Castle View Primary School

Headteacher: Miss Claire Bright

Keswick Road, Lancaster, LA1 3LE
Tel. 01524 67880

Castle View Primary School Information Governance Risk Assessment

Identified risk	Management strategy
Storage of data	Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use. Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access. The school will encourage a 'clear desk/ clear pigeon hole' policy whereby sensitive data is removed and locked away when not in use. Staff to make use of lockable cabinets in classrooms for storage of sensitive data. Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
Access to secure data on the school network.	Staff will be provided with individual log ins to the school's computer network, and will be responsible for the security of this log in. Staff must not share log ins. Non-staff personnel will be given lower-level access to the computer network and IT systems.
Staff accessing secure data (e.g. through email or CPOMS or WebDav) on unsecured or personal devices.	Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security

	procedures for school-owned equipment. The onus is on staff to ensure the security of school data accessed on personal devices. From April 2018 using a USB plug-in data storage to download data from the school network will require staff to encrypt their data storage device. Staff will be prompted to follow steps (see instructions circulated) to install and activate BitLocker. Staff will still be able to plug in a USB storage device to upload data from an unencrypted device onto the school network, but please be very wary about using unencrypted devices as a lot of the data staff will be carrying is likely to be considered sensitive. Staff do not have to encrypt their data storage device with BitLocker, but if staff are moving data in a different way, staff are responsible for keeping it safe. Instead of using a portable data storage device, staff may choose to use WebDav or the Office 365 cloud storage options, which will keep the information safe. Remember that if staff are accessing school information (through a portable storage device, or through WebDav, Office 365 cloud or emails, CPOMS, etc) on a personal device (personal laptop/ iPad/ phone) staff are responsible for ensuring its security. Staff must ensure that any devices used for accessing school data are secure – e.g. having encryption (or at least a strong password) on a phone, or having encryption on their laptop. Be especially wary of allowing personal devices to save their passwords for accessing school data (e.g. their Office 365 password), as this removes a layer of security. Staff should not download and save school data onto an unencrypted device, and must ensure that any downloaded data/files are securely deleted.

Staff taking personal information out of school, e.g. staff taking planning home; DSL taking information to a meeting.	Personal information may only be taken off site (in paper or electronic form) by named personnel, including family support staff, teachers and senior managers. The onus is on staff to ensure that documents taken off site are stored securely, and not exposed to undue risk – for example by being left in a car boot, or on a table at home when third parties are in proximity. The same precautions must be taken with data as when within the school.
Sending secure data to print on an open-access device.	Staff are expected to either send to a printer they are in physical proximity to and can supervise, or to make use of the school's 'secure print' facility.
Leaving secure data on a printer.	Staff are expected to print and collect documents straight away, and to store them securely.
Disposal of secure data	Staff are expected to make use of the 'confidential' shredding bins around school to dispose of any documents containing sensitive data. Personal information that is no longer needed, or has become inaccurate or out of date, will be disposed of securely. For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.
Secure data that is in use in school (e.g. notes in diaries, pupil pictures on wall displays) may be seen by third parties.	The school will vet third party contractors who come onto site, and ensure they read and sign our school induction folder. Visitors, such as families, who come into school will be escorted by staff, to ensure they do not take pictures of, or remove, sensitive data. When school is closed, blinds on windows and doors will be shut to prevent access to secure data.
Transferring sensitive data manually or digitally	Staff will ensure that they take all reasonable steps to ensure the protection of data they are transferring. Before sharing data staff will take steps to ensure they have the right to share it, and

	gain consent if necessary. Sensitive documents being transferred in person will be handed to the named recipient. Documents being transferred by third party will be by means of a reputable, tracked courier service, such as Royal Mail or Parcelforce. Staff will take all reasonable efforts to ensure that the information is addressed correctly and accurately, and is enveloped/ wrapped appropriately. Data being transferred digitally will be by means of an encrypted data storage device (e.g. USB stick), or by encrypted email, or encrypted website (e.g. the DfE S2S website). Staff will take steps to ensure the accuracy of the recipient's address before sending. Emails sent to third parties will be send BCC so that email addresses are not disclosed.
Sending sensitive information to families – e.g. letters; pupil information forms.	Sensitive information should only be communicated to the relevant recipient, not passed through third parties (unless the recipient has given specific consent, for example for use of an interpreter). Documentation containing sensitive information should only be handled by responsible members of staff, who should hand it directly to the named recipient. Documentation may alternatively be sent to the named recipient by a reputable courier service, such as Royal Mail or Parcelforce. Staff will take all reasonable efforts to ensure that the information is addressed correctly and accurately, and is enveloped/ wrapped appropriately.
Sharing pupil names within the school community – e.g. giving a parent a list of class names for Christmas cards.	The school will request consent to share pupils' first names with external parties, such as organisers of events happening in school; in nativity show programmes, or name lists for families to write Christmas cards. When sharing names the school will not give

	surnames or surname initials.
Promotion of the school making use of individuals' names and images.	The school will request consent to share pupils' first names with external parties, such as organisers of events happening in school; in nativity show programmes, or name lists for families to write Christmas cards. When using pupils' names in publications the school will only use their first name.
Third parties' use of the premises.	A note to lettings policies and agreements to explain expectations to lessee. Vet potential lettees before agreeing use. Data within school to be secured as described above.