

About Us | Data Protection Policy

1. Policy Statement

Diamond is committed to protecting the privacy and security of the Personal Data that we process. This policy sets out the way in which Diamond processes Personal Data in order to ensure that we meet the expectations of our stakeholders and our obligations under the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and associated data protection legislation.

2. Who does this policy apply to and how does it apply?

This policy applies to all processing of Personal Data by all persons working for Diamond or on our behalf in any capacity, including Diamond Employees, joint appointees, seconded workers, collaborators, members of our advisory groups/committees, members of our review panels, students, volunteers, interns, agents, contractors (specifically including suppliers and casual and agency staff), external consultants and third-party representatives ("you").

For the avoidance of doubt, this policy only applies to you insofar as you may be working for or on behalf of Diamond.

This policy does not form part of any Diamond Employee's contract of employment and may be subject to change at the discretion of Diamond.

3. Who is responsible for this policy?

Diamond's Data Protection Officer is responsible for overseeing this policy, monitoring internal compliance, advising on Diamond's data protection obligations and acting as a point of contact for individuals and the Information Commissioner's Office (ICO). Please contact the [Data Protection Officer](#) with any questions about the operation of this policy or data protection legislation or if you have any concerns that this policy is not being or has not been followed.

Diamond's Directors have overall responsibility for this policy. Any queries or suggestions relating to this policy should be sent to policies@diamond.ac.uk.

4. Compliance with other policies, regulations and procedures

This policy should be read in conjunction with any privacy notices and records management policies that Diamond may communicate to you.

5. The processing of Personal Data

The processing of Personal Data by or on behalf of Diamond must comply and be in accordance with six principles relating to the processing of Personal Data set out in the GDPR, which require that Personal Data is:

- Processed lawfully, fairly, and in a transparent manner;
- Collected and used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and, where necessary, up-to-date;
- Not kept for longer than is necessary; and

- Kept safe and secure using appropriate technical and organisational measures to protect the data.

Stricter rules apply to the processing of Special Categories of Personal Data (formerly called Sensitive Personal Data). This is information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

6. Lawful Processing

The first data processing principle requires that Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the individual.

You may only collect, process and share Personal Data fairly and lawfully and for specified purposes. This is important in order to ensure that we process Personal Data fairly and without adversely affecting the rights of individuals. The GDPR only allows processing for the following specified lawful purposes:

- **Consent:** The individual has given clear consent for Diamond to process their Personal Data for a specific purpose;
- **Contract:** The processing is necessary for the performance of a contract Diamond has with the individual, or because they have asked Diamond to take specific steps before entering into a contract;
- **Legal obligation:** The processing is necessary for Diamond to comply with the law (not including contractual obligations);
- **Vital interests:** The processing is necessary to protect someone's life;
- **Public Interest:** The processing is necessary for Diamond to perform a task in the public interest or for official functions, and the task has a clear basis in law;
- **Legitimate interests:** the processing is necessary for Diamond's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's Personal Data which overrides those legitimate interests.

Many of the lawful bases for processing Personal Data require that the processing is "necessary". This does not mean that the processing must be essential, but it must be a targeted and proportionate way of achieving the purpose. If other less intrusive means can reasonably achieve the purpose, you should use them instead.

7. Procedure for new processing of Personal Data

Before undertaking any new types of processing of Personal Data, including collecting Personal Data for a new purpose, you must undertake a 'Data Protection Impact Assessment'. These assessments help us to comply with our data protection obligations and meet the privacy expectations of individuals. Please contact Diamond's [Data Protection Officer](#) to assist with this.

8. Further information and guidance

Guidance from Diamond on the processing of Personal Data and the GDPR in general is available [here](#) and Privacy Notices are available [here](#). Additional guidance will be provided as required.

If you still have questions on the processing of Personal Data at Diamond, please contact the [Data Protection Officer](#) or another member of the legal team.

The ICO, which is responsible for enforcing compliance with data protection legislation, has published helpful guidance on data protection on its [website](#).

9. Monitoring

Awareness of this policy forms part of our induction and training process.

10. Breach of this Policy

Breach of this policy may:

- (a) In the case of Diamond Employees, result in disciplinary action up to and including dismissal.
- (b) In the case of individuals who are not Diamond Employees, result in termination of any contract that they may have in place with Diamond and/or termination of their access to Diamond.

11. Amendments to this Policy

Given much of the data protection legislation is new and procedures and practices are developing, this policy will be kept under review and may be revised by Diamond from time-to-time as considered appropriate. It will be the most recently published version of this policy that will apply if any issue arises which needs to be addressed under it.

Definitions

For the purposes of this policy, the following definitions shall apply:

Data Protection Officer: *Diamond's Head of Legal and Corporate Governance.*

Data Subject: *An individual who is the subject of Personal Data.*

Diamond: *Diamond Light Source Ltd, a company incorporated and registered in England and Wales, with company number 4375679 and with registered office at Diamond House, Harwell Science & Innovation Campus, Didcot, Oxfordshire, OX11 0DE, United Kingdom.*

Diamond Employee: *Any person working for Diamond under a contract of employment and any Diamond director or office holder.*

Personal Data: *Any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.*

Process/processing: *Any activity that involves the use of Personal Data, including obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third*

parties.

Sensitive Personal Data: Special Categories of Personal Data.

Special Categories of Personal Data: *Information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.*