Office for Students data protection and privacy policy

The appropriate policy document

Contents

Introduction

The OfS needs to collect and process personal data about people, including staff and individuals with whom it deals with, to operate its daily business, exercise its responsibilities and duties of care as an employer, and to fulfil its statutory functions and duties. In doing so the OfS must comply with Data Protection legislation and give regard to associated guidance and codes of practice. Legislation requires the OfS to protect personal information and to control how it is used in accordance with the legal rights of individuals (data subjects).

The OfS is fully committed to ensuring that personal information is collected and handled fairly, lawfully and in a transparent manner that also respects the rights of individuals. We recognise that being open and transparent with individuals about how we may use their information is a fundamental part of fulfilling that commitment.

As an employer, the OfS undertakes to provide training for staff who handle personal data so that they can act confidently, consistently and in accordance with relevant legislation.

Special category and criminal convictions data

In accordance with the data protection legislation, this is the 'appropriate policy document' for the OfS that sets out how we will protect special category and criminal convictions personal data for:

- performing or exercising obligations or rights, which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection

- reasons of substantial public interest.

It is designed to meet the requirements at:

- paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection, and

- paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018.

Policy scope

Current data protection law and relevant legislation applies to the scope of this policy. It covers all personal data and special category personal data collected and processed by the OfS in the conduct of its daily business, statutory functions and duties.

It does not apply to other information that does not contain personal data which is required to be kept confidential including, for example, information which is commercially sensitive or policy in development.

The policy is applicable to all OfS staff, contractors, and agency staff (hereafter referred to as 'staff') using OfS systems.

It also applies to OfS staff, contractors and agency staff, who may access OfS systems and information through non-OfS systems.

The OfS is registered with the Information Commissioner's Office. The OfS's entry on the Data Protection Register can be found on the ICO website by quoting Registration Number: ZA309955.

Policy objectives

The objectives of this policy are to ensure that:

- proper procedures are in place for the collection, processing and management of personal data, including special category and criminal convictions data
- responsibilities for compliance with data protection requirements are clearly set out
- all staff understand how to identify personal data and their responsibilities when handling such data
- individuals are assured that their personal data is processed in accordance with data protection legislation, including that their data is kept securely and safe from unauthorised access, alteration, misuse or loss
- other organisations with whom the OfS shares personal data meet compliance requirements
- any new systems being implemented that will hold personal data are assessed as to whether the system presents any risks, damage or impact to individuals and that appropriate mitigating action is taken in compliance with this policy.

Policy principles

The OfS will apply the data protection principles set out in data protection legislation to the collection, processing and disposal of all personal data by:

- Processing personal data **fairly, lawfully and in a transparent manner**. We will do this by only processing personal data where there is a legal basis to do so, not using personal data in a way which the individual could not reasonably expect and by providing fair processing or privacy notices to individuals. When processing personal data as a data processor, we will comply with instructions given to us by the data controller, including the terms of our contract with the data controller.

- Processing personal data for **specified, explicit and legitimate purposes**. We will do this by ensuring that personal data is not used for purposes incompatible with those purposes for which it was collected. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes. We will ensure that individuals are informed about the purposes of processing personal data through the use of privacy notices.

- Ensuring that personal data is **adequate, relevant and limited to what is necessary**. We will only process personal data to the extent that it is required for the specific purpose notified to the data subject.

- Ensuring that personal data is **accurate and where necessary up-to-date**. We will do this by having in place measures to check the accuracy of personal data as required and by providing data subjects with information about how to request rectification or erasure of their personal data. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data where required by law to do so.

- **Retaining personal data only as long as required**. We will do this by applying retention policies and secure destruction methods. Data will only be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected. Personal data may be stored for longer periods when it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

- **Protecting personal data, including against unauthorised or unlawful processing and against accidental, loss, destruction or damage**. We will do this by applying appropriate access controls on a ‘need to know’ basis, requiring all staff to complete personal data training supplemented as appropriate by procedures and guidance relevant to their role, and by having a framework of information security policies, procedures and technical controls in place.

- Applying **'privacy by design and default'** principles when developing and managing information systems or software to process personal data. We will do this by using data protection impact assessments to identify and mitigate risks at an early stage in project and process design, by minimising the amount of personal data collected and by anonymising data wherever possible.

- Seeking **informed consent when it is appropriate to do so** and being clear with individuals when consent is not required. We will do this by explaining what personal data processing is voluntary and the consequences of not providing it and what personal data is mandatory and why we are entitled or obliged to process personal data.

- **Upholding individuals' rights as data subjects**. We will do this by providing a means for individuals to make requests for access, to object to or restrict processing, rectification, erasure, data portability and by responding to such requests promptly and within the legal deadlines.

Lawful basis for processing personal information

Under data protection legislation, we require a lawful basis to be able to process personal information.

When we carry out processing personal information in pursuit the exercise of our functions, including but not limited to those as set out in the Higher Education and Research Act 2017, in the most part, the lawful basis for processing personal information upon which we rely falls within Article 6(1)(e) of the General Data Protection Regulation (GDPR):

"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

In addition, where we process special category data, such as health, religious or ethnic information, the lawful basis we rely on to process it is article 9(2)(g) of the GDPR:

"processing is necessary for reasons of substantial public interest".

The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018.

Where we process special category personal data for research or statistical purposes in the public interest, we rely on the lawful basis under Article 9 (2)(j) in accordance with Article 89(1) of the GDPR, and Schedule 1 part 1(4) of the DPA 2018.

We may also, depending upon context, make use of use another legal basis such as legal obligation, contractual, legitimate interests and consent-based processing; details of which are set out in specific privacy notices.

Accountability

Data protection legislation requires that data controllers shall be responsible for and be able to demonstrate compliance with the data protection principles.

We will:

- maintain records of personal data processing activities, and provide these to the Information Commissioner's Office on request
- carry out a Data Protection Impact Assessment (DPIA) for any high risk personal data processing, and consult the Information Commissioner if appropriate
- appoint a Data Protection Officer to provide independent advice and monitoring of the OfS's personal data handling, and ensure that this person has access to report to the highest management level of the department
- have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law.

The OfS Risk Management Policy includes processes for the identification and escalation of risks associated with data protection and information governance. The risk management approach outlined in the policy will help ensure data protection and privacy risks are escalated appropriately and in a timely manner within the governance and management of the OfS.

As part of the OfS's internal audit programme, the internal auditors will carry out periodic audits in relation to privacy and data protection compliance.

Data Privacy Group

The Data Privacy Group (DPG) will take a strategic, risk-based organisation-wide view of all matters affecting compliance with data protection legislation, escalating any matters of concern and will monitor, support and promote compliance with data protection legislation and best practice.

The DPG has responsibility for providing advice to standing members to assist them in carrying out their duties, particularly in relation to the identification of risks, mitigation and practicalities.

The Group will monitor new and on-going data protection risks and ensure that a risk register is maintained reporting this as required.

Implementation

This policy is implemented through the development, application, monitoring and review of the component parts of the OfS's governance and information management systems and processes, including:

- Information Asset Owners / Information Asset Managers to undertake information risk assessments to identify and protect confidential and business critical information assets.
- Co-ordination of effort between relevant teams and professional specialists to integrate IT, physical security, people, information management, risk management and business continuity to deliver effective and proportional controls.
- Generic and role specific training and awareness.
- Embedding information management and data protection compliance requirements into procurement and project planning.
- Monitoring compliance and reviewing controls to meet business needs.

Security

The OfS's approach to information security is set out in its Information and IT policies, procedures and standards which apply to all the information and IT systems or services for which the Board and management, staff, contractors and agency staff are responsible by certification, contract, and applicable laws.

Data sharing

Personal data will not be shared with a third-party organisation without a valid lawful basis or without the data subject's consent. The OfS undertakes due diligence checks to ensure that third parties processing personal data on its behalf do so in a way that is compliant with data protection legislation and individuals' rights. The sharing of personal information with third parties will be governed by contract or written agreement.

Personal data will not be transferred to countries or territories outside the European Economic Area unless that country or territory can ensure a suitable level of protection for the rights and freedoms of the data subjects in relation to the processing of personal data.

Transparency

Data protection legislation requires that clear and transparent information is provided to individuals about the use(s) that will be made of their personal information. The

OfS recognises that transparency is key to individuals being able to exercise their rights under data protection legislation, including the right of access.

To fulfil this obligation, the OfS will employ a layered approach to privacy notices, where a short form overview is provided at the point at which personal data is collected, with a link then provided to a full detailed privacy notice. We will make available on our website an overarching privacy notice encompassing a broad range of our work.

Data subject access requests and individual rights

All data subjects have a number of individual rights in relation to their personal data. The OfS will provide guidance to data subjects on how to request access to their personal data and how to exercise other individual rights. This guidance will be communicated through the OfS website as well as within privacy notices.

Consent

As a public body and an employer, the OfS recognises that it will need to take extra care to show that consent is freely given and will only use consent where the use of personal data is not a pre-condition of a service in circumstances where there is a genuine choice. Where consent is the lawful basis for processing personal data the OfS will ensure that individuals are offered a real choice and control over the use of their information by:

- using positive opt-in alongside a clear and specific statement of consent
- separating consent from other terms and conditions
- being specific and granular
- being clear and concise
- naming any third parties who will rely on consent
- providing an easy means to withdraw consent
- retaining evidence of consent
- keeping consent under review.

Retention and erasure of special category or criminal convictions data

The OfS will ensure, where special category or criminal convictions personal data is processed, that:

- there is a record of that processing, and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data

- where we no longer require special category or criminal convictions personal data for the purpose for which it was collected, we will delete it or render it permanently anonymous

- data subjects receive full privacy information about how their data will be handled, and that this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

Staff training

All staff will be required to undertake baseline data protection and information security training as part of their induction and annually thereafter. Staff that handle large volumes of data or special category data will be given additional training so that they understand the responsibilities associated with enhanced access to personal data.

Policy communication and review

This policy will be made available to all staff through publication on the OfS intranet and communicated externally by publishing it on the OfS website.

It will be reviewed in November 2019.