"Put your heart and soul into everything that you do."
Purpose. Passion. Success.

Pattishall CE Primary School – Staff and Pupil Acceptable Use & Fraud Policy

1. Purpose

This policy supports the **safe, responsible, and lawful use of technology** within the school. It aims to:

- Protect pupils, staff, and school assets
- Safeguard personal data
- Reduce the risk of cybercrime and fraud
- Meet statutory safeguarding and data protection requirements

It also supports compliance with **West Northamptonshire Council / LA guidance**, **UK GDPR**, and **KCSIE**.

2. Scope

This policy applies to:

- All pupils
- All staff, governors, volunteers, and contractors
- Parents and carers when supporting learning at home
- Any user of school-owned devices, systems, or networks

It covers use of:

- Email systems, internet, network resources
- Software, cloud services, communication tools (e.g., Class Dojo, ParentMail)
- Laptops, Chromebooks, iPads, tablets, cameras, peripherals
- Remote access systems

3. Legal and Statutory Framework (UK)

This policy is informed by and supports compliance with:

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- **Keeping Children Safe in Education (KCSIE)** – latest statutory guidance
- **Education Act 2002**
- **Prevent Duty**
- **National Cyber Security Centre (NCSC) guidance for schools**

4. Acceptable Use of Technology

School technology must be used:

- For educational and professional purposes only
- In line with staff instructions and school policies
- Respectfully, safely, and lawfully

Misuse may be treated as a safeguarding concern, disciplinary matter, or potential criminal offence.

5. Protecting School Hardware and Physical Assets

Pupils and staff must:

- Take reasonable care of all devices and equipment
- Use protective cases where provided
- Store devices securely when not in use
- Report **loss, theft, or damage immediately**

Users must NOT:

- Deliberately damage or interfere with hardware
- Remove devices from site without authorisation
- Connect unauthorised peripherals or storage devices
- Attempt repairs or modifications

Where damage is caused through **negligence or misuse**, the school may seek recovery of costs in line with its charging policy.

6. Account Security and Access Control

To protect systems and data:

- Users must only access authorised systems
- Passwords must be strong, confidential, and never shared
- **Multi-factor authentication (MFA)** must be used where enabled
- Staff must lock screens when away from devices
- Shared accounts are prohibited unless explicitly authorised
- Any suspected account compromise must be reported immediately

7. Data Protection and GDPR Compliance

In line with UK GDPR:

- Personal data must only be accessed for legitimate school purposes
- Data must be accurate, secure, and kept confidential
- Personal data must not be downloaded, shared, or transferred without approval
- Removable media and cloud storage must be **school-approved**

Data breaches (actual or suspected) must be reported immediately to:

- Headteacher
- Data Protection Officer (DPO)

8. Online Safety and Safeguarding (KCSIE)

- Online safety is a **safeguarding priority**
- Internet use is filtered and monitored, but risks remain
- Pupils are taught to stay safe online
- Concerns regarding online content, contact, conduct, or commerce must be reported
- Any online safety incident involving a pupil may be treated as a **safeguarding concern**

9. Social Media and Communication

- Staff must not be friends with pupils under 18, or ex-pupils under 18, on personal accounts
- Avoid social media connections with parents that compromise professionalism
- Posts must **not bring the school into disrepute** or share colleagues without permission

- Only share approved pupil images with **parental consent** on official accounts
- Staff must not discuss school initiatives publicly without approval
- Only school-approved systems (e.g., ParentMail, Class Dojo) may be used for communication with parents or pupils

10. Personal Mobile Devices

- Devices must not be used in lessons or where children are present
- Mobile phones must not be used to photograph or record pupils
- School iPads may be used for pupil images; media must be saved to the network and deleted from the device before leaving school
- Phones must be available during emergencies (e.g., lockdowns)

11. Fraud Prevention and Financial Controls

The school operates a **zero-tolerance approach to fraud**.

All users must NOT:

- Attempt to access financial systems without authorisation
- Impersonate staff, pupils, or parents
- Create or respond to fake payment requests
- Share banking details, card information, or passwords

Staff Responsibilities:

- All payment requests must follow **approved school finance procedures**
- Changes to supplier or bank details must be independently verified
- Financial approvals must follow **separation-of-duties principles**
- Emails requesting urgent payments must be treated with caution
- School email accounts must not be used for personal transactions

Parents and Carers:

- Payments should only be made via **official school systems**
- The school will never request sensitive information via email
- Any unexpected or suspicious payment request should be verified with the **school office**

Pupils:

- Must never engage in online buying, selling, or prize schemes
- Must tell an adult if they receive messages asking for money or personal information

12. Cyber Security and Phishing Awareness

- Be alert to phishing emails, fake links, and pop-ups
- Avoid opening unexpected attachments
- Report suspicious messages immediately
- Only use **school-approved software and websites**
- Cyber incidents may be reported externally (e.g., Local Authority, NCSC)

13. Monitoring and Use of Technology

- The school monitors network and device use for **safeguarding, security, and operational reasons**
- Monitoring is proportionate and lawful
- Logs may be used for safeguarding, disciplinary, or legal investigations

14. Consequences of Breach

Failure to follow this policy may result in:

- Restricted access to systems or devices
- Behaviour or disciplinary action
- Parental notification
- Referral to safeguarding leads
- Reporting to external authorities where appropriate

15. Reporting Concerns

All users must report:

- Lost or damaged equipment
- Suspected data breaches
- Cyber incidents or fraud

- Online safety concerns

Reports should be made to:

- Class teacher
- School office
- Designated Safeguarding Lead (DSL)
- Senior Leadership Team

16. Agreement

By using school technology, users agree to comply with this policy.

17. Approval and Review

- Adopted: February 2026
- Reviewed: Annually by the Full Governing Body (FGB)

Appendices

Appendix A – Finance & Fraud Response Procedure

- Full **fraud prevention, identification, and response procedure** including phishing, invoice fraud, supplier impersonation, and cyber-enabled fraud
- Preventative controls: separation of duties, two-person approvals, verification of bank detail changes, restricted access, annual staff fraud awareness training
- Immediate response: STOP → ISOLATE → REPORT → PRESERVE → CHECK
- Payment already made: notify bank, Local Authority, Action Fraud, Chair of Governors, NCSC if applicable
- Confidentiality assured; staff raising concerns in good faith supported

Appendix B – Phishing Response Flowchart

- Step-by-step guidance for suspicious emails/messages
- Key reminders: never click links, verify requests, report immediately, log all attempts

Appendix C – RACI Matrix for Finance, Fraud & Cyber Controls

- Defines roles and responsibilities for Headteacher, SBM, Finance Staff, ICT Lead, DSL, and Governors
- Ensures **no single individual has end-to-end control** over financial processes
- Supports SFVS and audit compliance

Appendix D – SFVS & Audit Controls Mapping

- Maps **school controls** to SFVS statements and LA audit expectations
- Covers governance, internal control, authorisation, supplier verification, fraud prevention, cyber security, data protection, monitoring, risk management, and audit readiness

Appendix E – Fraud Risk Heat Map

- Assesses likelihood × impact for risks such as phishing, invoice redirection, email compromise, unauthorised purchases, insider fraud, supplier impersonation, and data breaches
- Assigns residual risk and owner
- Supports SFVS risk management and governor oversight

Appendix F – Termly Governor Assurance Checklist

- Records termly oversight of finance, fraud, cyber security, and safeguarding controls
- Ensures accountability, monitoring, and compliance

Appendix A – Finance & Fraud Response Procedure

1. Purpose

This procedure sets out how Pattishall CE Primary School prevents, identifies, and responds to fraud or suspected financial irregularities, including cyber-enabled fraud.

2. Scope

This procedure applies to:

- All staff, governors, and volunteers
- Any person involved in financial transactions or access to financial systems
- All school financial systems, bank accounts, and payment platforms

3. Types of Fraud Covered

This procedure includes (but is not limited to):

- Phishing and email compromise
- Invoice fraud
- Change-of-bank-detail fraud
- Impersonation of staff, suppliers, or parents
- Misuse of school funds
- Unauthorised purchases or transactions

4. Preventative Controls

The school will:

- Maintain **separation of duties** for financial processes
- Use **approved finance systems only**
- Require **two-person approval** for payments where possible
- Verify **all changes to supplier or bank details independently**
- Restrict access to financial systems to authorised staff only
- Provide **annual fraud awareness training** for relevant staff
- Follow Local Authority and audit guidance

5. Responsibilities

Headteacher:

- Overall accountability for financial integrity
- Ensures procedures are followed
- Escalates serious incidents

School Business Manager / Finance Officer:

- Day-to-day financial controls
- Verifies payment requests
- Maintains audit trails

All Staff:

- Remain vigilant
- Follow finance procedures
- Report concerns immediately

6. Identifying Suspected Fraud

Warning signs may include:

- Urgent or unusual payment requests
- Requests for secrecy
- Changes to bank details via email
- Emails with spelling or formatting errors
- Requests that bypass normal procedures

7. Immediate Response to Suspected Fraud

If fraud is suspected:

1. **STOP** – Do not make any payment
2. **ISOLATE** – Do not reply to the email or message
3. **REPORT immediately** to:
    a. Headteacher
    b. School Business Manager

4. **PRESERVE evidence**:
    a. Do not delete emails
    b. Save screenshots or messages
5. **CHECK**:
    a. Verify requests through known contact details (not those in the message)

8. If a Payment Has Already Been Made

The school must:

1. Contact the bank immediately
2. Inform the Local Authority (if applicable)
3. Report to **Action Fraud**
4. Notify the Chair of Governors
5. Consider reporting to the **NCSC** if cyber-related
6. Record the incident in the school's risk register

9. Investigation and Review

- The school will cooperate with auditors and authorities
- Procedures will be reviewed following any incident
- Lessons learned will inform training and controls

10. Confidentiality

All fraud concerns will be handled confidentially and without prejudice.
Staff raising concerns in good faith will be supported.

Appendix B – Phishing Response Flowchart (Staff)

Use this flowchart if you receive a suspicious email, message, or request

```
RECEIVE EMAIL / MESSAGE
     |
     v
Does it ask for:
• Money?
• Urgent action?
• Passwords or data?
• Bank detail changes?
     |
     v
     YES
     |
     v
DO NOT CLICK LINKS OR OPEN ATTACHMENTS
DO NOT REPLY
     |
     v
Is it from a known sender but unusual?
     |
     +---- YES ----+
     |             |
     v             v
VERIFY via trusted contact details
(phone / known email)
     |
     v
Is the request legitimate?
     |
  +----+----+
  |         |
 YES      NO / UNSURE
  |         |
  v         v
Proceed   REPORT IMMEDIATELY
normally  to:
  • School Business Manager
  • Headteacher
  |
  v
DELETE ONLY AFTER ADVISED
```

Key Staff Reminders

- The school will **never** ask for passwords by email
- Urgency is a common fraud tactic
- Always verify financial requests
- When in doubt — **report it**

Record Keeping

All phishing or fraud attempts must be logged, even if no loss occurred.

Appendix C – RACI Matrix for Finance, Fraud & Cyber Controls

Key:

- **R** = Responsible (does the work)
- **A** = Accountable (overall ownership)
- **C** = Consulted
- **I** = Informed

Activity / Control	Head teacher	School Business Manager	Finance Staff	ICT Lead	DSL	Governors
Finance policy approval	A	C	I	I	I	R
Payment processing	I	A	R	I	I	I
Payment authorisation	A	R	I	I	I	I
Bank detail changes	A	R	C	I	I	I
Supplier verification	I	A	R	I	I	I
Separation of duties	A	R	C	I	I	I
Fraud awareness training	A	R	I	C	I	I
Phishing / cyber awareness	I	I	I	A	I	I
Cyber incident response	A	C	I	R	I	I
Data breach response (UK GDPR)	A	C	I	I	R	I
Reporting fraud to LA / Action Fraud	A	R	I	I	I	C
Risk register updates	A	R	I	I	I	C
SFVS completion	A	R	I	I	I	C
Internal audit liaison	A	R	I	I	I	C
External audit support	A	R	I	I	I	I

Notes

- No single individual has end-to-end control of a financial process
- Accountability always rests with the Headteacher
- Governors retain strategic oversight and challenge

Appendix D – SFVS & Audit Controls Mapping

This table demonstrates how the school's controls meet **SFVS requirements** and typical **Local Authority audit expectations**.

SFVS Theme / Audit Area	Control in Place	Evidence / Documentation
Leadership & Governance	Finance policies approved by governors	Signed minutes, policy review log
Accountability	RACI matrix defined and reviewed	Appendix C, staff roles
Budget monitoring	Regular budget reports to SLT / governors	Finance reports, minutes
Internal control	Separation of duties for payments	Finance procedures
Authorisation	Two-step payment approval	System logs
Supplier management	Independent verification of bank detail changes	Verification records
Fraud prevention	Zero-tolerance fraud policy	AUP, Appendix A
Fraud detection	Staff training and awareness	Training records
Incident response	Documented fraud response procedure	Appendix A
Cyber security	Phishing awareness and response	Appendix B
Data protection	GDPR-compliant data handling	DPIAs, breach log
Access control	Role-based system access	User access lists
Password security	Strong passwords / MFA	ICT policy
Monitoring	Network and finance system monitoring	Logs, reports
Risk management	Fraud and cyber risks logged	Risk register
Business continuity	Incident escalation and recovery	BCP
Audit readiness	Clear audit trail	Transaction logs
SFVS compliance	Annual SFVS submission	Completed SFVS form

How This Meets SFVS Statements (Examples)

- **SFVS Statement 2:** Clear governance and accountability → RACI matrix
- **SFVS Statement 10:** Effective internal controls → separation of duties
- **SFVS Statement 14:** Robust fraud prevention → Appendix A & B
- **SFVS Statement 23:** Risk management → documented procedures and review

Review and Assurance

- These controls are reviewed annually
- Outcomes inform SFVS self-assessment
- Any control weaknesses are added to the risk register with actions

Appendix E – Fraud Risk Heat Map

Purpose

This heat map identifies key fraud and cyber-related risks, assesses their likelihood and impact, and records mitigating controls.

It supports:

- SFVS risk management requirements
- Governor oversight
- Internal and external audit assurance

Risk Rating Key

Likelihood	Description
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

Impact	Description
1	Minimal
2	Minor
3	Moderate
4	Major
5	Severe

Risk Score = Likelihood × Impact

Fraud Risk Heat Map Table

Risk	Likelihood	Impact	Score	Controls in Place	Residual Risk	Owner
Phishing leading to payment fraud	4	5	20 (High)	Staff training, phishing flowchart, payment verification	Medium	SBM

Invoice redirection fraud	3	5	15 (High)	Bank detail verification, separation of duties	Medium	SBM
Email account compromise	3	4	12 (Medium)	MFA, password policy, monitoring	Low	ICT Lead
Unauthorised purchasing	3	3	9 (Medium)	Purchase orders, approval limits	Low	Headteacher
Misuse of school credit cards	2	4	8 (Medium)	Monthly reconciliation, card limits	Low	SBM
Insider fraud	1	5	5 (Low)	Segregation, audits, whistleblowing	Low	Headteacher
Data breach (financial data)	3	4	12 (Medium)	GDPR controls, access restriction	Low	DPO
Supplier impersonation	3	4	12 (Medium)	Verification processes	Low	SBM

Appendix F – Termly Governor Assurance Checklist

Area	Assurance Questions	Evidence Reviewed
Finance Controls	Are budget monitoring reports reviewed and challenged by governors?	Termly budget report, minutes
	Are payment authorisations and approvals in line with policy (separation of duties, two-step approvals)?	Payment records, RACI matrix
	Are changes to supplier or bank details independently verified?	Verification records
	Are any unusual or urgent payment requests reviewed?	Email logs, SBM notes
Fraud Prevention	Has any suspected fraud been reported and acted on?	Appendix A logs, risk register
	Are phishing and cyber incidents recorded and mitigated?	Appendix B, incident logs
	Have staff received annual fraud/cyber awareness training?	Training records
Cyber Security	Is the network and device monitoring report reviewed?	ICT logs
	Are multi-factor authentication and password policies enforced?	ICT audit
	Are any data breaches or access issues addressed?	DPIA/breach logs
Safeguarding / Online Safety	Are safeguarding concerns logged and followed up?	DSL reports, CPOMS
	Are online safety policies embedded in teaching practice?	Lesson plans, observations
	Are incidents of online risks or inappropriate use reviewed?	Incident logs
Policy Compliance	Is the Acceptable Use Policy up-to-date and signed by staff?	Signed AUP records
	Are all relevant policies (fraud, cyber security, safeguarding) reviewed for compliance?	Policy review log