SAAS | Student Awards Agency Scotland

Funding your future

Counter Fraud Policy and Response Plan

2020-23

✓ Informing Choices
✓ Funding Futures
✓ Supporting Success

www.saas.gov.uk

Contents

Introduction

SAAS is an Executive Agency of the Scottish Government (SG) and follows the guidance on fraud, outlined in the Scottish Public Finance Manual (SPFM).

This policy outlines SAAS' zero tolerance approach and resolve to prevent, detect and respond to fraudulent activity. The aim of this policy is to support SAAS' high standards, procedures and controls, in order to minimise the opportunity for fraud to occur and to assist in the early detection of fraud. It also emphasises the responsibilities of all managers and staff in relation to the identification and reporting of fraud.

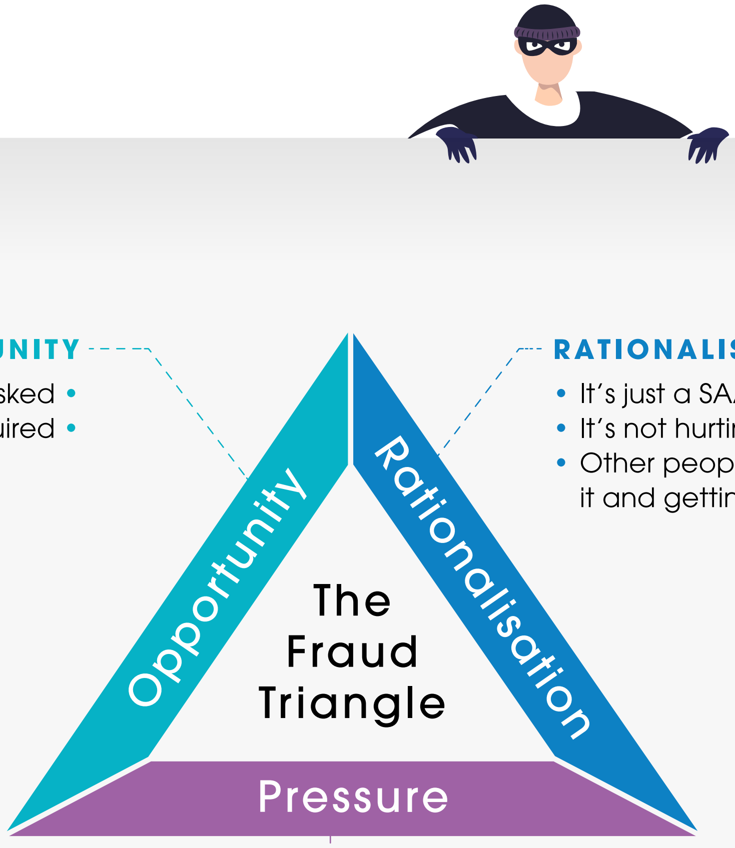
Reported or suspected frauds will be handled in accordance with our Counter Fraud Response Plan. The purpose of the Fraud Response Plan is to provide a framework to manage any allegation of fraud, bribery or corruption. It will act as a procedural guide to enable SAAS to take timely and effective action, whilst maintaining the integrity of the organisation and to manage any further risk.

Adhering to these procedures will ensure there is a clear understanding of roles and responsibilities. It will also ensure that investigations or any incidents are managed appropriately any evidence gathered is protected.

Fraud Triangle

The Fraud Triangle identifies three components that are present where fraud exists: Pressure, Opportunity and Rationalisation.

Breaking this fraud triangle is the key to fraud deterrence and an organisation must remove one of the elements to reduce the likelihood of fraudulent activity.



OPPORTUNITY

- No questions asked
- No evidence required

RATIONALISATION

- It's just a SAAS form
- It's not hurting anyone
- Other people are doing it and getting away with it

PRESSURE

- Student experiencing hardship
- Other issues such as gambling
- Pressure from someone else

Types of people who commit fraud

Naïve

Those who provide misleading or incorrect information and ultimately gain funding fraudulently but are unaware that they have committed fraud.

Opportunist

Those who see an opportunity to gain “**free**” money by deliberately providing false information.

Organised

Those who identify and exploit weaknesses to commit fraud. Monies gained may be used to fund further criminal activity.

Types of fraud

Fraud is the use of deception with the intention of obtaining personal gain, avoiding an obligation or causing loss to another party.

Fraud can be used to describe a wide variety of dishonest behaviour such as forgery, fraud by omission, false representation and the concealment of material facts.

The Counter Fraud Team (CFT) comprise of specialist staff who are Accredited Counter Fraud Specialists (ACFS) and are responsible for all allegations of external fraud investigations, to ensure that all investigations conform to the same standard and are undertaken in accordance with legislation.

External fraud

External fraud against SAAS has been committed by individuals obtaining student funding they are not eligible to receive.

For example:

- Falsifying personal information to obtain student funding when ineligible;
- Falsifying information to increase the level of student funding;
- Creating false identities to obtain student funding;
- Obtaining student funding but not attending a course of study.

The CFT are professionally trained in conducting interviewing of vulnerable witness or suspects under caution and managing criminal investigations.

As a Specialist Reporting Agency we have a duty to investigate any allegation of fraud and where there is evidence that a crime has been committed, report this directly to the Crown Office and Procurator Fiscal Service (COPFS) in line with advice of COPFS liaison. All investigations will be conducted in accordance with the CFT investigations procedures and the relevant legislation that we are governed by.

Types of fraud

Continued

Internal fraud

Occasionally internal fraud has been committed by staff members who have breached the trust placed in them, by using their knowledge of our systems to commit fraud.

For example:

- Re-directing of public funds to personal bank accounts;
- Abnormal travel or subsistence claims;
- Pressure from colleagues to avoid following procedures;
- Inappropriate relationships with suppliers.

A criminal act of this nature can be viewed by COPFS as embezzlement which is a more serious offence. SAAS is committed to promoting clear ethical standards and the Counter Fraud Policy communicates our approach to bribery and corruption. In the event that an internal fraud occurs, the Response Plan ensures that thorough investigations are conducted with the support of relevant areas of expertise.

Bribery and corruption

SAAS staff are governed by the Civil Service Code. This requires all staff to act honestly, with integrity at all times and to safeguard the public funds for which they are responsible.

We aim to positively influence the behaviours of individuals and promote clear ethical standards through our Counter Fraud Policy, the Civil Service Code and the Propriety Standards of Conduct. We promote integrity and increase awareness of fraud reporting and whistleblowing arrangements.

The SG will not accept any level of fraud or corruption; consequently, all cases are thoroughly investigated and dealt with appropriately. All employees should be aware that they are entrusted with and have responsibility for any information that they handle.

There are rules for accepting gifts or hospitality which can be found in the Procurement Policy Manual (for staff involved in purchasing and contracting) and, in more detail, in the Staff Handbook (Standards of conduct) available to all SG staff on the SG intranet, Saltire.

The CFT will manage all investigations relating to an internal fraud but in some instances it may be deemed appropriate for supplementary investigations or lines of enquiry to be carried out by other departments, depending on the type of fraud and the complexity of the cases, for example, HR.

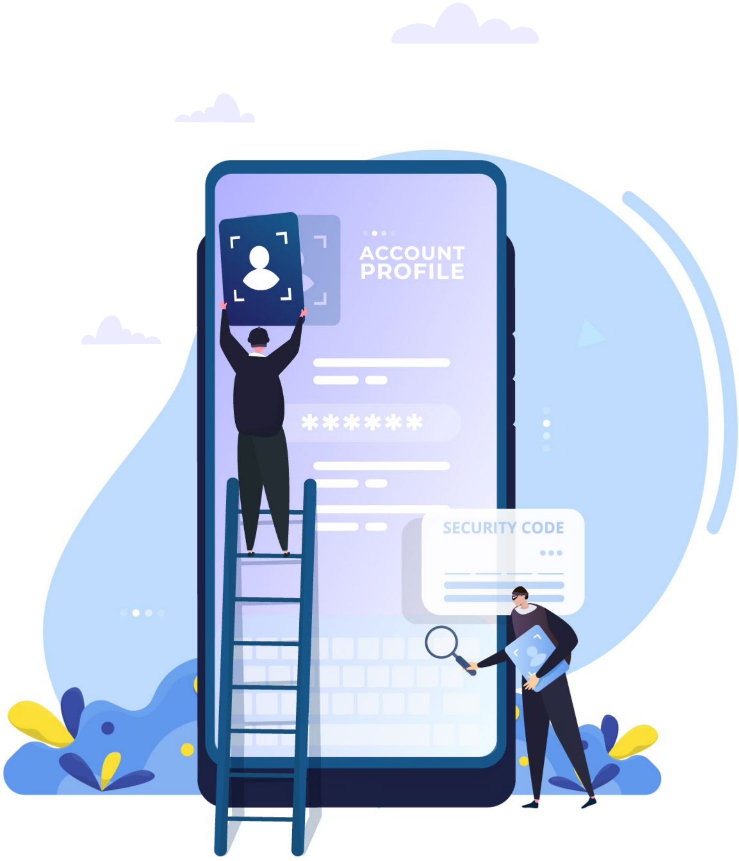
Governance

The SAAS Fraud Response Plan has been developed to ensure the Agency's responsibilities are in line with the requirements placed on SAAS by the Scottish Public Finance Manual.

The requirements are as follows:

- Organisations should draw up fraud response plans to ensure that timely and effective action is taken in the event of a fraud;
- Organisations are responsible for undertaking thorough investigations where there is suspected fraud and for taking the appropriate legal and/or disciplinary action in all cases where that would be justified;
- Fraud investigation is a specialised area of expertise, and organisations should ensure that those tasked with any investigation have received appropriate training, including that relating to the gathering of evidence. Investigations should consider any control failures and make recommendations on systems and procedures to minimise the risk of a recurrence;
- An Agency may establish its own arrangements, consistent with the SG Fraud Response Plan, covering both external and internal fraud;
- Business areas within the core SG that have significant grant-giving or contract-letting responsibilities should also establish additional local arrangements for dealing with external fraud.

This Policy and Response Plan also aligns to the Cabinet Office Counter Fraud Standards and Profession and the Counter Fraud Policy details the responsibilities of the Accountable Officer and the whole Agency in the event of a fraud.



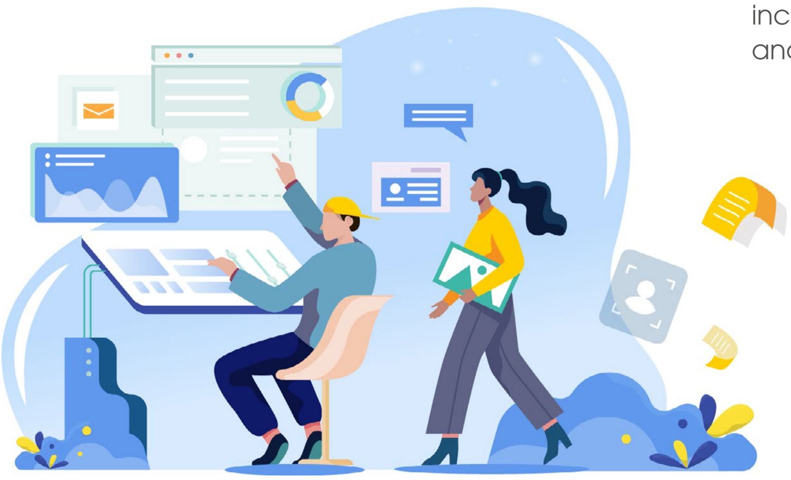
Data sharing

SAAS is committed to data sharing across the UK as a means of recognising and reducing fraud.

We participate in the National Fraud Initiative (NFI) data matching exercise to assist in the prevention and detection of fraud.

Data is gathered and matched across public bodies in the UK to identify potential fraud. In addition, the exercise can also be used to assess the arrangements that NFI participants have in place to deal with fraud. Section 26A of the Public Finance and Accountability (Scotland) Act 2000 provides that Audit Scotland may carry out data matching exercises or arrange for them to be carried out on its behalf.

The NFI exercise does not require the consent of individuals under the Data Protection Act 1998, but is subject to a Code of Data Matching Practice and the relevant provisions of the Data Protection Act 1998 are included in Appendix 3 of this code.



SAAS is a member of Cifas, which is a not-for-profit fraud prevention membership organisation. They are the UK's leading fraud prevention service, managing the largest database of instances of fraudulent conduct in the country. Their 400+ members are organisations from all sectors, sharing their data across those sectors to reduce instances of fraud and financial crime. If SAAS detect a fraud, it is our responsibility to upload this data onto the database as part of our Sanctions process. However, we will only upload if we have a good range of evidence that we would be willing to submit to court.

The SAAS Counter Fraud Team also partake in cross government data sharing exercises involving The Cabinet Office and HMRC. The purpose of the data matching exercise is to test for fraud and error in student applications where funding is based on household composition and income allows us to verify a student's eligibility for funding and to confirm that students have been awarded the correct amount of funding for the session.

We also share information with the Student Loans Company (SLC), local authorities, Nursing and Midwifery Council (NMC), Home Office and Police Scotland.

Privacy statements are issued to all students and benefactors that cover all SAAS functions, including SAAS Counter Fraud Team investigative and data matching exercises.

Fraud Risk Management

A regular assessment, management and review of the risk landscape will allow us to evaluate the effectiveness of the controls in place and the identification of emerging risks. This will inform our Risk Register which is reviewed regularly.

Where fraud risks have been identified we will ensure appropriate controls are in place.

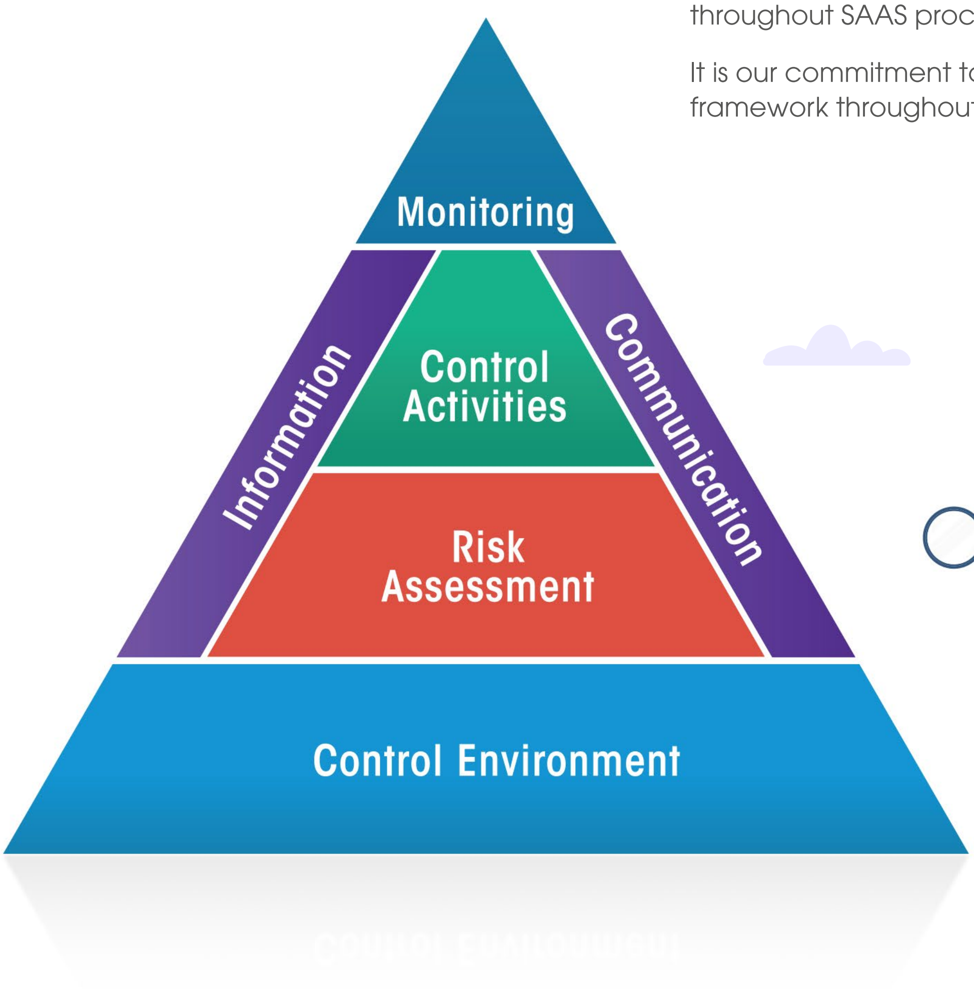
For example:

- Supervisory e.g. checking
- Authorisation e.g. authority levels
- Accounting e.g. budget reconciliation
- Segregation of duties e.g. goods ordering/ receipt

A Fraud Impact Assessment process is in place for every change that we make in SAAS to ensure early identification of fraud risk and possible mitigation.

To enhance this we aim to introduce a Fraud Risk Assessment framework to assess, analyse and report on existing and future fraud risks throughout SAAS processes.

It is our commitment to develop this process and framework throughout the next three years.



Strategic Objectives

Our objectives closely align to main SG and underpin the activities undertaken by the Counter Fraud Team. There is a focus on improving fraud prevention and early detection as well as learning from known frauds.

Our five objectives are Deter and Educate, Prevent and Detect, Investigate and Enforce, Review and Learn and Monitor and Measure.

⚠ Deter and Educate

Creating an anti-fraud culture

Through the use of a wide range of communication tools, we will use our Communications Plan to ensure that we increase fraud awareness both internally among staff and externally among our customers and partner organisations, to deter fraud and raise the profile of counter fraud work.

Students are educated and informed about the actions we take and the long-term consequences of committing fraud. We work with external partners on fraud awareness campaigns to alert our customers to fraud issues to protect them from falling victim to fraud. By working closely with colleges and universities, we aim to prevent fraud by sharing knowledge of best practice and updating our colleagues of any fraud trends.

Success for the Counter Fraud Team in this objective will see regular communication throughout the year both internally and externally and yearly recruitment of new Fraud Champions to expand the fraud culture within SAAS.

Strategic Objectives

Continued

Prevent and Detect

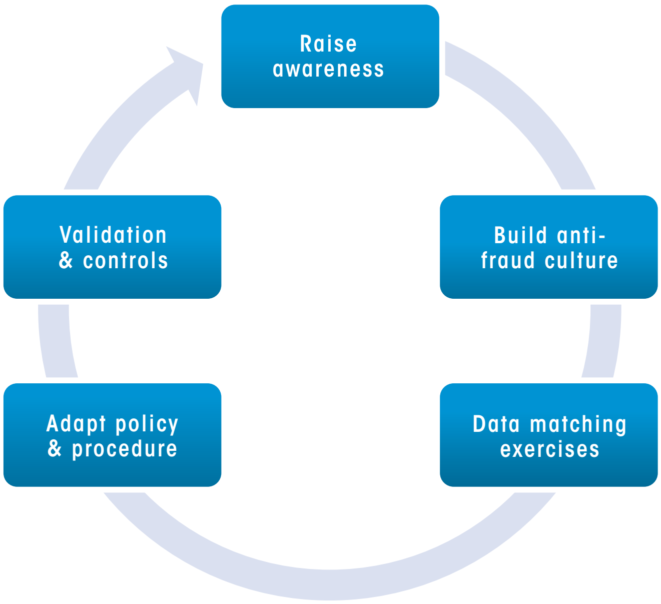
Fraud risk management

A fraud change impact assessment is used to support Agency change processes to ensure fraud risk is considered at every opportunity. Having fraud representation on boards and committees and having a comprehensive fraud risk management programme establishes clear ownership and accountability from the top down, ensuring the continuous monitoring of controls.

Training and awareness

We deliver regular training to all staff to help them to detect fraud at the earliest opportunity. Our training aims to inform staff about the common types of fraud that are attempted against SAAS and highlights that all staff members have an active role to play in the prevention and detection of fraud. Counter fraud awareness is introduced through the SAAS induction programme and is strengthened through a package of continuous learning and development.

In addition, each operational area has a 'Counter Fraud Champion' who is upskilled to build fraud capability. The champion acts as a connection between the CFT and operational areas, to share best practice for preventing and detecting fraud and as a point of contact for those who have a suspicion or concern about fraudulent activity.



Raise awareness

Build anti-fraud culture

Data matching exercises

Adapt policy & procedure

Validation & controls

Data analytics

We conduct internal analysis of data to look for and build fraud indicators. Interrogation and data mining, combined with targeted random sampling enables us to test areas of fraud risk through random sampling exercises.

Success for the Counter Fraud Team in this objective will see increase the use of digital tools and solutions to help us to prevent and detect fraud at the earliest opportunity. At the same time, we will continue to improve relationships with partners to increase data sharing and to expand our participation in data matching exercises, such as the National Fraud Initiative (NFI), Cifas and other Pilot initiatives. By working collaboratively across government, we share knowledge and data with our partner organisations who include universities & colleges, Universities and Colleges Admissions Service (UCAS), Student Loans Company (SLC), Department for Work and Pensions (DWP), National Health Service (NHS), the Home Office, Police Scotland and local authorities, which is instrumental to our success.

Strategic Objectives

Continued

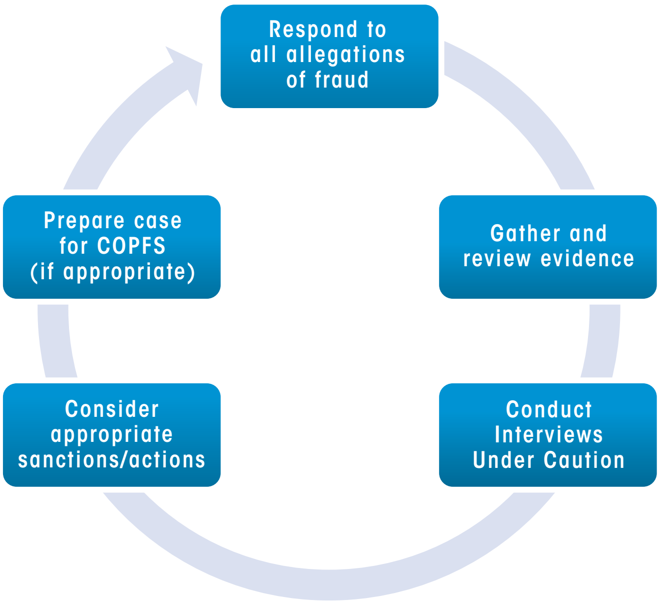
Investigate and Enforce

Fraud reporting

We have a number of reporting mechanisms in place for staff, partner organisations and members of the public to report a suspicion of fraud. This includes a dedicated email address, a fraud hotline number and an internal reporting form that is held on Saltire.

Tel: 0300 300 3138
Email: SAASCFT@gov.scot

Anyone who has received information about a suspected internal fraud or a suspicion of bribery or corruption must report it immediately in confidence to the Counter Fraud Manager. All reasonable steps will be taken not to breach confidentiality or to reveal the identity of the complainant and employees who make a disclosure will be treated in accordance with the Public Interest Disclosure Act 1998 (PIDA).


Respond to all allegations of fraud
Gather and review evidence
Conduct Interviews Under Caution
Consider appropriate sanctions/actions
Prepare case for COPFS (if appropriate)

Fraud response

Our Fraud Response Plan is in place to deal with both internal and external fraud, ensuring that a collection of evidence is gathered to criminal reporting standards and that clear lines of responsibility are made clear. Due to the specific nature of our cases, investigations are carried out by SAAS Counter Fraud investigators who are Accredited Counter Fraud Specialists and are Police College Scotland trained.

SAAS is a Specialist Reporting Agency and submits criminal cases directly to COPFS and can apply a range of sanctions.

Success for the Counter Fraud Team in this objective will see allegations being reported with ease, clear instructions and prompt action being taken to investigate any events which occur.

Strategic Objectives

Continued

Review and Learn

Lessons learned

As well as learning from concluded investigations, reviews conducted by the Fraud Analysts are used to assess our systems and processes and will consider our internal controls. They are responsible for ensuring that Management Information is communicated appropriately and results from analytical exercises and standard reporting are used to evidence the need for any operational or policy change. Recommendations are then reported to our Executive Team where appropriate.

Partnership Working

As well as working in partnership with our teams internally, we encourage greater integration and partnership working across other organisations and the public sector, to share information and develop a collaborative approach. We are connected to a wide range of networks and participate in both local and national events, to ensure our knowledge and skills are up to date. We are members of a number of working groups, to ensure we have the largest opportunity to share intelligence and knowledge of the latest fraud trends and best practice.

Success for the Counter Fraud Team in this objective will see the development and implementation of a Lessons Learned recording, reviewing and reporting process and greater partnership working.

Monitor and Measure

Our objective is to support SAAS' values that student funding is an investment in the people of Scotland and that the system is to be efficient and deliver value for money, by protecting this resource from those who intentionally seek to misuse it.

We will use the following to ensure we meet this objective:

- SAAS' Counter Fraud approach is modelled and measured against the Scottish Government Counter Fraud Maturity Model;
- We will use the maturity model to identify key activities, and we will plan to deliver these via our annual Counter Fraud Action Plan;
- We will collate Management Information to allow us to benchmark our progress and will publish our results as part of the Agency's annual report;
- We will use a Fraud Risk Management approach to ensure areas of higher risk are reviewed and process improvements are highlighted;
- We will use a Return On Investment (ROI) model to ensure resources are proportionally directed to the areas most in need, ensuring all efforts are adding value to the Agency;
- Our internal audit service provides assurance on the Agency's management of fraud risk;
- We report to the ARAC who will monitor our progress and ensure that appropriate arrangements are in place;
- Fraud has a lifecycle and will continue to evolve, we must therefore ensure that our response to fraud evolves too;
- We will continually evaluate our results against the Counter Fraud Strategy, publishing a refreshed Strategy in 2023.

Sanctions and further action

A range of sanctions including civil recovery, recommending an individual's funding is restricted or removed, reporting to fraud prevention agencies, reporting to COPFS and sharing information with Police Scotland and other Law Enforcement Agencies are applied appropriately and proportionally.

We can use parallel sanctions, meaning that multiple sanctions can be applied depending on the circumstances of each case and applied independently of each other, providing a layered and structured approach.

Our cases are reviewed and recommendations for further action are based on the sufficiency and admissibility of any evidence we have gathered. Case outcomes are determined on the weight of the evidence and whether it meets the requirement for civil action or meets the standard of proof for criminal action. This allows us to make an informed decision regarding next steps and the application of sanctions. Investigation cases are either 'not proven, proven on the balance of probabilities' (which allows for civil recovery of funds) or 'proven beyond reasonable doubt' which allows for the consideration of reporting the case to COPFS.

We continue to use a scoring matrix to ensure that the sanctions applied are proportionate and consistent to the type of fraud and the severity of the fraud. This also enables us to apply multiple sanctions and to maximise the value of funds recovered, where an individual has received funding they are not eligible for.

We engage fully with our COPFS liaison officer on cases which pass the evidence threshold for prosecution. Only the most serious cases which are deemed to be in the public interest will be passed to COPFS for them to consider prosecution.

The Restricted Funding Panel was set up to consider restricting the level of funding students may receive, in line with the Restricted Funding Policy and consider wider implications to the Agency in terms of controls, policies/practices and exposure to risk. The panel is made up of heads of department across the Agency. They will review all evidence available and make a determination based on this.

Sanctions and further action

Continued

On conclusion of an investigation appropriate action can include:

Warning
Where we have strong suspicions of fraud, we will send a written warning.

Repayment
Civil proceedings to recover monies, to supplement other sanctions.

Restricted Funding
Student no longer eligible for SAAS funding, for up to 6 years.

Cifas Upload
If we have identified a good range of evidence then we will upload the data onto Cifas.

Criminal Prosecution
We investigate and present cases to COPFS for criminal prosecution.

Sanctions applied should be proportionate to the level of fraud committed.

In the event of an internal fraud this can also include:

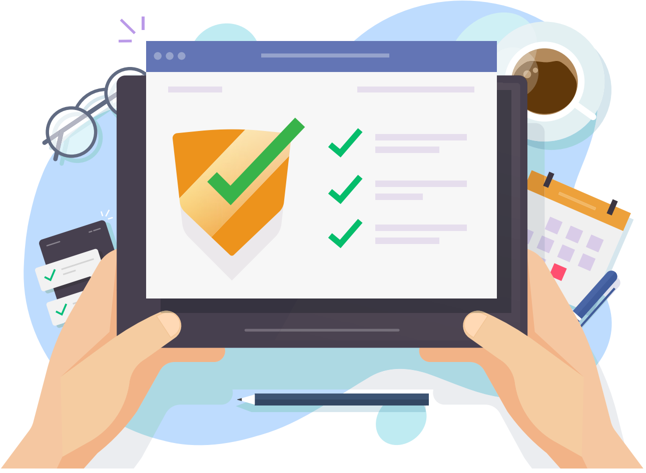
- Disciplinary action
- Dismissal

Although disciplinary action and dismissal may be appropriate sanctions, this does not negate the need to pursue criminal action if it is found that the individual has breached legislation or committed a criminal act.

If disciplinary action is pursued, this must be done so in a way which would not have a negative impact on criminal action.

If it is determined that an allegation is made frivolously, in bad faith or for personal gain, disciplinary action may be taken against the person making the allegation.

Success for the Counter Fraud Team in this objective will be to monitor activities and outcomes to ensure Return on Investment for SAAS and proportionate sanctions are applied at every opportunity.



Dissemination and Responsibilities

It should be recognised even with fraud controls in place, fraud is possible within our organisation and therefore responsibility for preventing and detecting fraud should be that of the whole Agency.

To support this and ensure fraud is visible, we will provide awareness to the Agency via our reporting routes and Communications plan.

It is important that everyone within the Agency is aware of their personal responsibility and fraud commitments, as set out in the table below.

SAAS Accountable Officer (the Chief Executive)	• Has responsibility for supporting the achievement of the Agency's objectives and targets whilst safeguarding public funds, ensuring the compliance with the SPFM. • Their accountability is subject to the respective overall responsibilities of the Permanent Secretary of the SG as the Principle Accountable Officer, The DG for Learning & Justice and the DG for Health & Social Care.
SAAS Management Board	• Support the SAAS Chief Executive by identifying those operational areas where the risk of fraud or other loss is greatest.
SAAS Audit, Risk and Assurance Committee	• Is responsible for overseeing and reviewing the risk, control and governance processes. It also receives reports on any fraudulent activity and considers the Agency's exposure and responses.
Internal Audit Division	• Provide independent assurance on effectiveness of systems of governance, controls and financial management, established to ensure management has reviewed its risk exposures and to ensure accountability of public funds.
SAAS Senior Managers	• Assess types of risk involved in operations, regularly review the control systems for which they're responsible for, to ensure the controls are being complied with. • Implement new controls to reduce risk of similar fraud occurring where frauds have taken place.
SAAS Counter Fraud Team	• Investigate all suspected external fraud cases, build and maintain intelligence to identify the profile of fraudsters that target SAAS and share this with staff. • Work with external partners to share knowledge and increase fraud awareness. • Carry out lessons learned and develop better controls to minimise the potential for fraud.
Each member of staff in SAAS	• Act honestly and with integrity, report any suspected fraud or control weaknesses identified to your Counter Fraud Champion or CFT, be alert to the possibility of fraud and remain vigilant.

Recording and Accounting

The Counter Fraud Team will report regularly to ARAC. In addition, fraud losses in respect of the budget are reported in the Annual Accounts. Losses due to fraud are subject to the guidance on Losses and Special Payments.

Review of the Counter Fraud Policy and Response Plan

The Counter Fraud Policy and Response Plan will be reviewed annually or following any incident of internal or organised fraud. This will ensure that it reflects changes which may be necessary to strengthen future responses to fraud and that it remains fit for purpose.

Conclusion

Our aim is to support SAAS' high standards, procedures and controls in order to minimise the opportunity for fraud to occur and to assist in the early detection of fraud. All cases of actual or suspected fraud will be vigorously and promptly investigated and appropriate action will be taken.

Cases will be reported to COPFS or Police Scotland, as appropriate. The robust measures and collaborative working arrangements detailed in this document, outline the processes which have been put in place in order to achieve this aim. We will continue to tackle fraud in our organisation through continual review and lessons learned. Fraud will continue to evolve, therefore we must ensure that our response to fraud evolves too and we remain alert where we conduct activities to detect fraud.

The role of the Counter Fraud Team

External Large Scale Frauds

All cases of external fraud are managed by the CFT, however, if it is considered that an external fraud case raises concerns regarding the integrity or reputation of the Agency, this will be immediately escalated to the SAAS Executive Team for awareness. The Counter Fraud Manager will present the findings of the investigation and will seek advice on a course of action to take, based on the sufficiency of evidence gathered.

In the event of a large scale fraud or significant loss, this will be immediately reported to the Director of Finance by the Counter Fraud Manager and the Rapid Response Group. The planning will involve determining next steps and who will be involved in the investigation. There may be a requirement to involve certain areas of expertise such as IT, Internal Audit or in more serious cases, Police Scotland.

We are also potentially vulnerable to fraud by our stakeholders, including colleges and universities who receive tuition fee payments and with any supplier of goods which trades with SAAS. Although there are no recorded frauds of this nature, they are considered within this document.

Internal Fraud Investigation

It is imperative that any suspicions are reported as soon as possible to the Counter Fraud Manager and that the allegation is not discussed with anyone else.

Any investigation or enquiry must be dealt with in the strictest confidence as it is imperative that even initial enquiries do not compromise subsequent investigations or evidence. At this stage the Director of Finance will be consulted for overview, to determine an investigations plan and the setting up of a Fraud Rapid Response Group to investigate.

The Counter Fraud Team will have unhindered access to staff and resources to enable them to investigate potential fraud and the investigation will be conducted in accordance with the CFT investigation procedures and regular progress updates will be reported to the determined Fraud Rapid Response Group, as appropriate.

In the event of any expected disciplinary action, HR will be involved and any decisions should be made in consultation with the Investigation Team. This will allow evidence to be secured and action to be taken without one investigation jeopardising the other and to ensure that any evidence gathered would be admissible in civil and criminal courts.

No staff member should handle evidence that may need to be used for court purposes at a later date. This must be managed by the Investigating Team to ensure the integrity and admissibility of evidence, as this will increase the chances of successful investigation.

Throughout the investigation, consideration should be given to next steps, such as whether working with HR to determine if suspension of the individual is required to prevent evidence from being removed or destroyed, or if there is a need to restrict access to systems and when it would be appropriate or necessary to notify the individual. If any of these actions are considered, the appropriate teams should be notified, such as HR, IT and building security.

The role of the Counter Fraud Team

Continued

Any employees under suspicion who are allowed to remain at work, should be closely monitored. This may include: monitoring of movements, monitoring of IT usage, monitoring of telephone, email and internet usage etc conducted within adherence to the individual's right to privacy, monitoring will be conducted by appropriate departments such as HR, Management or IT.

If the investigation is considered in the context of both criminal and disciplinary procedures, both the ACAS Guide and Investigation Standard Operating Procedures must be followed, as evidence gathering must be to criminal law standard.

In any investigation, there will probably be a need to interview employees, witnesses, suspects, or any other person involved. Interviews under caution must only be conducted by trained interviewers. Criminal investigations and prosecution can often take substantially longer to undertake than disciplinary investigations and consequently any disciplinary investigation should not be delayed pending the outcome of any criminal investigation.

It should always be remembered that an allegation of fraud may be unfounded and in order to respect the employee and ensure good working relations after an investigation, any action taken, such as suspension, and interviewing should be handled very carefully.

Staff must not:

- Contact the suspected perpetrator in an effort to determine the facts;
- Discuss the case facts, suspicions, or allegations with anyone outside the Investigating Team;
- Attempt to personally conduct investigations or interviews or question the individual under any circumstances.

The role of the Counter Fraud Team

Continued

Press or Media Enquiries

Occasionally there may be interest from a journalist, newspaper or other media enquiries. It is important that any enquiries are reported or referred directly to the SAAS Communications Team (SAASComms@gov.scot) so they can invoke their own processes and communications protocols.

Conclusion

Our aim is to support SAAS' integrity, high standards, procedures and reputation, in order to minimise the fraud opportunity and ensure the correct action is taken. All cases of actual or suspected fraud will be professionally and promptly investigated and appropriate action will be taken.

As part of our commitment to this plan we will aim to constantly review and understand our current fraud risks which are relevant to SAAS. We are currently improving our prevention and detection activity and are investigating Identity Verification tools, to ensure student funding is directed to genuine individuals and to assist us in the early detection or fraudulent activity.

Following the concluding of the investigation, the Counter Fraud Manager will report as necessary to the Executive Team, Fraud Rapid Response Group, the SAAS Management Board and Audit, Risk and Assurance Committee (ARAC). Quarterly and annual reports are also submitted to ARAC, who may make additional recommendations for improvement.

Our Counter Fraud Policy and Response Plan will be reviewed annually to ensure these are up to date and they remain relevant to the current and key fraud risks posed.

SAAS Student Awards Agency Scotland

Funding your future

SAAS Fraud Unit
Saughton House
Broomhouse Drive
Edinburgh
EH11 3UT

SAAS Fraud Line: 0300 300 3138
Email: SAASCFT@gov.scot

www.saas.gov.uk

- Facebook
- Twitter
- YouTube
- Instagram
- TikTok

INVESTORS IN YOUNG PEOPLE GOOD PRACTICE AWARD

INVESTORS IN PEOPLE

Smarter Scotland Scottish Government

We are a Living Wage Employer

✓ Informing Choices

✓ Funding Futures

✓ Supporting Success