Science Council Employee and Applicant Privacy Notice

The wording in this document reflects the requirements of the General Data Protection Regulation (GDPR), which came into effect in the UK on 25 May 2018.

This notice applies to prospective, current and former employees, workers and contractors.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection.

We may collect, store, and use the following categories of personal information about you:

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). The organisation collects and processes personal data relating to its applicants, employees, workers and contractors 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.
There are “special categories” of more sensitive personal data which require a higher level of protection.

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 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;
- 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, performance improvement plans and related correspondence;

We may also collect, store and use the following "special categories" of more sensitive personal information including:

- 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.
- biometric data, including fingerprints, hand geometry and samples.

How is your personal information collected?

The organisation may collect this information in a variety of ways. For example, data might be 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 benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.
In some cases, the organisation may collect personal data about you from third parties, such as references supplied by former employers and information from employment background check providers.
Data will be stored in a range of different places, including in your personnel file, in the organisation's Payroll and HR management system, and in other IT systems (including the organisation's email system).

Why does the organisation process personal data?

The organisation 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 entitlements [benefit, pension and insurance].
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:-

- where we need to protect your interests (or someone else's interests);
- where it is needed in the public interest (or for official purposes).

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:

- 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, 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;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

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).
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. Data that the organisation uses for these purposes is anonymised. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to enter into a contract with you, perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. We may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Who has access to data?

Your information may 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 and where required by law. The organisation shares your data with third parties in order to obtain pre-employment references from other employers and to obtain employment background checks from third-party providers. 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 and the provision of occupational health services.

Your data will also be shared externally where part of our recruitment activity is outsourced, for example, WorkNest HR who assist us with the administration and management of the recruitment process.

We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our

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

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. This includes:-

- An Internet facing firewall to prevent outside penetration of the organisations network. Policies allow mail to be delivered into the mail server from a specific set of addresses (our external spam filter) but no other access is allowed. This firewall also maintains a list that prevents access to malicious sites on the WWW.
- Spam filtering. All our mail passes through a spam filter which looks for unsolicited mail, malicious software and dangerous links.
- Local firewalling. All our machines are individually protected by firewalls. This prevents problem software proliferating through the network and unauthorised access from one machine to another e.g. only the IT department can remotely connect to a Company laptop.
- Local anti-virus to prevent any malicious software getting through the firewall or spam filters or be brought in by other means. Every machine in the Science Council has anti-virus software installed which is constantly updated via a server on the network. This software also maintains a web blacklist to prevent access to malicious sites.
- File access controls. Access to data on the servers is controlled based on need. Management authority is required before any changes of access are made.
- IT Policy. This policy is to ensure that all information technology users within the organisation or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organisations boundaries of authority.

Where the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions; these parties 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?

If your application for employment is unsuccessful, the Science Council will hold your data on file for 6 months after the end of the relevant recruitment process. If you agree to allow the Science Council to keep your personal data on file, we will hold your data on file for a further 6 months for consideration for future employment opportunities. At the end of that period, or once you withdraw your consent, your data is deleted or destroyed.

The organisation will hold your personal data for the duration of your employment. At the end of employment your data will not be kept longer than necessary for the purpose for which it was processed. For example, personal information of employees, including terms and conditions of employment, disciplinary records, reviews and annual leave records will be kept for 7 years after employment ends. The organisation will keep hold of employees' PAYE, Payroll records for 7 years after employment ends given the relevance to any pay disputes and as HMRC may request to see them in this time.

Your rights

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us. Under certain circumstances, by law you have the right to:

- 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; and
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing.
- request the transfer of your personal information to another party.

If you would like to exercise any of these rights, please contact the CEO.
If you believe that the organisation 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 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.

We will regularly review this Privacy Notice to ensure it remains accurate and up to date.