SBS INSIGHT HUB

SHARD Business Services

INTRODUCTION TO TACKLING FRAUD: KEY FACTS AND GUIDANCE FOR SCHOOLS - OVERVIEW

HELPING SCHOOLS STAY VIGILANT, COMPLIANT, AND PROTECTED FROM FRAUD

Fraud occurs when someone deliberately deceives an organisation for personal or financial gain. In education settings, this can involve:

- Theft or misuse of school funds or assets
- False invoicing or fabricated expenses
- Misuse of purchasing cards or credit cards
- Cybercrime or phishing attacks
- False reporting or manipulation of records

Fraud is not limited to financial loss — it can also damage your school's reputation and erode trust within your community.

WHY FRAUD HAPPENS

PERSONAL MOTIVES

- Financial pressures, gambling, or addiction
- Expensive lifestyle needs
- Disgruntlement or resentment toward management

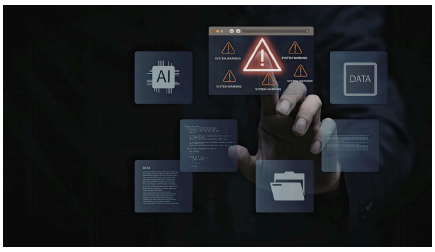
ORGANISATIONAL MOTIVES

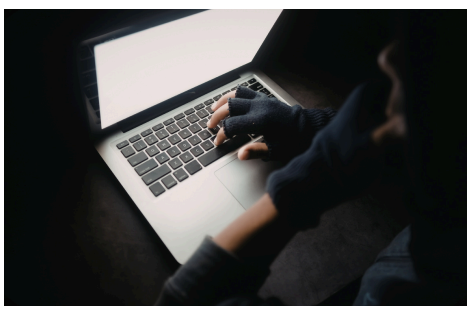
- Financial instability or funding pressures
- Weak internal controls or oversight
- Poorly defined job roles and responsibilities
- Overreliance on one person for financial processes

COMMON WARNING SIGNS

Be alert to behavioural and transactional red flags:

- Unexplained wealth or sudden lifestyle changes
- Employees unwilling to take leave or share duties
- Missing financial records or inconsistent audit trails
- Vague subcontractor agreements or inflated claims
- Reluctance to provide evidence for transactions
- Excessive working hours or unusual system access





FRAUD RISK MANAGEMENT

A strong ***Fraud Risk Management Strategy*** should include:

- A clear fraud response plan and defined reporting lines
- Regular staff training on fraud awareness
- Financial controls such as dual authorisation and segregation of duties
- Periodic internal and external audits
- A confidential whistleblowing policy to protect staff who raise concerns

TACKLING FRAUD: KEY FACTS AND GUIDANCE FOR SCHOOLS

TACKLING CYBERCRIME

Cyber fraud is a growing threat to schools.

Common risks include:

- Theft or loss of digital devices
- Use of insecure public Wi-Fi
- Compromised passwords or accounts

Mitigation steps:

- Follow school cybersecurity and remote working policies
- Keep antivirus and software systems up to date
- Use strong, unique passwords and two-factor authentication
- Avoid downloading or opening unverified attachments or links

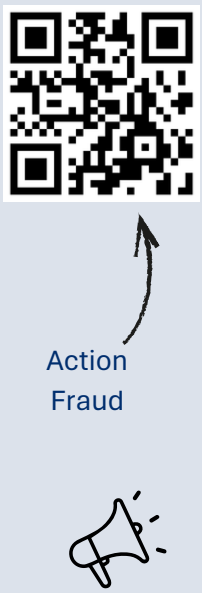
KEY CYBER SECURITY STEPS

- Risk management
- Network security
- User education and awareness
- Malware prevention
- Home and mobile networking controls
- Secure configuration
- Access control
- Incident management
- Monitoring
- Removable media controls

KEY RESOURCES & SUPPORT

- National Cyber Security Centre (NCSC):
- Cyber Exercising Toolkit
- Cyber Security Small Business Guide
- Phishing and password guidance
- Action Fraud: www.actionfraud.police.uk
- ESFA Guidance: Fraud and Cyber Security for Education Providers
- CIPFA Counter Fraud Centre: Fraud prevention tools for public bodies
- HM Treasury: Managing Public Money
- International Public Sector Fraud Forum: Guide to managing fraud risks

IF YOU SUSPECT FRAUD



Fraud prevention is everyone's responsibility. Stay vigilant, question anomalies, and report concerns promptly — awareness and prevention are the best defence.

SUMMARY CHECKLIST FOR SCHOOLS

- ☑ Maintain transparency and robust financial systems
- ☑ Train staff to recognise and report fraud indicators
- ☑ Regularly review IT and access controls
- ☑ Ensure clear reporting lines for suspected fraud
- ☑ Keep fraud and cyber policies up to date and tested

shardbusinessservices.co.uk
07714651415
office@shardbusinessservices.co.uk
shardbusinessservices
shardbusiness
@shardbusiness