RECORDS MANAGEMENT REFERENCE SHEET FOR SCHOOL STAFF

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.

DIGITAL SECURITY

1. SECURITY, ACCOUNTS, AND DEVICES 💻

- **MFA: ALWAYS USE MULTI-FACTOR AUTHENTICATION (MFA) ON ALL SCHOOL ACCOUNTS (EMAIL, MIS, CLOUD STORAGE) WHERE AVAILABLE.**
- **PASSWORDS: NEVER WRITE DOWN YOUR PASSWORDS OR USERNAMES.**
- **STRONG CREDENTIALS: USE STRONG, UNIQUE PASSWORDS.**
- **DEVICE LOCKING: LOCK YOUR DEVICE WHEN YOU STEP AWAY.**
- **SECURE STORAGE: TURN OFF ALL DEVICES AT THE END OF THE DAY AND STORE THEM SECURELY.**
- **TAB MANAGEMENT: AVOID HAVING MULTIPLE TABS OPEN THAT MAY HAVE LOG-IN WINDOWS FOR SENSITIVE SYSTEMS SUCH AS CPOMS AND MANAGEMENT INFORMATION SYSTEMS.**
- **PERSONAL DEVICES: 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.**
- **SOFTWARE UPDATES: ENSURE ANY PERSONAL LAPTOPS/DESKTOPS USED FOR SCHOOL WORK HAVE UP-TO-DATE OPERATING SYSTEMS, ANTI-VIRUS SOFTWARE, AND FIREWALLS BEFORE CONNECTING TO SCHOOL SYSTEMS. ALWAYS USE SCHOOL DEVICES IF POSSIBLE.**
- **PORTABLE TECH: 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. IF THERE IS NO SECURE CODE ON THE DEVICE IT IS YOUR RESPONSIBILITY TO FOLLOW THIS UP.**

2. EMAIL AND DIGITAL COMMUNICATION 📧

- **PHISHING DEFENSE: VERIFY ALL UNEXPECTED REQUESTS FOR SENSITIVE INFORMATION BY CALLING THE SENDER ON A KNOWN, OFFICIAL NUMBER; NEVER CLICK LINKS OR OPEN ATTACHMENTS FROM UNFAMILIAR OR SUSPICIOUS EMAILS.**
- **EMAIL HYGIENE: AVOID USING YOUR EMAIL AS A FILING SYSTEM; TRANSFER RELEVANT STAFF/STUDENT INFORMATION TO SECURE SCHOOL SYSTEMS.**
- **REGULAR DELETION: DECLUTTER AND DELETE ALL EMAILS FROM YOUR INBOX THAT YOU NO LONGER NEED.**
- **SECURE SHARING: IF SHARING SENSITIVE FILES VIA EMAIL, SEND VIA SECURE LINKS WITH LIMITED ACCESS RATHER THAN ATTACHING THE DOCUMENT.**
- **BCC AWARENESS: ALWAYS USE BCC WHEN SENDING EMAILS TO MULTIPLE EXTERNAL RECIPIENTS WHO DO NOT KNOW EACH OTHER; NEVER USE CC FOR BULK EMAILS OR SEND SENSITIVE DATA THIS WAY.**
- **APPROVED SYSTEMS: WHERE POSSIBLE USE ONLY SECURE, AUTHORISED PLATFORMS FOR COMMUNICATING WITH PARENTS AND SHARING STUDENT INFORMATION.**
- **APP VERIFICATION: 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.**

3. FILE MANAGEMENT AND RETENTION 📂

- **CONSISTENCY: MAINTAIN A CONSISTENT FILING STRUCTURE TO EASILY LOCATE AND DELETE OUTDATED INFORMATION.**
- **SECURE DISPOSAL: SECURELY DESTROY OUTDATED INFORMATION, INCLUDING OLD CLASS LISTS AND NOTES, USING THE 'EMPTY TRASH' OR 'SECURE DELETE' FUNCTION; CHECK RECYCLE BINS FOR AUTO-DELETION.**
- **REGULAR REVIEW: REVIEW ALL SCHOOL-RELATED FOLDERS AND DELETE STUDENT DATA YOU NO LONGER NEED.**
- **ACCESS CONTROL: ENSURE THAT SHARED FOLDERS ON CLOUD SERVICES ARE ONLY ACCESSIBLE TO THOSE WITH A GENUINE NEED.**
- **RETENTION SCHEDULES: REGULARLY REVIEW AND SECURELY DELETE STUDENT DIGITAL PORTFOLIOS OR WORK THAT IS NO LONGER NEEDED FOLLOWING A CLEAR RETENTION SCHEDULE.**
- **ACCURACY: ENSURE RECORDS ARE ACCURATE AND KEPT UP TO DATE BY LIAISING WITH SCHOOL ADMIN FOR UPDATED MEDICAL OR CONTACT INFORMATION.**
- **PHOTO POLICY: ARCHIVE PHOTOS USED FOR WHOLE-SCHOOL PURPOSES AND DELETE ALL OTHERS AS PER SCHOOL POLICY.**

PHYSICAL SECURITY

1. SECURE STORAGE 🔒

- **LOCKED CABINETS: SECURE ALL SENSITIVE PHYSICAL FILES IN LOCKED CABINETS AND CUPBOARDS.**
- **MEDICAL/EHCPS: KEEP MEDICAL INFORMATION AND EHCPS IN A DESIGNATED, SECURE LOCATION; NEVER LOOSE IN FOLDERS OR ON DISPLAY. NOTE: IF AFTER COMPLETING A RISK ASSESSMENT YOU DO DECIDE TO DISPLAY EHCP/MEDICAL INFORMATION IN A RESTRICTED SECURE LOCATION, MINIMISE DATA I.E. COVER AND USE INITIAL ONLY.**
- **CLASS LISTS: SECURELY STORE CLASS LISTS WITH FULL NAMES AND STUDENT INFO (SUCH AS NON-CONSENT FOR PUBLICATIONS) WHEN NOT IN USE; DO NOT LEAVE VISIBLE ON A DESK OR NOTICE BOARD.**
- **COMMUNICATION BOOKS: ALWAYS KEEP COMMUNICATION BOOKS/DIARIES LOCKED IN A DRAWER OR CUPBOARD WHEN NOT IN USE.**
- **CONFIDENTIAL PRINTING: LABEL SENSITIVE DOCUMENTS AS 'CONFIDENTIAL'; NEVER PRINT SENSITIVE DOCUMENTS TO SHARED PRINTERS.**

2. DESK & DISPLAY MANAGEMENT 🧹

- **CLEAN DESK: IMPLEMENT A 'CLEAN DESK' POLICY TO PREVENT SENSITIVE INFORMATION FROM BEING LEFT ON DISPLAY.**
- **UNATTENDED DATA: DO NOT LEAVE SENSITIVE INFORMATION WITHIN IN-TRAYS OR UNATTENDED.**
- **PRINTER PICK-UP: COLLECT ALL PRINTED INFORMATION PROMPTLY; USE SECURE CODES WHEN POSSIBLE.**
- **DOOR DISPLAYS: AVOID USING THE BACK OF CUPBOARD OR CLASSROOM DOORS TO DISPLAY LISTS OR SEATING PLANS.**
- **PHOTOS & NAMES: AVOID DISPLAYS WITH FULL NAMES AND PHOTOS WITHOUT EXPLICIT CONSENT.**

3. DATA DESTRUCTION & OFF-SITE SECURITY 🗑️

- **SECURE DISPOSAL: USE CONFIDENTIAL WASTE BINS/SHREDDERS; ENSURE BINS ARE NOT OVERFLOWING.**
- **OUTDATED INFO: DESTROY OLD CLASS LISTS, SEATING PLANS, OR TRANSCRIBED NOTES; REMOVE PERSONAL DATA FROM TEMPLATES.**
- **TRANSPORTING DATA: USE A SECURE, LOCKABLE BAG OR BOX FOR OFF-SITE TRANSPORT; NEVER LEAVE DATA VISIBLE IN A CAR.**
- **SCHOOL TRIPS: CARRY MEDICAL/EMERGENCY INFO IN A SEALED FOLDER/BAG BY A DESIGNATED STAFF MEMBER AT ALL TIMES.**

DIGITAL SECURITY

4. ARTIFICIAL INTELLIGENCE (AI) BEST PRACTICE 🤖

- **POLICY ADHERENCE: ALWAYS ADHERE TO THE SCHOOL'S AI POLICY.**
- **NO PII: NEVER INPUT ANY PERSONALLY IDENTIFIABLE INFORMATION (STUDENT NAMES, GRADES, STAFF DETAILS) INTO OPEN AI TOOLS.**
- **DPO/LEADERSHIP TEAM(LT) CONSULTATION: CONSULT THE LT/DPO BEFORE USING ANY NEW AI TOOL THAT PROCESSES DATA.**
- **HUMAN OVERSIGHT: ENSURE HUMAN OVERSIGHT IS USED TO FACT-CHECK ALL AI-GENERATED OUTPUTS.**

5. TRIPS AND CLASSROOM TECHNOLOGY 🚌

- **TRIP SECURITY: ENSURE ALL TABLETS AND IPADS TAKEN ON SCHOOL TRIPS ARE PASSWORD PROTECTED AND ENCRYPTED; REMOVE DATA PROMPTLY UPON RETURN.**
- **WHITEBOARD PRIVACY: BE AWARE OF DISPLAYING SENSITIVE DATA ON ELECTRONIC WHITEBOARDS; CONSIDER WHO CAN VIEW THIS INFORMATION.**
- **SYSTEM DUE DILIGENCE: REPORT ALL INTENTIONS TO INTRODUCE NEW SYSTEMS OR APPS TO THE LEADERSHIP TEAM RESPONSIBLE TO DISCUSS WITH THE DPO BEFORE IMPLEMENTATION.**

DATA PROTECTION IS A COLLECTIVE RESPONSIBILITY. IF YOU ARE UNSURE, ALWAYS ASK YOUR DATA LEAD AND/OR DPO

END OF SCHOOL DAY SWEEP

ELECTRONIC SWEEP 💻

1. **CLEAR THE TABS: CLOSE ALL BROWSER TABS LOGGED INTO SENSITIVE SYSTEMS (CPOMS, MIS, ETC.).**
2. **EMPTY THE TRASH: MANUALLY EMPTY YOUR COMPUTER'S RECYCLE BIN TO ENSURE DELETED DATA IS GONE.**
3. **THE FINAL CLICK: SHUT DOWN YOUR DEVICE FULLY AND LOCK YOUR DEVICE IF YOU LEAVE IT FOR A MOMENT BEFORE TURNING IT OFF.**

PHYSICAL SWEEP 📂

1. **LOCK THE FILES: SECURE ALL SEND, MEDICAL, AND EHCP FOLDERS.**
2. **CLEAR THE DESK: REMOVE ANY FOLDERS WITH SENSITIVE INFORMATION, CLASS LISTS, SEATING PLANS, AND ROUGH NOTES FROM YOUR DESK SURFACE/IN-TRAY.**
3. **SECURE THE BIN: MOVE ALL SENSITIVE PAPER WASTE TO THE CROSS-CUT SHREDDER OR CONFIDENTIAL WASTE BIN.**

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.

DATA RIGHTS: IMMEDIATELY FORWARD ANY REQUESTS FROM PUPILS, PARENTS, OR STAFF REGARDING THEIR PERSONAL DATA RIGHTS (E.G., ACCESS, CORRECTION, ERASURE) TO THE DATA LEAD AND/OR DPO