SAAS Student Awards Agency Scotland

Funding your future

Data Protection Policy

Protect the Student, Protect SAAS, Protect Yourself

Last updated: May 2018
Next review: November 2018

Contents

1. Introduction

The General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (the Act) regulates the way in which personal data is held and processed. This policy explains the scope of the Act, the principles of data protection and the approach adopted by Student Awards Agency Scotland (SAAS) to comply with the legal obligations and requirements under the Act.

During the course of our activities SAAS will collect, store and process personal information about our customers, staff, suppliers and other living individuals. SAAS recognises the need to treat this information in an appropriate and lawful manner.

The information SAAS holds, which may be held on paper, on a computer or other media, is subject to certain legal safe guards specified in the Act and other regulations[1]. GDPR and the Act also imposes restrictions on how SAAS may use that information. It is essential that all SAAS employees, contractors, part time and fixed term workers and Agency staff adhere to these requirements.

2. Scope of the policy

This policy applies to all employees working for SAAS including all full-time and part-time permanent members of staff, consultants, contractors and fixed term workers and Agency staff.

3. Status of the policy

This Policy has been approved by the SAAS Executive Team. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling processes, storage, transportation, retention and destruction of personal information.

This Policy should be read in conjunction with our Privacy Statement[2] which gives further guidance on how SAAS processes information.

[1] **https://www.gov.uk/data-protection/the-data-protection-act**

[2] **http://www.saas.gov.uk/privacy_data_protection_index.htm**

4. Definition of data protection terms

Data is personal information which is stored in any format (paper, electronic, phone recordings) in any filing system, whether centralised, decentralised or dispersed on a functional or geographic basis.

Data subject for the purpose of this policy includes all living individuals about whom we hold personal information. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal information means any information relating to an identified or identifiable person. Identifiable person is one who can be identified, directly or indirectly, in particular to an identifier such as a name, an identifiable reference number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. who can be directly or indirectly identified in particular by reference to an identifier. The personal information does not have to be held by SAAS.

Data users include employees/contractors whose work involves using personal information. Data users have a duty to protect the information that they handle by following our data protection and security policies at all times

A **Data controller** determines the purpose for which and the manner in which any personal information is processed. He/she has a responsibility to establish practices and policies in line with the Act.

A **Data processor** is responsible for processing personal data on behalf of a controller.

Processing is any activity that involves the use of information, whether or not by automated means. It includes obtaining, recording or holding information or carrying out any operation or set of operations on the information including organising, amending, retrieving, using, disclosing, erasing, or destroying it.

Special categories of personal data formerly referred to as ‘sensitive personal data’ under the Data Protection Act 1998. Information about a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation genetic data and biometric data where processed to uniquely identify a person.

5. Compliance under the data protection principles

Article 5 of the GDPR requires compliance with the following principles.

5.1. Lawfulness, Fairness and Transpanacy

Data will be processed fairly and lawfully and in a transparent manner in relation to the data subject

Data subjects will be told why SAAS needs any personal information that is collected about them and inform data subjects of the ways in which information will be used.

SAAS will do this by the use of a Privacy Statement (see section 3) to inform data subjects why SAS collects information, what information is collected, what SAAS does with that information, who it will be shared with, how it will be held securely and how data subjects may access it and how the data subject can make a complaint in the event that they believe SAAS isn't processing data correctly.

Data subjects will be informed if any automated decision making will take place. This is specified in our Privacy Statement.

5.2. Purpose Limitation

Data will be collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes

Personal information will not be re-used for any purpose that is incompatible with the original purpose for which it was collected. For example SAAS collects personal information to assess a student's eligibility for funding; this information will not then be used to identify students in any direct marketing for private sector student accommodation.

If SAAS considers using personal information for a new purpose, a Data Protection Impact Assessment will be undertaken. If the data can be used for a new purpose the SAAS Privacy Statement will be updated and consideration will be given to other means of informing data subjects.

5.3. Data Minimisation

Data must be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed

Enough personal information must be obtained to allow SAAS to fulfil its purpose(s) for collecting it, including assessing eligibility for student support.

Additional personal information will not be collected if it is on the basis that it might possibly be useful for an unspecified purpose in the future.

Where specific information is obtained from a group of individuals for a particular purpose, SAAS should only ask for that information from that particular group. For example, SAAS collects disability information from students who apply for Disabled Students Allowance (DSA), this information should only be collected if students have applied for DSA support.

5.4. Accuracy

Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay, taking into account the purpose for why it is being processed.

SAAS must ensure reasonable steps will be taken to keep personal information up to date and accurate. This may periodically include asking data subjects to confirm their personal details when they contact SAAS by phone or email.

SAAS must endeavour to promptly correct any inaccuracies identified. This includes where SAAS identifies inaccuracies through application checks and system developments.

If a data subject informs SAAS that their personal information is incorrect, steps will be taken to investigate this and correct the data. SAAS has a specific process for handling requests under right to rectification and right to erasure. This information can be found in the SAAS Guide to Individual Rights.

5.5. Retention

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

SAAS is required to retain personal information for business, regulatory and legal reasons. To ensure fair processing, personal data will not be retained by SAAS for longer than necessary

SAAS must ensure erasure and destruction of data is in line with SAAS' Retention policies[3] and procedures.

SAAS will review the retention of personal data at least annually to ensure we do not keep data for longer than necessary.

[3] http://www.saas.gov.uk/about_us/classes_of_information.htm

SAAS will implement privacy by design where possible, into all new processing systems.

5.6. Security, Integrity and Confidentiality

Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

SAAS is responsible for ensuring appropriate technical and organisational policies and procedures are in place so that personal data is held securely.

Staff will ensure they comply with all policies and procedures in relation to security.

Staff will ensure that all personal information is securely stored whether in electronic, digital or in hard copy format.

Staff will ensure that personal information is transferred to others in a secure manner, whether in paper, digital or electronic format and with appropriate markings in line with the Government Security Classification Policy[4]. Staff will also ensure that only Scottish Government issued encrypted devices are used to access third party platforms that hold personal information.

Staff and/or contractors will only have access to personal information as required in relation to the purpose for which it was obtained and in relation to the functions that they are performing. Line Managers must ensure staff and/or contractors are made aware of their responsibilities under this policy.

Any new projects or changes to processes which involves personal information will be assessed for any security and privacy risks and a Data Protection Impact Assessment must be undertaken.

All staff will securely destroy any paper documents that contain confidential or personal information. SAAS operates a ‘white bag’ system where physical confidential waste is shredded and removed from office areas and confidentially destroyed by a third party contractor.

Data Processors

Where SAAS uses a contractor to process personal information on its behalf, the contractor must sign a data processing agreement which ensures that they are taking adequate steps to comply with their responsibilities under GDPR and the Act as a processor on SAAS’ behalf. Processors are legally responsible to ensure

[4] **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf**

compliance under GDPR and the Act. Those managing contracts must ensure that all processor obligations are specified in the contract, and it is subsequently monitored to ensure that they are in place. Further advice can be obtained via the SAAS Information Manager.

Data Sharing

Personal information may be shared with partner organisations where this is required in relation to the purpose for which it was obtained. For example SAAS share student information with the Student Loans Company where students have applied for and been given a loan so that loan payments can be administered and paid. Any sharing of information must be done in a way that complies with the law, is fair, transparent and in line with the rights and expectations of the people whose data is being shared. Any data sharing should follow the Information Commissioner's Code of Practice[5]. If any data sharing requests from third parties are received the SAAS Information Manager should be contacted for further information and guidance on how to handle data sharing requests..

Disclosure of personal information

SAAS may receive requests for the disclosure of personal data, without the consent of the data subject, to certain organisations. Requests for such disclosures from third parties, such as the Police, Home Office, UK Border Agency, local authorities must be made in writing. The request should include:

- What information is needed;
- Why is it needed; and,
- How the investigation will be prejudiced without it.

The validity of all requests for disclosure of personal data without consent from the data subject must be checked. The identity of those requesting data and their legal right to request or demand information must be validated. The reason for the disclosure made without consent must be documented. This work is undertaken by the Counter Fraud Team overseen by the Head of Counter Fraud.

The main reasons why SAAS might disclose personal information without the data subject's consent is where this information is required in relation to the prevention, detection, investigation and reporting of crime; or where disclosure is required by law or for legal proceedings. The exemptions provided under the Act allow the disclosure of personal information without the data subject's consent. This is not a blanket exemption and every request for information must be assessed on a case by case basis. If a request is complex and involves other legislation other than just data

[5] **https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/**

protection legislation then legal advice will be sought by SAAS from Scottish Government Legal Directorate, in discussion with the SAAS Information Manager.

Data breach reporting

SAAS has Personal Data Breach Response Plan in place which sets out actions to be taken by staff in the event of a data breach. If a member of staff becomes aware of an actual or potential breach in relation to personal information, they must report it immediately and inform their line manager. They should complete a data breach reporting form which will automatically be send to the Information Management mailbox on submitting of the form.

6. Rights of the individual

The GDPR and The Data Protection Act, 2018 expands the existing rights of data subjects. These rights are:

- Right to be Informed
- Right of access;
- Right to rectification;
- Right to erasure;
- Right to restrict processing;
- Right to data portability
- Right to object; and
- Rights in relation to automated decision making and profiling.

SAAS will ensure that processes, policies and practices are designed to accommodate individuals' option to exercise their rights.

SAAS will ensure that there is someone with specific responsibility for data protection in the organisation. The nominated person is currently the Information Manager.

The Information Manger may be contacted at:

Student Awards Agency Scotland
Saughton House
Broomhouse Drive
Edinburgh
EH11 3UT

Email: **SAASDataProtection@gov.scot**

Requests under these rights must be made in writing by the data subject. The identity of the data subject must be established by SAAS before responding to any request.

SAAS must respond to all written requests within 30 days of a valid request, this can be extended to up to three months where requests are complex.

If SAAS do not comply with a request, SAAS will provide an explanation why no action is being taken. A data subject will also be provided with information about how to complain to the Information Commissioners Office and the right to apply to the Court of Session.

More detailed information about each right and what SAAS needs to take into consideration when making a decision to comply or not comply with a request can be found in the Guidance on Individual Rights.[6] The majority of this guidance has been incorporated from the Information Commissioners website.

7. Management and responsibilities

The Chief Executive, as Accountable Officer (AO), has overall responsibility for data protection within Student Awards Agency Scotland.

The Executive Team is responsible for ensuring appropriate co-ordination and oversight is in place to ensure that SAAS remains compliant with the Act. The Team approves Data Protection policies and procedures.

The Director of Corporate Services is designated as SAAS' Senior Information Risk Owner (SIRO). The SIRO's responsibilities are to lead a culture of good information management, own the overall information risk policy and procedures and advise the Accountable Officer on information risk.

The Data Protection Officer (DPO) has overall responsibility for monitoring SAAS' compliance with the data protection laws, and is the named contact point for any data protection compliance issues a data subject may have. The DPO has the authority to report to the ICO directly without discrimination in the event that serious breach breaches are not reported directly by the organisation.

The Information Management Team is responsible for ensuring data protection policy and guidance are kept up to date. They are responsible for co-ordinating responses to data protection enquiries and data subject rights. To support all SAAS staff to comply with their obligations under the Act and to issue training and guidance.

All managers are responsible for ensuring this policy is communicated and implemented within their area of responsibility, including ensuring all staff receives data protection training provided by SAAS and requests for any specific training in their areas are considered.

[6] http://www.saas.gov.uk/privacy_data_protection_index.htm

Managers are responsible for ensuring that the appropriate access to personal information is given to staff in line with their duties, and that all staff are aware of their degree of access to personal information that is authorised for the purpose of their role. They are also responsible for reporting any potential or actual data protection breaches.

All staff are responsible for adhering to the principles set out in this policy. All staff are responsible for ensuring they understand what degree of access to personal information they are authorised to have for the actual purpose of their job roles.

8. Relationship to other SAAS policies

- Information Security Policy
- Subject Access Request Guidance
- Personal Data Breach Response Plan
- Guidance on Individual Rights
- Privacy Statement
- Corporate Retention Schedule
- Call Recording Policy

9. Compliance

Deliberate or reckless breaches of this policy may lead to disciplinary action, in line with Scottish Government's Civil Service Code and associated disciplinary procedures. All staff must familiarise themselves with the content of this policy.

All staff should be aware that it is a criminal offence to deliberately or recklessly disclose personal information without the authority of the SAAS.

Data subjects have a right to apply to the courts for unlimited compensation for any damage suffered through SAAS' failure to comply with the Act. Where damage is suffered, they can claim for resulting distress.

The ICO can also impose a monetary fine on SAAS up to a maximum of £17 million in addition to compensation awarded by the courts.

10. Complaints procedure

SAAS aims to fully comply with its obligations under the Act. If an individual has any questions or concerns regarding SAAS' management of personal data, they should be directed to Data Protection Officer.

Data Protection Officer
Student Awards Agency Scotland
Saughton House
Broomhouse Drive
Edinburgh
EH11 3UT

Email: **SAASDataProtection@gov.scot**

If an data subject is still dissatisfied, they have the right to contact the Information Commissioner's Office, the independent body overseeing compliance with the Act and should be directed to the ICO website[7].

Data subjects have the right in certain circumstances to seek a judgement through the courts where they are not satisfied with a decision made by SAAS. Data subjects can seek a judgement via the Court of Session.

11. Monitoring and review of this policy

The policy will be reviewed on an annual basis. However, we will continue to review the effectiveness of this Policy throughout 2018 as guidance for GDPR is published and to ensure that it is achieving its stated objective.

SAAS aims to develop Data Protection guidance to support this Policy.

If you have any concerns, questions or areas of improvement about this policy please contact the Information Manager.

[7] **http://ico.org.uk**