Leadgate Primary School

Staff Protocol and guidance around GDPR April 2018

To read in conjunction with the GDPR policy and appendixes

This document outlines school policy and procedure relating to GDPR requirements and ensured the compliance of the school when processing both personal and special category information. This protocol must be followed by all staff working at Leadgate Primary School. It is by no means an exhaustive list of requirements and is a working document. Any additional issues may arise and lead to the development of these practices further.

For the purpose of this document data is classified into 2 categories:

1. Data that contains neither personal or special category information (e.g. worksheets, display signage)

2. Data that contains personal or special category information (e.g. planning, assessment, support plans)

All personal and special category data must be held securely at all times.

Office 365

Wherever possible Office 365 will be used to store data however staff must ensure that they access Office 365 via a 2 stage log in process e.g. log into a computer and then use personal log in to access Office 365. Passwords should remain secure and complex to avoid detection. E.g. a combination of capital and lower case letters, numbers and symbols.

USB

To avoid any aspect of data breach or confusion around what data is personal or special category all electronic school information that is transported around school and off site will be kept on an **encrypted** USB. Any staff who have a specific need for a USB, must apply for an encrypted device from the Headteacher, with a clear reason why it is needed instead of OneDrive. These are the only USBs to be used in school and remain the property of school. Please remember that if you forget the password for your USB it cannot be recovered and work is lost.

Servers

Work that does not contain special category information can be kept on servers. If it contains special category information it must be password protected. In the case of planning and assessment ensure that only initials are used to identify pupils.

Email

Whenever communicating via email ensure that pupil initials are used and if a document is shared and has data within it it must be password protected with the recipient to contact the sender to verify the password.

Emails must not be used for personal use.

Emails between parents and school must always be processed via the school generic email address and again these must be verified before communication can continue.

Phone calls

When making phone calls with agencies or parents it is important to verify the caller. This is particularly important when leaving a message. Some LA agencies will verify themselves or the pupil by offering additional information e.g. a phone call from Dawn Grant at the MASH will be verified by offering the last 4 digits of the pupils' UPN.

Individual pupil paper-based records (transfer folders, SEND information, safeguarding information) are held in locked cupboards. Paper safeguarding information is held within a locked office and then within a locked cupboard. Within the classroom setting paper based records may include assessment data, date of births etc. these should remain with a member of staff, not be left lying around the classroom and if transported offsite remain securely stored. No special category data e.g. SEN records, should be taken in paper form offsite with prior discussion with the HT and DPO. Any queries regarding this should be directed to key staff.

Transport of documents

The transportation of documents offsite must be carefully considered at all times. All data must be transferred either on Office 365 or an encrypted USB. Laptops may be held in personal vehicles between moving from school to home or vice versa. No data which identifies staff or pupils will be held on laptops and therefore should they be stolen no data will be lost.

Transferring data

When a pupil moves school the transfer of data is controlled by the senior office admin, the SLT and safeguarding team. The senior office admin ensures CTF files are transferred securely via Secure Access. Paper based records (including SEND and safeguarding) are organised and taken in person to the relevant school by a member of the SLT or safeguarding team. As part of this process a transfer record sheet is completed and signed by Leadgate staff and the receiving staff – a copy is retained for the new school and also kept by Leadgate Primary. For pupils who move out of the LA then special delivery is used to transfer information as a last resort after pursuing secure email sharing.

Books

Books will be retained for progress purposes in school in a secure / locked setting. Books can be taken offsite for the purpose of marking however they must be stored safely and taken directly to the home, not left in cars unattended at any time.

Portable devices

No data that identifies pupils or staff is to be held on any portable device. This significantly reduces the risk of a data breach due to crime. No cameras are to be taken off site (see below). For staff with school issue iPads these must contain a password or code to open and must not contain any personal or special category data.

If through necessity staff must access their work emails via their personal phone then their phone and email access must be password/code protected at all times.

No portable devices must be used for personal use.

No portable hard drives to be used.

Cameras and photos

Whilst cameras will be taken offsite to take photos (e.g. on a school trip) cameras and storage cards must not be taken offsite to process photos as the cameras are not secure. Photos that are to be processed offsite must be held either on Office 365 or an encrypted USB.

Photos of pupils who have left should not be displayed.

Mobile Phones

Personal mobile phones must not be used for processing any data containing personal or special category data at any time.

Websites

The school website contains information about pupils and their images. Parental consent will be sought yearly to process this information. On these websites, no full names will be used and photos of pupils who have left the school must be processed accordingly.

The school office will hold a list of pupils whose images cannot be used online in any capacity.

Child Protection

Wherever possible, any paper documents relating to Child protection, safeguarding or from other outside agencies, should be scanned and saved onto the secure site, then the paper record shredded.

Passwords

Rather than changing passwords regularly (e.g. every 3 months) passwords should be significantly robust to ensure there is not a data breach. The following guidelines are advised:

Strong passwords contain at least a combination of the following:

* upper case letters

* lower case letters

* numbers

* symbol

they should not be recognisable words related to the person e.g. password, family names etc.

Retention of records

The records management toolkit will be followed for the retention of all records please see the retention policy for further information.

Back-up of information

Information must only kept for the amount of time as outlined in the records management toolkit. Where personal data is held e.g. planning for future years ensure that no personal data is kept on file.

The school backs up its servers daily and also has a NAS box as additional back up.

School building access

Access to school is via personal fob / key and the main entrance during normal school hours.

Your school entrance fob must not be attached to your school ID.

Any loss of school ID badge or personal fob must be reported immediately to the Headteacher.

Consent

Consent must now be actively sought. Consent cannot be given through non response e.g. if you do not reply we take this as you consent to this trip/information etc.

If the GDPR policy and advice in this document are not followed and there is a data breach then the member of staff is liable and disciplinary action could be taken.