



Anti-Bribery and Anti-Fraud Policy

Policy Owner: Chief Finance Officer (CFO)

ISSR Reference: N/A

Reviewed: Michaelmas 2025

Approved: Full Governing Body Michaelmas 2025

Next Review: Michaelmas 2026

Version Control Information

Reason for Amendment	Role	Date	Main Changes
Annual review	Chief Financial Officer (CFO)	Michaelmas 2025	Combination of Anti Bribery and Anti-Money Laundering Policies. New template. No material amendments.

Contents

1. Aims	3
2. Legislation.....	3
3. Roles and responsibilities	3
4. Policy content.....	4
5. Monitoring	10
6. Links with other policies.....	10

1. Aims

This policy is applicable to all staff of St Dunstan’s Education Group (the Group) and anyone who acts on behalf of the Group.

The aim of this policy is to confirm the Group’s commitment to detecting and preventing fraud, bribery, corruption and money laundering.

2. Legislation

This policy is informed by the following legislation:

- Bribery Act 2010
- Fraud Act 2006
- Proceeds of Crime Act 2002

3. Roles and responsibilities

3.1 St Dunstan’s Education Group

The governing body has a duty to:

- ensure adequate procedures are in place to prevent fraud, corruption, bribery and money laundering.
- lead by example in ensuring adherence to legal requirements, financial rules, codes of conduct and prescribed procedures and practices.

but will delegate day-to-day responsibility to the CFO.

3.2 The CFO

The CFO is responsible for implementation of this policy and for investigating any reported concerns.

This includes maintaining systems of accountability and control to ensure that Group resources are properly applied as intended and will detect fraud and corruption, whilst also ensuring that the Group is not a recipient of illicit funds.

3.3 Other key role holders and their duties

All budget holders must complete the iHasco Anti-Bribery course annually and follow this policy and the iHasco guidance when making decisions on behalf of the Group.

The Group will train its staff from time to time on how to limit the money laundering risks faced by the Group, by enabling staff to spot potential 'red flags' and what steps they must take if a potential risk factor is identified.

All members of the Finance and Development teams must be alert to the risks of money laundering and identify any 'red flags' as listed in Appendix A.

3.4 Staff

All staff are responsible for notifying the CFO if they have any concerns that the policy has been breached.

4. Policy content

4.1 Anti Fraud, Corruption and Bribery

The Group will not tolerate fraud, corruption or abuse of position for personal gain in any area of the Group's activities.

The Group considers that all instances of fraud, corruption and other dishonest behaviour endangers the achievement of the Group's objectives as they divert its resources from the provision of education. There is clear recognition that the abuse of the Group's resources, assets and services undermines the Group's reputation and threatens its sound financial standing.

4.1.2 Definitions

Fraud

Fraud is a range of abuse and malpractice that is covered by the Fraud Act 2006.

Fraud can be defined as an abuse of knowledge or financial position that is done deliberately to create a financial gain for the perpetrator or for a related person or entity and/ or cause a loss to another. It can take place in many ways: withholding information, deliberately misleading, misrepresenting a situation to other, or by abuse of position. Irrespective of the definition applied, fraud is always deceitful, immoral and intentional and creates a financial gain for one party and/ or a loss for another.

Gains and losses do not have to be direct. A gain to a related party or company through intentional abuse of position, albeit not directly to the officer involved, is still fraudulent. In the same way, using the Group's name to procure personal goods and services is also fraudulent where there is a deliberate abuse of position to make a gain in the form of goods and services at a discount price or to get the Group to pay for them.

Corruption

Corruption will normally involve the above with some bribe, threat or reward being involved.

Bribery

There are four key offences under the Bribery Act 2010:

- Bribery of another person
- Accepting a bribe
- Bribing a foreign official
- Failing to prevent bribery

Bribery is not tolerated. It is unacceptable to:

- Give, promise to give, or offer a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given.
- Give, promise to give, or offer a payment, gift or hospitality to a government official, agent or representative to 'facilitate' or expedite a routine procedure.
- Accept payment from a third party that you know, or suspect, is offered with the expectation that it will obtain a business advantage for them.
- Accept a gift or hospitality from a third party where you know, or suspect, that it is offered or provided with an expectation that a business advantage will be provided in return.
- Retaliate against or threaten a person who has refused to commit a bribery offence or who has raised concerns under this policy.

Facilitation Payments

Facilitation payments are not tolerated and are illegal. Facilitation payments are unofficial payments made to public officials in order to secure or expedite actions.

Gifts and Hospitality

This policy does not change the requirements of the Group's approach to gifts and hospitality as set out in the Group's Gifts and Hospitality Policy, which requires all offers of gifts and hospitality above a *de minimis* level to be registered, whether they are accepted or not.

The Group expects that individuals and organisations (e.g. suppliers, contractors and service providers) with which it deals, will act with integrity and without thought or actions involving fraud and corruption. Where relevant, the Group will include appropriate clauses in its contracts about the consequences of fraud, bribery and corruption. Evidence of such acts is most likely to lead to termination of the particular contract and will normally lead to prosecution.

The Group expects staff to act with integrity and to conduct themselves in a manner which does not damage or undermine the reputation of the Group.

The Group requires staff and those acting on the Group's behalf to be alert to the possibility of fraud, corruption and dishonesty in all their dealings.

The Group also requires that those responsible for designing systems and procedures to ensure that the processes in place minimise losses due to fraud, corruption and other dishonest action and abuse.

4.1.3 Raising Concerns

Staff and anyone acting for, or on behalf of, the Group, are an important element in the Group's defence against fraud and corruption; they are expected to raise any concerns that they may have on these issues, where they are associated with the Group's activities.

DET will be robust in dealing with financial malpractice of any kind. Staff and anyone acting for, or on behalf of, the Group should follow the guidance issued in the Group's Whistleblowing Policy.

All concerns reported, by whatever method, will be treated in confidence. Concerns should be raised with the CFO in the first instance, except when it relates to the CEO, in which case the concern should be raised with the Chair of the Board. This may mean that, depending on the level, type and details of the concerns you raise, that your concerns are investigated by the CFO, the CEO, the Board of Directors or, in the case of very serious concerns, the Police.

4.2 Money Laundering

The Group could be used as a vehicle through which criminals seek to launder the proceeds of crime (Illicit Funds). The Group, or a member of staff, is at risk of committing a money laundering offence if they accept Illicit Funds in circumstances where they have knowledge or a reasonable suspicion that the payment is from Illicit Funds.

Staff must be vigilant to the risk of accepting Illicit Funds and play their role in assisting law enforcement agencies in combatting money laundering. The Proceeds of Crime Act 2002 (POCA) (as amended from time to time) imposes obligations on the Group and staff personally, in respect of

money laundering and associated activities.

Linked to this, there are charity law requirements to ensure that reasonable skill and care are used when making decisions about procedures for the receipt and use of the Group's funds.

4.2.2 Definitions

Money laundering is the process by which Illicit Funds are processed or spent to create the appearance that the Illicit Funds have come from a legal source. Although cash-based money laundering continues to be a major method of laundering Illicit Funds in the UK, stricter rules have made it more difficult for criminals to introduce Illicit Funds into the UK banking system. Consequently, criminals are using more inventive methods to disguise the origins of their cash and staff should be alert to practices and payments that they consider to be suspicious, including payments made to the Group via bank transfer.

The term 'money laundering' covers several offences, each of which relate to the improper handling of Illicit Funds so that they appear to come from a legitimate source. Money laundering underpins most forms of organised crime, allowing criminals to further their operations. However, it can also benefit individuals engaging in bribery and dishonest activities such as receiving stolen goods or tax evasion.

Money laundering can take many forms, but in relation to the Group it could involve, but will not be limited to:

- the payment of fees;
- the payment of fees from third parties;
- the donation of sums to projects for which an appeal is being run;
- the donation of sums for no obvious reason;
- the payment in advance of fees; and
- the requested return of donation or fees paid in advance.

These examples are not exhaustive, and staff should remain vigilant in relation to all payments the Group receives.

Donations

Donations are a particular area of potential risk faced by the Group. To mitigate the risk the Group should know, at least in broad terms, where the money it is being given comes from and should be able to identify and be assured of the provenance of substantial donations. A good, open and transparent relationship between the Group and its donors is essential for building trust and confidence.

Good due diligence will help to:

- assess any risks to the Group that may arise from accepting a donation or types of donations;
- ensure that it is appropriate for the Group to accept money from the particular donor;
- give the Group reasonable assurance that the donation is not from any illegal or inappropriate source; and
- ensure that any conditions that may be attached the donation are appropriate and can be accepted.

Where a donation of over £10,000 is being made, the relevant member of staff should review what they know about the donor and the proposed payment using the checklist in Appendix A. The thresholds for giving final approval of accepting gifts are set out in the Gift Acceptance and Ethical Fundraising policy (related document to P17 - finance policy).

If when completing the checklist, the member of staff identifies any red-flags, the member of staff must report the concern to the CFO immediately.

Repayments

The Group's policy is that any refunds or repayments of sums paid to the Group can only be remitted to the bank account that made the payment. If a parent / carer or donor asks for a refund to be made to a different account, in particular one that belongs to someone other than the original payer, you must refer this to the CFO promptly.

Charity Commission

When accepting payments or donations the Group needs to be confident that it knows:

- who is making the payment or donation; and
- the source of funds that are being used to fund the payment.

The Group will also use the following Charity Commission advice to assess the risk of money laundering:

- 'identify' who the Group is dealing with;
- 'verify' where reasonable, and if the risks are high, verify identities;
- 'know what the organisation's or individual's business is' and be assured this is appropriate for the Group to be involved with;
- 'know what their specific business is with the Group' and have confidence that they will deliver what we want them to; and
- 'watch out' for unusual or suspicious activities, conducts or requests.

If the Group is not satisfied with the explanation or evidence provided the Group should obtain further information from the parent or donor.

What warning signs should staff be alert to?

The Appendix to this policy provides staff with a non-exhaustive checklist of potential 'red flags' that may indicate a higher risk of potential money laundering. These questions form part of the Group's risk assessment when accepting payments. They are potentially relevant to all transactions and payments accepted by the Group.

The Group is not expected to consider every payment in detail against the red flag checklist and will consider payments on a risk basis. The CFO has identified the payments listed below as being payments that may expose the Group to a higher risk of money laundering. If a proposed payment is within one of the specified risk categories, you must complete the 'red flag' checklist before the Group can accept the payment:

- Donations over £10,000
- cash payments over £100
- payments from high-risk countries
- payments from PEPs

Where payments are within one of the risk categories listed above, staff must consider the payment against the red flag checklist before the payment can be accepted by the Group. You must promptly report any concerns to the CFO.

All staff, but particularly those staff who in the course of their day-to-day work are likely to deal with financial transactions, including the payments of fees and donations, must ensure that they are familiar with the checklist and understand the nature of the red flags that should be reported to the CFO.

Where you make a report to the CFO you must not discuss your concerns with any other person, including other members of staff, pupils, parents or a donor as this could result in you, or the Group, committing a secondary offence of prejudicing an investigation.

What must the CFO do where a payment seems suspicious?

Where a member of staff identifies a red flag in relation to a payment, the CFO must consider the relevant circumstances relating to the transaction that has raised the concern. The enquiries the CFO will make will depend on the circumstances, but could include:

- asking the payer to explain who is making the payment where this is not clear;
- asking for an explanation of why the payment is being made in a particular way, for example, where payments are being made from a variety of sources or accounts;
- asking the payer for proof of the source of the funds; or

- carrying out a google or other internet search to establish that the payer is not involved in alleged criminal activities.

After having made appropriate enquiries, the CFO will decide whether:

- the payment can be accepted;
- further explanation or evidence as the legitimacy of the funds is required;
- the Group should submit a suspicious activity report (SAR); and
- the Group should make a report to the Charity Commission.

The CFO will keep a record of the decision made in relation to the payment and evidence supporting the decision.

Reporting to the National Crime Agency and Charity Commission

If the parent / carer (or payer) or donor is not able to provide a satisfactory explanation or where there are other factors (for example adverse media publicity) that cause the CFO to have a reasonable suspicion or knowledge that the funds being used to make the payment may be Illicit Funds the CFO must make a SAR to the NCA and, where appropriate request consent to proceed with the transaction.

If the Group has requested a defence against a money laundering offence (DAML) in the SAR the Group should not accept, pay away, return or otherwise use the suspicious payment for any purpose until the time limit for the NCA to respond to the SAR has expired.

The CFO will also consider whether the incident should also be reported to the Charity Commission.

5. Monitoring

This policy will be reviewed by the CFO annually.

At every review, the policy will be approved by the Full Governing Board.

6. Links with other policies

This policy links to the following policies:

- Finance policy
- Gifts and Hospitality policy
- Code of Conduct
- Whistleblowing policy
- Gift Acceptance and Ethical Fundraising policy

Appendix A: Checklist for identifying potentially suspicious transactions

You must consider the following questions in relation to each high-risk payment. If any of the answers to the questions are “yes”, you must refer the payment to the CFO for further consideration. This list is not exhaustive. Even if all the answers to the questions are “no” if something seems unusual you must raise your concern with the CFO.

	Potential red flags	Ask...	Yes/ No
1.	Transactions	<p>Are payments to the Group unusual because of their size, frequency or the manner of their execution?</p> <p>For example:</p> <p>Is the parent unexpectedly or unusually making lots of small payments from several different accounts?</p> <p>Are the payments unexpectedly being paid from a different account?</p>	
2.	Bank account:	Is the payment being made from an account that is not in the same name as the payer?	
3.	Arrangements	<p>Does the payment involve complex or illogical arrangements that make it unclear who is making the payment?</p> <p>For example:</p> <p>Is the payment coming from a variety of sources or payers?</p> <p>Is the payer seemingly unconnected to the pupil, parent or donor?</p>	
4.	Third party payments	<p>If the payment is from an account that is not the parent’s account is the connection between the third-party making the payment and the pupil unclear?</p> <p>For example, is the payment from someone who is not the parent’s employer or a known relative of the pupil?</p>	
5.	Internet search	Are there any adverse media articles about the payer suggesting an involvement in criminal activities?	

6.	Erroneous payments	Has the Group been asked to reverse a payment made because the payment was made in error? Has the Group been asked to send a repayment to a person that is different to the original payer?	
7.	Country of residency	Is the parent resident in or have they recently relocated from, a high-risk country? You should ask the CFO for the current list of high risk countries.	
8.	PEP (Politically Exposed Person – broadly an individual who is performing a prominent public function)	Are either of the parents or the person paying the fees (where different) a PEP? If the parent is a PEP, is their business activity unusual given the public role they hold?	
9.	Assets:	Does it seem that a parent's assets are inconsistent with their known legitimate income?	
10.	Resources	Are the funds being used bearer's cheques or cash?	
11.	Identity	Is the payer difficult to identify?	
12.	Early or quick payments	Is the parent unusually anxious to make a payment? Is the parent unable to justify why they need to make the payment quickly or early?	
13.	False documents	Do any documents appear to be falsified?	
14.	Representative	Have you, or other professionals involved been instructed at a distance, asked to act outside of your usual specialty, or offered an unusually high fee?	