

# Are criminals targeting your school?

The risks associated with accepting funds from fee payers and donors without conducting appropriate due diligence.



TOMORROW  
BEGINS TODAY



**Criminals will try to spend their illicit gains in different ways. This may include paying fees or making donations to your school. For example, there have been high profile examples of bribes being paid to educational institutions in the guise of charitable donations. This guidance is intended to help you identify circumstances that may cause concern so that you can take steps to protect your school.**

The National Crime Agency (NCA) reported that serious and organised crime is estimated to cost the UK economy at least GBP37 billion a year<sup>1</sup>. They also confirmed that the independent education sector submitted only 34 out of the 573,085 suspicious activity reports received in 2019–2020<sup>2</sup>. This suggests that the independent education sector may be under-reporting and/or failing to identify funds relating to criminal activity. As such, you may unwittingly become involved in criminal activity; this can have serious consequences, which can include: (i) Committing a criminal offence under the relevant legislation; (ii) Failing to meet your **Charity Commission**<sup>3</sup> obligations (if applicable); and/or (iii) Exposing your school to reputational risk. Each school should consider its own legal obligations and how the risks can be mitigated, including whether it is appropriate to put policies and procedures in place and provide training to relevant staff.

Some examples of the screening tools, the applicable legislation and practical advice on setting up the appropriate policies can be found at the **Independent School's Bursars Association (ISBA) website**. This document aims to help you consider the practical elements and should be read in conjunction with ISBA's guidance. You may also want to consider obtaining independent legal advice to help guide your approach.

Having robust policies and procedures in place can help ensure that: (i) You conduct sufficient due diligence on payments in order to have an adequate understanding of the source of funds you receive from fee payers (such as parents or guardians) or donors and any risks associated with these; (ii) Staff are aware of "red flags" that require further investigation; and (iii) Staff concerns regarding potential criminal funds are handled appropriately, including (where appropriate) making reports to law enforcement bodies. You may also consider whether it is appropriate to make a member of staff responsible for ensuring that these policies and processes are kept up-to-date and followed by staff.

## **Additional sanctions considerations**

In response to the Russian invasion of Ukraine in February 2022 an unprecedented number of sanctions have been and continue to be imposed on Russian banks, several entities, and a large number of individuals. Financial sanctions are restrictions put in place by the UN or UK to achieve a specific foreign policy or national security objective. In the UK, guidance is produced by the Office of Financial Sanctions Implementation (OFSI), part of HM Treasury. Schools are required to ensure they do not accept payments from banks, entities, and individuals on the UK sanctions list. Furthermore, where a person on the UK sanctions list holds more than 50% of the shares or voting rights in an entity, that entity is usually also subject to UK sanctions. OFSI maintains two lists of those subject to UK sanctions: The consolidated list<sup>4</sup> and list of investment ban targets<sup>5</sup>.

### **In particular:**

- If you know or have 'reasonable cause to suspect' that you are in possession or control of fees or donations paid by a designated bank, entity, or person you must:
  - Not deal with them or make them available to, or for the benefit of, the designated person, unless:
    - (a) There is an exception in the legislation that you can rely on; or
    - (b) You have a licence from OFSI
  - Report them to OFSI

---

<sup>1</sup> <https://nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file>

<sup>2</sup> <https://nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file>

<sup>3</sup> [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/654821/Chapter3.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/654821/Chapter3.pdf)

<sup>4</sup> <https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets>

<sup>5</sup> <https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/ukraine-list-of-persons-subject-to-restrictive-measures-in-view-of-russias-actions-destabilising-the-situation-in-ukraine>

- In practice, this means that the funds from a fee/donation from a designated bank, entity or person should not be used, altered, moved, or transferred. In addition, the designated bank, entity, or person should not be allowed to access the funds. In effect, they should be ‘frozen’.
- In addition to screening new customers, schools should review any existing customers who may have been designated post payment of fees or providing financial donations to the school.

## Red flags to look out for

The scenarios below are examples of where you may want to undertake further due diligence to protect your school from unwittingly receiving the proceeds of crime. The below will help you recognise ‘red flag’ warning signs as quickly as possible and take appropriate action. Please note that the examples provided are based on known case studies, typologies and intelligence but is a non-exhaustive list. It is intended for guidance purposes only:

| Red flags you could discover   | Suggested actions you could take  |
|--|---|
| School receives funds for donations or fees from an unexpected third party without a logical reason or explanation.  | You may wish to:<br>Ask the fee payer/donor to provide evidence of the rationale and their connection to the third party; and/or<br>Scrutinise the source of funds and consider identifying the third party yourself independently through screening tools and/or open-source information.  |
| Third parties dealing with your school request account details outside the normal course of business.  |   |
| Significant changes in the size, nature, and frequency of transactions with a fee-payer or donor that is without reasonable explanation, e.g. if payments start to be made from a different jurisdiction.                    |   |
| Fee payer takes steps to hide their identity and/or is difficult to identify.  | Consider verifying any ID Documents.  |
| Fee payer withholds ID documents or is in possession of falsified information or documents.  | Consider asking a fee payer for reasons for not providing any requested information in writing.   |
| Fee payer displays unusually secretive behaviour, including reluctance to provide requested information (such as source of funds) without a reasonable explanation.  |   |
| Fee payer is unusually anxious to complete a transaction or unable to justify why they need to make a payment quickly.   |   |
| School/staff receive a donation, lavish gifts, entertainment, cash, or items of value and/or donor has intimated that they may expect something in return such as a contract or a place in the school for a connected party. | Ensure you have details of the donor and reasons why the donation has been offered or made. You could scrutinise the source of funds more closely.  |
| Fee payers hold position in a public office and/or may have been the subject of criminal allegations and/or bribery and corruption.  | Consider performing Politically Exposed Person (PEP) screening to see if they hold a position entrusted with a prominent public function. Perform “Adverse Press Checks” to establish if they have been subject to investigations or previous allegations of corruption. Consider screening on a frequent basis and scrutinise source of funds. These actions may equally be appropriate in respect of other red flags. |
| External parties such as donors or investment partnersm have a history of poor business records, controls, or inconsistent dealing.  |   |
| School receives cancellation, reversal, or requests for refunds of earlier transactions from fee payer/donors.   | Consider asking fee payer to confirm the reasons for this payment/reversal in writing. Any request to refund via a different method or to a different bank account is a significant red flag.   |
| School receives payment significantly in excess of what was expected from fee payer/donor for no good reason.  |   |
| Fee payer makes a payment of any substantial sum in cash or bearer’s cheques.  | Consider having a policy under which cash is not accepted as a form of payment if over a relatively low threshold (e.g. GBP100).  |

|   |   |
|---|---|
| Child is in possession of substantial amounts of cash representing “pocket money”.  | Consider having a policy which limits the amount of cash children can carry (e.g. not over GBP1000) and advise fee payer to fund child’s bank account rather than use cash. |
| Fee payer appears to have assets inconsistent with their known legitimate income or sudden increase in wealth.  | Consider performing screening on fee payer. Scrutinise the source of funds.   |
| School employees are instructed at a distance or asked to act outside their usual speciality or offered an unusually high fee.                                    |   |
| School has an entirely non face to face relationship with the fee payer for the child which increases risks around source of funds.                               |   |
| School employees have doubts about the honesty, integrity, identity, or location of fee payer/donors e.g. via overheard conversations, sudden increase in wealth. | Consider performing adverse press screening on fee payer and scrutinise the source of funds.  |

## How can you report any suspicions?

If a school suspects that money laundering may be taking place, it can submit a Suspicious Activity Report (SAR) to the **National Crime Agency**.

If a school is a Charity, there is also guidance available on the [gov.uk website](#) which covers The Charity Commission requirements to report serious incidents which include; money laundering as well as fraud, theft and cyber-crime.

If you identify money laundering or sanctions concerns as well as notifying the authorities, you should also notify your Bank at the earliest opportunity.

You should also bear in mind any data protection and confidentiality obligations your school may have.

Guidance on how to implement reporting mechanisms could be sought from independent legal advice and the Independent School’s Bursars Association ([ISBA website](#)).

This document has been prepared by National Westminster Bank Plc and its affiliates (together “NatWest”) for information purposes only. Furthermore, although the information contained herein is believed to be reliable, it does not constitute legal, investment or accounting advice and NatWest makes no representation or warranty as to the accuracy or completeness of any information contained herein or otherwise provided by it. NatWest does not undertake to update this document or determine the accuracy or reasonableness of information or assumptions contained herein. NatWest accepts no liability whatsoever for any direct, indirect or consequential losses (in contract, tort or otherwise) arising from the use of this material or reliance on the information contained herein.

National Westminster Bank Plc. Registered in England & Wales No. 929027. Registered Office: 250 Bishopsgate, London, EC2M 4AA. National Westminster Bank Plc is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.