DATA PROTECTION EDUCATION

RECORDS MANAGEMENT

SCHOOL LEADERS AND CLASSROOM PRACTITIONERS

A STEP-BY-STEP HANDBOOK

From Policy to Classroom and Beyond

Whole School Approach to Physical and Digital Data

Get in touch

dpo@dataprotection.education

info@dataprotection.education 0800 0862018 dataprotection.education

Table of Content

Introduction

Our Commitment to Data Security

Protecting personal data is a vital part of maintaining the trust that parents, students, staff, and all stakeholders place in you. The way personal data is handled, processed, stored, and securely destroyed is pivotal in maintaining that trust. Our goal is to help schools move beyond ***baseline compliance toward a culture where process improvement enables improved ways of working***

James England, Director and Stuart Lee (author)

The Purpose of This Handbook

This booklet provides practical, manageable steps to support records management in the classroom environment, office, and digital workspace. It is designed to embed a culture where data protection is a seamless part of your daily routine, rather than an additional burden. The guidance within has been developed through direct experience working with schools to implement best practices for both physical and electronic data. This resource is primarily for data leads and school staff responsible for implementing and maintaining data protection standards.

Strategic Goals

To reach these objectives, we utilise a **three-pillar strategy:**

- **Physical Security:** Transitioning toward secure storage solutions and "Clear Desk and Clear Wall" practices to protect sensitive physical records.
- **Digital Integrity:** Ensuring the digital workspace is organised and maintained to adhere to the records management policy and retention schedules.
- **Data Minimisation:** Empowering you to keep only what is necessary, reducing the "data footprint" in your classroom to make information easier to manage and find.

How to use this handbook

This handbook is both a strategic roadmap for leadership and a practical daily guide for the classroom. It has been designed to help you move away from high-risk physical filing toward secure, traceable digital environments. **Work through the phases** for both **physical security** and **electronic record management** across all school systems. **Assess Your Status and Identify Gaps.**

For School Leaders & Data Leads: The strategy

- **Audit & Action:** Focus on the 12-Step Roadmap and the OPERATIONAL REQUIREMENTS (Phases 1–3).
- **Policy Foundation:** Use these sections to audit current systems and establish your master RECORDS MANAGEMENT POLICY.
- **Timeline:** Set the school-wide implementation schedule for both physical and electronic data security.

For Line Managers And Classroom Practitioners: The habits

- **Practical Resources:** Focus on APPENDIX A and the classroom posters (Reference Sheet and S.W.E.E.P. Guide).
- **Daily Routine:** These resources translate strategy into daily habits—such as locking cabinets and managing digital files—ensuring regulatory obligations are met without extra burden .
- **Regulatory Peace of Mind:** Follow the 6-step paths to ensure individual compliance across your workspace .

For All Staff: The Daily Finish

- **Visual Reminder:** Refer to the S.W.E.E.P. (3-MINUTE DATA SWEEP) poster before you leave.
- **The Secure Exit:** Use this as a quick check to secure your workspace, lock your devices, and clear sensitive surfaces .

The Approach

This handbook has been designed as a phased, 12-step walkthrough that covers the full lifecycle of data—from physical displays and cupboards to cloud-based solutions. Whether you have already moved away from storing physical files and utilise the Cloud, or are at the start of your journey, this booklet acts as a useful checklist

Additional support is available via DPE's Record Management Best Practice Area and online Retention Schedule.

At a Glance: The 12-Step Data Security Roadmap

Our data security strategy is built on two parallel paths. **Start with this high-level** summary to assess your current status, then use the detailed operational steps (reference sheet) to ensure full compliance.

The Physical Path (6 steps) 📂

Focusing on the classroom and office environment:

1. Secure Storage: Ensure all sensitive cupboards are locked with managed keys.
2. Minimise Folders: Audit classroom files and move what you can to digital storage.
3. Secure Solutions: Transition from paper-based tracking to secure online systems.
4. Clear Desk/Wall: Enforce a policy to remove sensitive data from public view.
5. Secure Disposal: Provide cross-cut shredding and confidential waste bins.
6. Regular Audits: Conduct unannounced spot checks to maintain standards.

The Electronic Path (6 steps) 💻

Focusing on the digital workspace and cloud storage:

1. Management Policy: Establish a formal Records Management Policy.
2. System Inventory: Document and classify all electronic data by sensitivity.
3. High-Risk Focus: Prioritise retention schedules for SAR-heavy areas (e.g. Email).
4. Security Controls: Mandate MFA and implement secure, traceable file sharing.
5. Data Purging: Automate archiving and delete redundant "digital clutter."
6. Ongoing Review: Audit access logs and review the management policy annually.

Key Definitions

To ensure clarity across all staff levels, we use the following terms throughout this guide:

- MFA (Multi-Factor Authentication): A security process requiring two forms of identification (e.g. a password plus a code on a mobile device) to access a system.
- Data Minimisation: The practice of only collecting and keeping the personal data you actually need, and deleting it once its purpose is served.
- SAR (Subject Access Request): A legal request from an individual (usually a parent or staff member) to see all the personal data the school holds about them.
- Retention Schedule: A timetable that dictates how long specific types of records (e.g. registers, accident forms) must be kept before they are destroyed.
- Regulatory Obligation: Our legal duty to follow data protection laws (such as the UK GDPR and Data Protection Act 2018) to keep people's information safe.
- PoLP (Principle of Least Privilege): Ensuring staff only have access to the specific electronic folders and data required to do their job, and nothing more.

Operational Requirements

Work through the phases/6 steps for both physical security and electronic record management. if you have already implemented step 1, go to step 2 and so on to assess your current status. Highlight areas that need addressing using this booklet and reference sheet as your action plan.

Physical security and data

6 step approach to keeping personal information secure

Phase 1: Physical storage and security of sensitive data

STEP 1

- **Ensure all areas/cupboards storing sensitive data are secure**

If using cupboards/cabinets for storing sensitive data, ensure each cupboard/cabinet has a working key and is secured at night. Either replace lost keys and ensure spare/master keys are kept secure in the office key safe, and reinforce end-of-day routines for locking cupboards/cabinets, or consider key code locks for doors.

Phase 2: Data Minimisation (physical) and Digitalisation (electronic)

STEP 2

- **Review and minimise physical data on walls and in folders**

Remove sensitive data from **walls** and add it to a folder system.

Identify **what data can be minimised in folders**; identify contents of each folder, what is needed, what can be stored and accessed securely online, and what data can be minimised? Could you just have a summary sheet for each class with the essential code (e.g., forename, SEND, G&T, Medical) with the main information stored centrally and/or electronically?

Is information being kept that is no longer needed and can it be securely destroyed?

STEP 3

- **Utilise secure online solutions**

Identify how you can **utilise online secure solutions** for storing and accessing sensitive data (discuss with staff how they currently use existing systems and what obstacles exist).

Develop a timeline and plan for moving from physical to secure online systems.

Operational Requirements

Physical security and data

Phase 3: Policy, Disposal, and Enforcement

STEP 4

- **Define and enforce a 'clear desk and clear wall' policy**

Introduce or **reinforce policy** mandating that all sensitive or confidential data (hospital, medical, SEND, assessment data, contact information etc) must be removed from view on walls, noticeboards, and desks, and stored securely at the end of the school day. **If after a risk assessment it is decided to display certain critical medical information (e.g. significant risk of anaphylactic shock), record your justification and reasons for this. Minimise as much as possible and make parents aware of the information being displayed.**

STEP 5

- **Implement a secure data disposal process**

Ensure every area that handles sensitive data has access to secure, cross-cu**t shredders** or utilises locked, **confidential waste bins** for scheduled collection.

Focus on clearing out unnecessary **"old clutter,"** especially in folders. Establish a clear protocol for when and how physical data must be securely disposed of (records management). Raise staff awareness of the process to follow.

STEP 6

- **Conduct regular, documented compliance audits**

Schedule regular, unannounced **spot checks** to monitor adherence to all security protocols (cupboard locking, key storage, clear wall/desk policy). These can be internal walks and as part of regular DPO visits.

Feedback to staff any spot check findings and regularly remind staff of their responsibilities. Ensure mandatory data protection training and cyber security training (including induction for new staff) is completed annually.

Continually identify opportunities to transition from physical record-keeping to secure online or cloud-based systems. Where physical records remain necessary, perform a risk assessment to determine the sensitivity of the data and apply data minimisation to ensure only strictly essential information is recorded.

Operational Requirements

Electronic record management and recommendations

6 step approach to establish a plan for managing electronic data, starting with establishing policy, guiding documents and ensuring risk identification are in place.

Phase 1: Policy and Risk Foundation

STEP 1

- **Step 1 - Establish Policy Documents**

Establish a Records Management Policy and System Inventory 💻 Develop a formal Records Management Policy and Retention Schedule to act as your "master document". This policy assigns responsibility for electronic data management and sets clear rules for data retention, retrieval, and disposal.

STEP 2

- **Step 2 - Document all electronic systems and data classification**

Document exactly where data resides by identifying all electronic systems, software, and Cloud platforms in use. This baseline is essential for guiding all subsequent security and compliance steps. Note: DPEs supplier best practice area, process to follow and generic third party list can support this process.

Classify this data based on sensitivity (e.g., public, internal, confidential, highly restricted) to help prioritise security and retention efforts.

Phase 2: Implementation and prioritisation

This phase focuses on tackling the most problematic areas first and setting the rules

STEP 3

- **Prioritise systems and apply retention schedules**

Start with the systems you know can be problematic. For example, email (Subject Access Requests).

Apply a retention period to this data. Liaise with your IT provider - can the period set be automated.
Note: Use DPE's online retention schedule for determining retention periods.

Mandate Multi-Factor Authentication (MFA) for accessing all sensitive electronic systems (e.g. email and cloud storage). MFA significantly reduces the risk of unauthorised access due to compromised passwords.

Operational Requirements

Electronic record management and recommendations

STEP 4

- **Work through remaining systems and implement controls**

Liaise with your IT provider regarding what aspects of retention and security can be automated. Implement the **principle of least privilege (PoLP)** to control access, ensuring users only have the minimum permissions necessary for their duties.

Work your way through the different systems (email, Cloud, MIS etc) and identify how you are using these systems and then start to apply retention schedules.

Focus on **reducing data leakage** when sharing securely: Where data must be shared electronically, use secure, traceable methods (e.g. encrypted cloud links, password-protected files) and avoid sharing highly restricted data via standard email attachments.

Check **folder naming conventions** to make it easier to identify folders of leavers for example.

Check against your new Records Management Policy/retention schedule and use it as a working document.

Phase 3: Ongoing Management and Auditing

This phase focuses on actively clearing out old data and ensuring compliance is maintained.

STEP 5

- **Step 5 - Implement data minimisation and archiving protocols**

Establish and communicate a mandatory process for archiving or deleting data that has met its defined retention period.

Focus on clearing out unnecessary "**old clutter**," especially in shared drives and mailboxes. Implement automated email archiving and auto-deletion policies for low-risk, temporary communications to reduce data volume for SARs.

STEP 6

- **Step 6 - Schedule regular audits and policy review.**

Conduct regular audits of access logs, data retention adherence, and folder structures (especially for leavers' data) to ensure compliance. Schedule an annual review of the Records Management Policy to ensure it remains relevant to current data usage and technology.

Appendix A

Classroom guide

Protect Our Pupils: Data Security for Every Teacher, Every Day

This guide is a practical reference for your daily data protection responsibilities. It is based on the seven key principles of UK GDPR, which require us to handle personal data with lawfulness, fairness, and transparency. We must only use data for specific, explicit, and legitimate reasons (purpose limitation), practice data minimisation (not collecting unnecessary data), ensure accuracy, and apply storage limitations (not keeping data for longer than we need to). All data must be handled with integrity and confidentiality, and we must be accountable for our actions.

For all tasks, you must follow the school's official data policies and data retention schedules. If you are ever unsure about how to handle any data, always ask a designated member of staff, such as the Data Protection Officer (DPO) or your line manager.

Mandatory Reporting: Data Breaches (including loss, theft, or accidental exposure) must be reported immediately to your DPO/line manager regardless of how minor they appear. A data breach is defined as any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

PHYSICAL RISKS		
ALL STAFF RESPONSIBILITIES	**Accountability and Lawfulness**	**Timeline**
Immediately forward any requests from pupils, parents, or staff regarding their personal data rights (e.g. access, correction, erasure) to the DPO.	Mandatory under UK GDPR to ensure the school meets the legal time frame, fulfilling Accountability.	Ongoing/Immediate.

SECURE STORAGE AND RESTRICTED DOCUMENTS	Integrity and Lawfulness	Timeline
Secure all sensitive physical files in locked cabinets and cupboards.	Prevents unauthorised physical access to documents, upholding Integrity and Confidentiality.	Daily.
Keep Medical Information and Education, Health and Care Plans (EHCPs) in a designated, locked location, never loose in folders or on display. Note: If after completing a risk assessment you do decide to display a copy in a restricted secure location, minimise data i.e. cover and use initial only.	Essential for protecting special category data, upholding Integrity and Confidentiality and Lawfulness.	Ongoing/Daily.
Securely store class lists with full names and additional student information (such as non-consent for publications) when not in use and do not leave them visible on a desk or counter.	Protects highly sensitive and restricted data from unauthorised viewing, supporting Integrity and Confidentiality.	Ongoing.
Always keep communication books locked in a drawer or cupboard when not in use.	Protects sensitive notes from being read by others, supporting Integrity and Confidentiality.	Ongoing.
Label all sensitive physical documents (e.g., safeguarding notes, medical lists) as 'CONFIDENTIAL' when printing. Never print sensitive documents to shared printers.	Clearly identifies high-risk data that requires heightened security, directly supporting Integrity and Confidentiality.	Ongoing.

CLEAN DESK AND DISPLAY MANAGEMENT	Integrity and Data Minimisation	Timeline
Implement a 'clean desk' policy to prevent sensitive information from being left on display.	Minimises the risk of physical data breaches, supporting Integrity and Confidentiality.	Daily.
Do not leave sensitive information in in-trays or unattended.	Protects information from being viewed by unauthorised individuals, addressing Integrity and Confidentiality.	Ongoing.
Collect all printed information promptly from the printer. Avoid sending sensitive data to printers. Use secure codes when possible.	Protects printed data from unauthorised collection, upholding Integrity and Confidentiality.	Ongoing.
Avoid using the back of cupboard doors or classroom doors to display lists, seating plans, or any other sensitive pupil information.	Prevents accidental viewing of confidential lists, directly supporting Integrity and Confidentiality.	Ongoing.
Avoid putting up displays with full names and photos unless explicit consent has been obtained. Use first names or student IDs instead.	Ensures public displays do not unnecessarily expose personal data, aligning with Data Minimisation and Lawfulness.	Ongoing.

DATA DESTRUCTION AND OFF-SITE	Storage and Integrity	Timeline
Use confidential waste bins/shredders for all sensitive material, ensuring bins are not overflowing and that no sensitive data is left lying around.	Prevents unauthorised access during disposal, supporting Integrity and Confidentiality and Accountability.	Ongoing/Daily.
Destroy all outdated information, including old class lists, seating plans, or transcribed notes. If keeping a template, remove personal data.	Adheres to the principle that data should not be kept longer than necessary, implementing Storage Limitation.	Termly.
Destroy all printed and electronic photos that are no longer needed.	Ensures data is not retained beyond its purpose, implementing Storage Limitation.	As needed.
Remove leaver information from displays and lists for all leavers.	Ensures data is not retained for those who have left, supporting Storage Limitation.	As needed.
When transporting sensitive physical documents outside of the school premises, use a secure, lockable bag or box and transport them directly. Never leave them visible in a car or public transport.	Prevents loss or theft of data while in transit, upholding Integrity and Confidentiality.	As Needed.
Ensure all paper-based medical and emergency contact information is securely stored in a sealed folder or bag and carried by a designated staff member at all times during a school trip.	Protects sensitive health data from loss or theft while off-site, supporting Integrity and Confidentiality and Data Minimisation.	As Needed (per trip).

ELECTRONIC RISKS

SECURITY, ACCOUNTS, AND DEVICES	Security and Integrity	Timeline
Always use Multi-Factor Authentication (MFA) on all school accounts (email, MIS, cloud storage) where available.	Adds a critical second defence against password theft, upholding Integrity and Confidentiality.	Ongoing.
Never write down your passwords or usernames.	Prevents credentials from being easily stolen, adhering to Integrity and Confidentiality.	Ongoing.
Use strong, unique passwords.	Protects accounts by making unauthorised access difficult, ensuring Integrity and Confidentiality.	Ongoing.
Lock your device when you step away.	Prevents unauthorised access and protects data, upholding Integrity and Confidentiality.	Ongoing.
Turn off all devices at the end of the day and store them securely.	Protects data from physical risks after hours, supporting Integrity and Confidentiality.	Daily.
Avoid having multiple tabs open that may have log-in windows for sensitive systems such as CPOMS and Management Information Systems.	Prevents accidental exposure to third parties, addressing Integrity and Confidentiality.	Ongoing.

Follow the school's policy on personal devices (BYOD), avoiding storing sensitive data on them and ensuring they only use the school's authorised Wi-Fi.	Manages data security risks introduced by personal devices, addressing Integrity and Confidentiality.	Ongoing.
Ensure any personal laptops/desktops used for school	Prevents malware from infecting the network, upholding Integrity	Ongoing/Before Use.
Follow the school's retention policy for iPads and tablets ensuring all teacher iPads/tablets have secure codes and 'find my device' activated. Store securely at the end of the school day.	This demonstrates due diligence and oversight, fulfilling the principles of Storage Limitation, Integrity and Confidentiality and Accountability.	Before use/Daily/Ongoing.

EMAIL AND DIGITAL COMMUNICATION	**Data Minimisation and Confidentiality**	**Timeline**
Verify all unexpected requests for sensitive information (like password resets) by calling the sender on a known, official number. Never click links or open attachments from unfamiliar or suspicious emails.	The primary defence against phishing and social engineering attacks, protecting Integrity and Confidentiality.	Ongoing.
Avoid using your email as a filing system. Where possible, avoid adding personal sensitive information to emails. If you do, transfer any relevant staff/student information to secure school systems.	Supports Storage Limitation, Data Minimisation, and Integrity and Confidentiality.	Ongoing.
Declutter and delete all emails from your inbox that you no longer need.	Reduces the overall volume of data that must be managed, supporting Storage Limitation and Data Minimisation.	Weekly.
If you have to share a sensitive file and will be using email, send via secure links with limited access (e.g. restricted to specific users/time) rather than attaching the document to an email.	The link can be instantly revoked, preventing data leakage and supporting Integrity and Confidentiality.	Ongoing.
If you have to use email to communicate with parents, always use BCC when sending emails to multiple external recipients (e.g., parents or job applicants) who do not know each other. Never use CC for bulk emails. Avoid putting any sensitive information in emails. Always double check before sending!	Prevents unnecessary disclosure of sensitive information and personal email addresses, upholding Integrity and Confidentiality and Data Minimisation.	Ongoing.
Use only secure systems for communicating with parents (where possible).	Ensures sensitive information is transmitted securely, protecting Integrity and Confidentiality.	Ongoing.
Only use authorised, secure platforms for student communication and sharing of sensitive information.	Ensures data is processed only within secure systems, protecting Integrity and Confidentiality and Purpose Limitation.	Ongoing.

Do not use any apps for sharing personal data unless they have been authorised by your leadership team and a due diligence third-party assessment has been completed.	Ensures third-party apps meet data protection standards, demonstrating Accountability and protecting Integrity and Confidentiality.	Ongoing.

ARTIFICIAL INTELLIGENCE (AI) BEST PRACTICE	**Accountability and Purpose Limitation**	**Timeline**
Always adhere to the school's AI policy. Never input any personally identifiable information (student names, grades, staff details) into open AI tools (e.g., public chatbots).	Prevents unauthorised disclosure and potential use to train public models, safeguarding Integrity and Confidentiality and Purpose Limitation.	Ongoing.
Consult the Leadership Team/DPO before using any new AI tool that processes data, and ensure human oversight is used to fact-check all AI-generated outputs.	Demonstrates Accountability and ensures high-risk technology is vetted, aligning with the Accuracy principle.	Ongoing.

FILE MANAGEMENT AND RETENTION	**Storage and Accountability**	**Timeline**
Maintain a consistent filing structure (e.g., using year group naming) to easily locate and delete outdated information.	Improves efficiency for deletion, demonstrating Storage Limitation and Accountability.	Ongoing.
Check all online folders. Securely destroy outdated information, including old class lists and notes, using the 'empty trash' or 'secure delete' function. Follow the school's protocol for shared drives. Check the recycle bin and delete contents - is the recycle bin set to auto delete after a set period of time?	Ensures old data is securely and permanently deleted, implementing Storage Limitation.	Termly.
Review all school-related folders, documents, and spreadsheets on your classroom and shared drives. Delete any student data you no longer need.	Shows a systematic process for data management, demonstrating Accountability and Storage Limitation.	Termly/Annually.
Ensure that shared folders on cloud services are only accessible to those with a genuine need.	Ensures data is only visible to those who need it, protecting Integrity and Confidentiality and Data Minimisation.	Ongoing.
Archive photos used for whole-school purposes and delete all others as per school policy.	Ensures photographic data is not retained indefinitely, adhering to Storage Limitation.	Annually

Regularly review and securely delete student digital portfolios or work that is no longer needed, following a clear retention schedule. Check lesson materials or resources for hidden personal data before sharing them (e.g., sample documents that might accidentally include real student names or comments). Ensure records are accurate and kept up to date by liaising with school admin for any updated record, such as medical or contact information.	Applies the Storage Limitation principle to student-specific data. Keeping records up to date demonstrates a systematic effort to maintain compliance, fulfilling Accuracy and Accountability.	Termly.

TRIPS AND CLASSROOM TECHNOLOGY	**Integrity and Confidentiality**	**Timeline**
Ensure all tablets and iPads taken on school trips are password protected and encrypted. Data should be removed promptly upon return.	Protects devices from loss/theft off-site, supporting Integrity and Confidentiality and Storage Limitation.	As Needed (per trip).
Be aware of displaying sensitive data on electronic whiteboards, Who can view this information?	Prevents unauthorised viewing of information left on display, addressing Integrity and Confidentiality.	Daily.
Report all intentions to introduce new systems or apps that process pupil or staff data to the leadership team member responsible, who can discuss with the DPO before implementation (supplier due diligence).	Ensures a DPIA(risk assessment) is conducted to mitigate high risks, demonstrating Lawfulness, Fairness and Transparency, Accountability and Integrity and Confidentiality.	Before Use.

TRIPS AND CLASSROOM TECHNOLOGY	Integrity and Confidentiality	Timeline
Ensure all tablets and iPads taken on school trips are password protected and encrypted. Data should be removed promptly upon return.	Protects devices from loss/theft off-site, supporting Integrity and Confidentiality and Storage Limitation.	As Needed (per trip).
Be aware of displaying sensitive data on electronic whiteboards, Who can view this information?	Prevents unauthorised viewing of information left on display, addressing Integrity and Confidentiality.	Daily.
Report all intentions to introduce new systems or apps that process pupil or staff data to the leadership team member responsible, who can discuss with the DPO before implementation (supplier due diligence).	Ensures a DPIA(risk assessment) is conducted to mitigate high risks, demonstrating Lawfulness, Fairness and Transparency, Accountability and Integrity and Confidentiality.	Before Use.