LONDON GRID FOR LEARNING

TRUSTnet

Data handling check list for compliance & best practice

Introduction

Schools have a duty under the 1998 Data Protection Act to ensure that personal data is stored and accessed securely. Schools also have a need to prepare for the General Data Protection Regulations (GDPR), which will be enforced from 25 May 2018. Personal data includes information in any form (text, images) relating to an identified or identifiable pupil or member of staff. Data protection legislation applies to paper records as well as electronically stored data.

Data protection legislation requires access to personal data to be strictly controlled and also for the integrity of the data to be maintained. This requires the data to be secured against loss through systems failure and also loss through theft of computer equipment or storage media, together with irreparable damage to hardware or media due to, for example, fire or flood.

It is recognised that this is not always easy to fully implement owing to conflict with other existing policy, practice and the limits of some technology.

Strategic	Person Responsible:	Next review date:

- ☐ Ensure school registers every 3 years with the Information Commissioner's Office (ICO)[1]
- ☐ Appoint a named Senior Information Risk Officer (SIRO). This could be the Headteacher.
- ☐ Appoint a named Data Protection Officer (DPO) with responsibility for data protection compliance. This should be a discrete appointment and must avoid conflicts of interest (see DPO FAQs document at gdpr.lgfl.net
- ☐ Consider whether to conduct a Data Protection Impact Assessment, especially prior to the implementation of new processing activities or new IT systems[2].
- ☐ Make sure ALL staff are fully aware of, and understand the implications of, the school's Acceptable Use Agreement and Policy (AUP), and its updates and have signed an agreement.
- ☐ Make sure ALL staff have Disclosure and Barring (DBS) checks in-place (formally CRB) and keep your data as a Single Central Record (preferably in your MIS, such as SIMS Personnel)[3].
- ☐ Ensure all data subjects (staff, learners and parents where applicable) are aware of what data is being held about them, for what purpose and how it is used by issuing privacy or fair processing notices[4].
- ☐ Ensure contracts for employment state that misuse of data is a disciplinary matter.
- ☐ Identify your information 'assets' (e.g. HR data, exam data, student contact data) and for each one, identify an Information Asset Owner (IAO). Check the risks and controls on those data assets. There is a data asset audit/log template at gdpr.lgfl.net to help you with this.
- ☐ Have strategies for managing and recovering from incidents where information at risk, *i.e. who to contact, where to get advice, how communicate, etc*.
- ☐ Have procedures in place to detect, investigate and report a data breach to the ICO when necessary[5] (within 72 hours under GDPR).

Transferring data	Person Responsible:	Next review date:

□ Protectively mark documents (electronic or paper) that are sensitive
□ Do not send sensitive data across unencrypted routes and if no alternative is available, take sensible precautions (e.g. password protect the file and send the password separately) or don't send it.
□ Never just 'forward' sensitive documents/data out of one email system to another email system without protecting the data. Care should be taken to ensure the email is correctly addressed.
□ Only transfer documents with the Local Authority / Health and Welfare services using a Local Authority approved secure transit (usually not email).
□ Do not use personal computer systems or personal email addresses; these may not have adequate security protection.
□ Tryto avoid sending anything sensitive by fax (this old technology is still sometimes requested!), be careful to dial correctly and take steps to ensure the intended recipient has received the information as soon as possible after sending the message.
□ If sending through post - double bag and mark the inside bag confidential/sensitive. Consider using courier / recorded post if particularly sensitive.

Staff practices	Person Responsible:	Next review date:

□ **Ensure staff accessing sensitive data know to use complex (strong) passwords, change them regularly and keep such passwords unique.**
□ **Staff should never share passwords.**
□ **Ensure staff do not take any data off site that is not on an encrypted device and minimise the need to ever take data off-site. Treat paper copies with the same care.**
□ Staff should lock computer screens or log-off when away from the computer.
□ Ensure staff are aware of their responsibilities - data security issues and risks, and know who to report to when information put at risk (e.g. USB key lost, folder of contact details mislaid) – and provide periodic refresher training.
□ Do not permit staff to store / hold pupil or staff data on any device that is not owned by the school or part of the school network (such as personal cameras, laptops, smart phones, personal 'drop boxes', etc.)

Administration practices	Person Responsible:	Next review date:

□ **Ensure data is updated regularly so it is as accurate as possible.**
□ **Ensure filing cabinets used to stored sensitive documents are locked.**
□ **Shred sensitive paper documents when no longer required,** e.g. at end of meetings; **preferably use a cross cutter shredder.**
□ **Only transfer pupil data (CTFs) using the DFE secure method (S2S).**
□ **Only transfer Key Stage and Census returns to via the approved system**
□ When printing or photocopying documents, don't leave copies behind and take care to ensure you collect the correct number of pages and the originals.
□ Use the Pan-London Admissions System (combined with OTP tag).

Technical systems	Person Responsible:	Next review date:

□ Dispose of equipment following WEEE (Waste Electrical and Electronic Directive[6]). Ensure the disposer/recycler securely wipes data to ICO standards on all hardware (include photocopiers).

□ Ensure all computers are 'on the network' or synchronised with it regularly, so kept up to date with protection software (anti-virus etc.,) so data is not put at risk.

□ If staff are storing sensitive documents or photographs on the school network, ensure they are in folders in an area restricted to relevant staff only.

□ Ensure that all devices (laptops, USB keys, external hard drives) are actively encrypted if they will be used for storing sensitive data.

□ Ensure back-up is daily and stored in encrypted format. If you use physical tapes, ensure they are stored in a secure, fire-proof safe. Periodically, check back-ups are correctly working. Preferably, use remote, secure back-up, such as LGfL GridStore, for disaster recovery.

□ Set-up auto-lock after 'X' minutes on relevant devices to secure them if they are left idle.

□ Allocate OTP (one time password) tags to staff sending sensitive data across London so all exchange has 'two-factor' data security applied (i.e. username, password, and OTP PIN number.)

□ Use LGfL's USO-FX2 or similar approved system to exchange sensitive data and documents across London schools, e.g. for sending references or documents about named children.

□ Enforce regular password changes where possible. This is essential for systems that contain personal information, e.g. your MIS. (Normal recommendation is every 90 days.)

□ Use recommended email, online platforms or portals and remote access to school or web hosted resources, (i.e. ones that use SSL or IPSec encryption). (Take advice from your MAT, LA, LGfL, etc).

[1] http://www.ico.org.uk/what_we_cover/register_of_data_controllers.aspx

[2] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[3] www.homeoffice.gov.uk/dbs

[4] http://www.education.gov.uk/researchandstatistics/datatdatam/privacynotices/a0064374/pn

[5] https://ico.org.uk/for-organisations/report-a-breach/

[6] http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx