implemented a comprehensive programme of work delivering the changes necessary for GDPR compliance. This privacy policy should be used alongside the GDPR Policy.

IEG also has a data protection statement that sets out our commitment to the safeguarding of personal data processed by its staff and students and our stances on compliance with data protection legislation. This statement describes how IEG will discharge its duties in order to ensure compliance with the data protection principles and rights of data subjects in particular and will be updated for GDPR in due course.

You can find information about GDPR from the Information Commissioner’s Office (ICO). The ICO is the UK regulator who oversees compliance with data protection legislation.

Notice about how we use your personal information

We are the data controller of personal information about you.

We are: Inspire Education Group

Our address is: Park Crescent, Peterborough PE1 4DZ

Our Data Protection Officer is Rob Cottrell

If you have any questions about this statement or the ways in which we use your personal information, please contact our Data Protection Officer at the above address or via email at: DPO@ieg.ac.uk

This privacy notice has been prepared in accordance with the UK General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018.

IEG is committed to protecting your privacy and respecting the confidentiality of information which you provide when you visit our websites at:

- <https://www.ieg.ac.uk>
- <https://www.peterborough.ac.uk>
- <https://www.stamford.ac.uk>
- <https://www.ucp.ac.uk>
- <https://www.stamfordfitness.co.uk>



- <https://www.parcsnursery.co.uk>
- <https://www.stamfordgastraining.co.uk>
- <https://www.ap4u.training>

At the same time, we want to try to ensure that you obtain full value from our website and from the services which you may want to receive via our website.

You should read this privacy statement in conjunction with all of the IEG's website terms of use, of which this privacy statement forms a part. By agreeing to our terms of use, you are consenting to our processing of your personal data in accordance with this privacy statement. Any changes to this privacy statement will be posted on our website and, where appropriate, notified to you by email.

It is possible to use our website without providing any personal data. However, IEG may automatically collect certain information about you when you use our website, including by our use of "cookies", such as the IP address of your computer and the dates and times of your visits.

In some areas of our website, IEG may ask you for personal data, such as your name, address and email details, that will enable us to make your site visit a more rewarding experience for you and/or to contact you after your visit. Examples of this might be where you complete an online form asking for a copy of a prospectus or to book a place on an open day with us, where you ask for information about a job vacancy, or where you subscribe to an online newsletter.

In some other areas of our website, where you can register as an online user, IEG may ask you for more detailed information about yourself. In order to provide these types of services, it may be necessary for us to collect and process additional personal data, such as information about your educational history.

Our full GDPR Subject Access Request Statement and Procedure can be found on the website alongside this statement.

The Appendices of this document contains a number of privacy statements specific to job applicants, staff and students.

How we may use this information

Personal data which we collect about you via our website is held on and processed by computers situated at IEG. IEG will retain this data for a reasonable period or for as long as the law requires.

IEG will not disclose any of your personal data collected via our website to any third party, other than in circumstances set out in this privacy statement and/or where you have given us permission to do so, unless we are required to do so by law.

IEG may use personal data collected from you via our website to manage and monitor use of our website. Otherwise, we will only use this personal data for the purposes for which it was collected, unless you have given us permission to use it for other stated purposes. For example, if you supply us with your name and address so we can send you a prospectus for a particular department, and at the same time you



agree that we may send you similar information in the future, we may subsequently invite you to an open day at that department.

There may be circumstances in which IEG will ask you to agree to us disclosing your personal data to certain third parties under this lawful basis.

If at any time you want to withdraw any permission you have given us to provide you with services, or to use your personal data in any other way, please inform us by email.

Your rights

You have a number of rights over your personal information, which are:

- the right to ask us what personal information about you we are holding and to have access to a copy of your personal information;
- the right to ask us to correct any errors in your personal information;
- the right, in certain circumstances such as where our use of your personal information is based on your consent and we have no other legal basis to use your personal information, to ask us to delete your personal information;
- the right, in certain circumstances such as where we no longer need your personal information, to request that we restrict the use that we are making of your personal information;
- the right, in certain circumstances, to ask us to review and explain our legitimate interests to you; and
- the right, where our use of your personal information is carried out for the purposes of an agreement with us and is carried out by automated means, to ask us to provide you with a copy of your personal information in a structured, commonly-used, machine-readable format.

Other websites

Our website may contain links to other websites which are outside IEG's control and are not covered by this privacy statement. We are not responsible for the privacy policies of any such linked websites.

For more information on your privacy and cookies please read our Cookie Notice 2021

Freedom of Information

The IEG website guides you to information and explains how you can request information. The Freedom of Information Act 2000 established a general right of access to information held by public authorities, subject to certain exemptions. So far as is possible, IEG wishes to provide members of the public with any information it holds, on request. IEG is committed to promoting public understanding of its nature and activities via the systematic publication of relevant information. It will provide, where practical and permissible, additional information to members of the public in cases where routinely published information does not provide them with the information they require.

To find out more about the Freedom of Information Act and your rights, please see the Information Commissioner's Office website, <https://ico.org.uk>



Inspire
Education Group



Peterborough
College



Stamford
College



University Centre
Peterborough

Inspire Education Group

We welcome feedback on our policies and procedures and the way they operate. We are interested to know of any possible or actual adverse impact that our policies may have on any groups in respect of gender or marital status, race, disability, sexual orientation, religion or belief, age or other characteristics. Please email any comments to FOI@ieg.ac.uk

How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us at Inspire Education Group.

You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: <https://www.ico.org.uk>



APPENDIX 1

IEG Student Privacy Notice

This notice relates to students at University Centre Peterborough, Peterborough College, Stamford College and Anglia Professional Training

Data controller: Inspire Education Group

Our address is: Park Crescent, Peterborough PE1 4DZ

Data protection officer: Group Director of IT & Digital Innovation, DPO@ieg.ac.uk

IEG runs full-time courses for school leavers 16+, Higher Education courses for students 18+, part-time courses for adults and local business. The Colleges also offers apprenticeships in many sectors.

This Privacy Notice, published in response to the introduction of the General Data Protection Regulations, which came into effect in May 2018, describes what personal data IEG collects, processes, shares and retains during the application and enrolment processes and during our students' period of study.

It applies to full-time students, part-time students, those studying via apprentices. It also refers to the processing of data in relation to our former students via destinations surveys and our alumni association. This notice sits within the group's wider privacy notice. Data we collect:

- Student and apprentice personal information (such as name, student number, address, date of birth, national insurance number)
- Student and apprentice contact information (which may include phone number, email and postal address)
- Parent or guardian personal information in relation to students under the age of 18 (name, address, relationship to student)
- Parent or guardian contact details in relation to students under the age of 18 (email address, phone number)
- Next of kin contact details (email address, phone number)
- Educational Information (including qualifications, school details, predicted grades, learning support needs, attendance information – number of absences and reasons and individual achievements)
- Employment history (apprentices), including reference information · Current employment status and if you are in receipt of benefits
- Protected characteristics (such as sex {legal status}, age, ethnicity, first language, nationality, country of birth and free school meal eligibility)
- Financial information (bank details)
- Information about personal preferences and interests (in relation to programmes of study) · Information about your entitlement to study in the UK
- Information regarding your household situation, including marital status and household member employment status
- Information about your criminal record (declaration of criminal record)
- Details of your schedule (study hours and working hours) and attendance; 2
- Details of periods of absence and the reasons for the absence



- Details of any disciplinary or complaint procedures in which you have been involved, including any warnings issued to you and related correspondence
- Details of achievement, progress reviews and career plans
- Information you disclose in relation to safeguarding issues
- Information on career destinations after leaving College
- Whether you wish to join our Alumni Association after leaving College

Why we process this data

Personal data will be used for purposes relating to education, training, employment, general advice services, well-being, safeguarding and research.

The College may share non-sensitive personal information about you with other organisations as follows:

Most of the information is passed to Government agencies (including but not limited to the Education and Skills Funding Agency) to meet funding arrangements.

Where necessary it is also shared with the Department for Education (DFE). The information is used to enable these Government departments to meet their statutory responsibilities, including legislation relating to the Apprenticeships, Skills, Children and Learning Act 2009.

It is also used, in collaboration with the appropriate organisations, to create and maintain a unique learner number (ULN) and a Personal Learning Record (PLR).

The lawful basis for the College processing the aforementioned personal data is 'legal obligation' and its 'public task' to run its Colleges safely and effectively.

IEG also uses this personal data as follows:

- To process applications, enrolments and contracts
- For the College's own internal records so that it can provide you with a high quality service
- To contact individuals in response to a specific enquiry
- To contact individuals about College services, disruption to services courses, deliver important educational key messages, to provide information on courses leading to academic progression and other messages the College deems to be relevant to its students
- We take photographs of all students as part of the enrolment process. These are used to produce student identification cards. Wearing these cards at all times on our campuses is a mandatory safeguarding requirement of students
- We seek consent to take photographs of students for use on the College website, to be shared with the press, or to be used in the production of marketing materials. This consent is gathered explicitly via a consent form which lays out the exact usage of these photographs and the duration for which they are stored on secure College systems.



At no time will the College assume permission to use information that is provided for anything other than the reasons stated here.

IEG will not send marketing messages or materials on non-college matters or marketing material from third parties. It will only send information relating to IEG services, courses, activities and opportunities that are of legitimate interest to students and parents/guardians.

IEG has identified that it meets a number of lawful basis for processing personal data (as set out in Article 6 of the GDPR). In summary:

- For processing enquiries the lawful basis is legitimate interest
- For communicating with those who have submitted an enquiry i.e. responding to their enquiry, inviting them to related events and sending updates on College activities and opportunities, the lawful basis is legitimate interest
- For processing applications, the lawful basis is legitimate interest
- For communicating with those who have submitted applications i.e. informing them of their application progress, inviting them to related events and sending them updates on College activities and opportunities, the lawful basis is legitimate interest
- For processing information relating to enrolment on an individual's programme of study, the lawful basis is legal obligation in relation to information we are required to provide to Government departments by law and public task in relation to information required to ensure we run the College safely and effectively
- For communicating with enrolled students and their named parent/guardian in relation to College closure, disruption of services, personal performance and attendance and information relating to safeguarding and wellbeing the lawful basis is public task
- For communicating with students in relation to important educational messages, work experience and employment opportunities, College updates and courses that provide progression opportunities, the lawful basis is legitimate interest
- To taking photographs for the production of student ID cards the lawful basis is public task to ensure student safety on campus. Consent is not required
- For communicating with enrolled students and their parents/guardians/carers in relation to College activities and progression opportunities, including new courses the lawful basis is legitimate interest
- For taking photographs of students for marketing purposes the lawful basis is consent, which will be explicit. Consent will be gathered before photographs are taken. Consent can be withdrawn and a request for the data to be destroyed can be made via our Data Protection Officer
- For gathering information about the destination of an individual once they have left the College the lawful basis is legitimate interest
- For contacting individuals who have completed a course at the College for the purposes of inviting them to join our Alumni association or to conduct Government agency research, the lawful basis is legitimate interest.



The information provided may be shared with other organisations for purposes of administration, the provision of career and other guidance and statistical and research purposes, relating to education, training, employment and safeguarding.

This will only take place where the sharing is in compliance with GDPR. Individuals may be contacted after they have completed their programme of learning to establish whether they have entered employment or gone onto further training or education. Following that initial contact and information gathering exercise, individuals will be offered the opportunity to join the College's alumni.

Individuals may be contacted by the European Social Fund (ESF) Managing Authority, or its agents, to carry out research and evaluation to inform the effectiveness of the programme. Information may be passed to the ESF for this purpose.

For how long does the organisation keep data?

We keep data related to the application and enrolment of 16 to 18-year old students on our management of information system for six years, in line with government requirements for the aforementioned legal obligation.

We are currently required to retain personal data on apprentices and adults studying courses funded via the Government's Adult Education Budget until December 2030 in line with European Social Fund regulations.

Security

IEG will hold personal information securely. To prevent unauthorised disclosure or access to personal information, it has strong organisational and technical security safeguards. If information is shared with another organisation (reasons for this are given in the section below) it will ensure an Information Sharing Agreement is in place and that information is transferred securely. The College follows stringent procedures to ensure it processes all personal information in line with the GDPR.

Automated Processing

IEG does not use automated processing and decision making.

Information Sharing and Disclosure

IEG does not sell or rent personal information. Information may by necessity be disclosed to appropriate staff members of IEG and to Government bodies (as previously outlined).

Organisations that IEG may share personal information with includes:

- Awarding Bodies • Department for Education
- Education and Skills Funding Agency • Student Loans Company (where applicable)
- Employers (in relation to apprenticeships, work experience placements and where an employer has funded the course)
- HMRC
- Higher Education Institutions
- Local Authorities



- Ofsted
- Police (where applicable for safeguarding issues)
- Schools
- Social Care (where applicable for safeguarding issues)
- Educational Partnerships sub-contractors
- UCAS

Information may be shared with third parties if it is in connection with the service being provided to individuals, for example, the College might share information with market research companies contracted to undertake work on its behalf to assess satisfaction with the College's service, or to gather employment destinations once students have finished their course. When IEG does this it will always ensure an Information Sharing Agreement is in place.

If, as part of the entry requirements for a course, the College needs to take up a reference or obtain 'disclosure' from the Disclosure and Barring Service, it will inform you beforehand. Parental consent is not required. There may be exceptions in regard to students with severe learning difficulties, school link students and those who are otherwise unable to decide for themselves.

The College has found it beneficial to students' progress if it is able to engage with the parents (or guardian/carer). Therefore, parents' details are recorded on our management of information system. Parents/carers/guardians of further education students (or any other third party) are not automatically entitled to the students' information.

The College can only release information about its students if it has their consent for this recorded on the College management of information system. Students are asked for their consent for sharing information with parents/others when enrolling on its digital portal, or face-to-face at an enrolment event. Students may withdraw their consent at any point by contacting our Data Protection Officer.

We reserve the right to share any personal information we deem necessary with the police and local authorities to ensure the safeguarding of students.

Your rights Accessing Your Own Personal Information

Individuals have the right to ask for a copy of any of their personal information held by IEG. They can make a 'subject access request' under the GDPR.

Make a Subject Access Request by emailing our Data Protection Officer.

You can also contact the Data Protection Officer with any questions about the College's collection and use of personal data.

Requests to delete personal data

One of the key principles which underpins the GDPR is the right of an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This is also known as the right to be forgotten.



Inspire
Education Group



Peterborough
College



Stamford
College



University Centre
Peterborough

Inspire Education Group

Please note, as a current student removal of personal information outlined within this notice, excluding that requiring consent, could jeopardise our ability to continue delivering your course of study.

Any requests from individuals to:

- have inaccurate personal data rectified (right to rectification)
- restrict or suppress processing of personal data (right to restrict processing)
- obtain and reuse personal data across different services (right to data portability)
- object to how personal data is used, should be made directly to our Data Protection Officer



APPENDIX 2

IEG Employee Privacy Notice

Data controller: Inspire Education Group

Data protection officer: DPO@ieg.ac.uk

IEG collects and processes personal data relating its employees to manage the employment relationship. IEG is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does IEG collect?

IEG 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 insurance 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 sabbaticals, 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;
- Details of possible deductions i.e. trade union membership deductions; and
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

IEG collects this information in a variety of ways. For example, data is collected through application forms, CVs; 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 pension benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.



The Group collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks permitted by law.

Data is stored in a range of different places, including in your personnel file, in the group's HR management system and in other IT systems, including the Group's email system.

Why does the organisation process personal data?

IEG needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer pension and entitlements.

In some cases IEG 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. It is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

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

- Run recruitment and selection 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, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- 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;
- Comply with group and company audits;
- Respond to and defend against legal claims; and
- Maintain and promote equality in the workplace.



IEG considers legitimate interests as a reason for processing data; we have considered whether or not those interests are overridden by the rights and freedoms of employees and have concluded that they are not.

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). Information about trade union membership is processed to allow the organisation to operate check-off for union subscriptions, where paid through payroll.

Where IEG 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, payroll, your line manager, managers in the business area in which you work, and IT staff as and when access to the data is necessary for performance of their roles.

IEG shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service.

IEG also shares your data with third parties that process data on its behalf, in connection with the provision of benefits and the provision of occupational health services.

The organisation will not transfer your data to countries outside the European Economic Area.

How does the organisation protect data?

IEG takes the security of your data seriously. The group 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 group 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?

IEG will hold your personal data for the duration of your employment. After your employment ends, the group will continue to hold your personal data on your personnel file (hard and electronic copies) for seven years. At the end of this period, your data will be deleted or destroyed. Any personal data relating to pension membership will be held indefinitely.



Your rights

As a data subject, you have a number of rights.

You can:

- Access and obtain a copy of your data on request;
- Require IEG to change incorrect or incomplete data;
- Require IEG 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 IEG 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, please make the request in writing to the Group Director of IT & Digital Innovation/Data Protection Officer DPO@ieg.ac.uk.

If you believe that the group has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You have some obligations under your employment contract to provide IEG 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 IEG 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 IEG 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. IEG does not use automated processing and decision making.



APPENDIX 3

QRS Staff Privacy Notice

Data controller: Quality Resourcing Solutions (QRS), Drift Road, Stamford, Lincolnshire, PE9 1XA

Data protection officer: Group Director of IT & Digital Innovation, DPO@ieg.ac.uk

QRS is a subsidiary company of Inspire Education Group and an employment business as defined in the Employment Business Regulations 2003 (our business). QRS collects and processes personal data relating its employees to manage the employment relationship. QRS is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does QRS collect?

QRS 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 insurance 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 sabbaticals, 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;
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

QRS collects this information in a variety of ways. For example, data is collected through application forms, CVs; 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 pension benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.



QRS collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks permitted by law.

Data is stored in a range of different places, including in your personnel file, in QRS's HR management system and in other IT systems, including QRS's email system.

Why does the organisation process personal data?

QRS needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your contract and to administer pension and entitlements.

In some cases, QRS 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. It is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

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

- Run recruitment and selection 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, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- 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;
- Comply with company audits;
- Respond to and defend against legal claims; and
- Maintain and promote equality in the workplace.



QRS considers legitimate interests as a reason for processing data; we have considered whether or not those interests are overridden by the rights and freedoms of employees and have concluded that they are not.

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). Information about trade union membership is processed to allow the organisation to operate check-off for union subscriptions, where paid through payroll.

Where QRS 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, payroll, your line manager, managers in the business area in which you work and IT staff as and when access to the data is necessary for performance of their roles.

QRS shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service.

QRS also shares your data with third parties that process data on its behalf, in connection with the provision of benefits and the provision of occupational health services.

The organisation will not transfer your data to countries outside the European Economic Area.

How does the organisation protect data?

QRS takes the security of your data seriously. QRS 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 QRS 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?

QRS will hold your personal data for the duration of your employment. After your employment ends, QRS will continue to hold your personal data on your personnel file (hard and electronic copies) for seven years. At the end of this period, your data will be deleted or destroyed. Any personal data relating to pension membership will be held indefinitely.

Your rights

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

- Access and obtain a copy of your data on request;
- Require QRS to change incorrect or incomplete data;



- Require QRS 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 QRS 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, please make the request in writing to the Group Director of IT & Digital Innovation/Data Protection Officer DPO@ieg.ac.uk.

If you believe that QRS has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You have some obligations under your employment contract to provide QRS 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 QRS 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 QRS 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 on automated decision-making. IEG does not use automated processing and decision making.



APPENDIX 4 Job Applicant Privacy Notice

Data controller: Inspire Education Group
Data protection officer: DPO@ieg.ac.uk

As part of any recruitment process, the group collects and processes personal data relating to job applicants. IEG is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does IEG collect?

IEG group collects a range of information about you.

This includes:

- Your name, address and contact details, including email address and telephone number;
- Details of your qualifications, skills, experience and employment history;
- Information about your current level of remuneration;
- Whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process;
- Information about your entitlement to work in the UK; and
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

IEG collects this information in a variety of ways. For example, data might be contained in application forms, CVs, obtained from your passport or other identity documents, collected through interviews and other forms of assessment.

IEG will also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks. IEG will seek references from third parties before interviews, only if you have given consent on the application form or CV.

Data will be stored in a range of different places, including on your application record, in the HR management system and on other IT systems (including email).

Why does IEG process personal data?

IEG needs to process data to take steps at your request prior to entering into a contract with you. It also needs to process your data to enter into a contract with you.

In some cases, we need to process data to ensure that we are complying with our legal obligations. For example, we are required to check a successful applicant's eligibility to work in the UK before employment starts.

The group has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the organisation to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a



job. The organisation may also need to process data from job applicants to respond to and defend against legal claims.

IEG processes health information if we need to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out our obligations and exercise specific rights in relation to employment.

We process other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief; this is for equal opportunities monitoring purposes.

IEG is obliged to seek information about criminal convictions and offences. We do so because it is necessary for us to carry out our obligations and exercise specific rights in relation to employment.

IEG will not use your data for any purpose other than the recruitment exercise for which you have applied.

Who has access to data?

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, and managers in the business area with a vacancy.

IEG will not share your data with third parties before a job offer has been made, unless you have given consent for us to contact an employment background check provider to obtain a reference. After an offer of appointment, we will then share your data with third parties to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

IEG will not transfer your data outside the European Economic Area.

How does the organisation protect data?

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

For how long does the organisation keep data?

If your application for employment is unsuccessful, the organisation will hold your hard copy data on file for six months after the end of the relevant recruitment process. At the end of that period, or once you withdraw your consent, your hard copy data is deleted or destroyed. Your data will be held on our secure recruitment database unless you make a request for us to remove it.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file (hard and electronic copies) and retained during your employment. The periods for which your data will be held are detailed in our Retention Policy.



Your rights

As a data subject, you have a number of rights.

You can:

- Access and obtain a copy of your data on request;
- Require IEG to change incorrect or incomplete data;
- Require IEG 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, please contact the Data Protection Officer DPO@ieg.ac.uk

You can make a subject access by requesting in writing to the Data Protection Officer.

If you believe that IEG has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to the organisation during the recruitment process. However, if you do not provide the information, the organisation may not be able to process your application properly or at all.

Automated decision-making

Recruitment processes are not based on automated decision-making.