St John's Catholic Primary School

Information Security Policy

DRAFT

Approving Body	St John's Governing body
Approval Date	September 2018
Review Date	September 2019

Contents

DRAFT

1. Introduction

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 (f) of the GDPR requires that personal data shall be:
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."
All personal data whether manual or electronic must be kept secure to prevent accidental loss, damage or destruction. The extent of the security measures required will depend on the sensitivity of the data.

2. Responsibility for information security

The **Headteacher or Principal** must ensure that all staff are aware of their responsibilities for information security as set out in this policy.

All staff and governors have a responsibility to ensure that they have read this policy and that they take all practical steps to ensure that they keep personal data secure.

All staff must take the following basic steps:

- Lock the office when leaving it unattended for any length of time to prevent unauthorised access to personal information.
- Manual records containing personal information should be locked away in a cabinet or drawer when not in use.
- When documents containing personal information have reached the end of their life dispose of them by shredding or use the confidential waste bins.
- Do not share your user ID or password with anyone.
- If you have a laptop which holds personal data, make sure it is encrypted.
- Ensure that your computer screen cannot be viewed by any unauthorised personnel.
- Do not send personal information by fax unless the information has been depersonalised or the fax machine is a 'safe haven' one (in a secure area, which is locked when unattended).
- Do not send personal information by unsecured email as its security cannot be guaranteed. If it is necessary to send information in this way and you do not have access to secure email, make sure the personal information has been either password protected or de-personalised. Send the data as an attachment to the email and flag as confidential.
- If sending any email to multiple recipients outside of the academy, consider using blind copy facility so recipients can't view other recipients' email addresses (which, depending on the subject of the email, could constitute personal information)
- If you are required within the course of your duties to take personal data home (including laptops, videos, etc), do not leave the information unattended for any length of time, especially in a vehicle overnight.

DRAFT

- Do not give out personal information over the telephone; invite the caller to put the request in writing. If the request is urgent take the callers name and telephone number and verify their details before responding.
- Do not discuss other people's personal business in public areas where conversations can be overheard by people with no right to know the details of the information.
- Remember - at all times treat people's personal information as you would wish your own to be treated.

All staff must also ensure that they report any suspected or confirmed information security breaches to the KCSP Data Protection Officer IMMEDIATELY they become aware of the breach. The contact details are:

Michelle Boniface dpo@kcsp.org.uk 01622 232662/ 07718 424788.

Jon Gambell (St John's GDPR Link person) jgambell@stjohnsprimary.kent.sch.uk 01474 534546

3. Transporting information securely

When there is a need to transport information held within documents, laptops, mobile devices etc, which are of a confidential nature i.e. personal to staff or pupils, or commercially sensitive, it is important to ensure precautions are taken to reduce the possibility of these being stolen.

Staff should therefore take all reasonable steps to ensure security is maintained when transporting information between work and home or between work bases. Documents and mobile devices should be transported in a way to minimise the opportunity of destruction or loss by ensuring vehicles used to transport them are kept locked and secure particularly when unoccupied.

Car Crime

Many thefts from cars are opportunist crimes of items that may or may not be of value, but are visible to a thief. Thefts can occur whilst stationary at traffic lights, moving through slow moving traffic or whilst parked in a drive/car park. They do not necessarily have to occur when vehicles are left unattended in badly lit or deserted places. Opportunist thefts take place anywhere, anytime and often within seconds.

The best guard against theft of personal information and mobile devices is to avoid having to transport where there is no absolute need. If it is necessary to transport personal information the following steps should be taken:

- Avoid transporting complete files. Only take the relevant documents where possible.

DRAFT

-

- Do not advertise that you are or will be taking home or transporting items of a confidential nature.
- Ensure that personal information or mobile devices are transported within secure bags, boxes, folders etc to reduce the risk of loss or damage.
- Personal information and mobile devices transported in vehicles should be kept hidden away in a locked boot wherever possible or otherwise kept out of sight to discourage opportunist grab crimes.
- Personal information and mobile devices should not be left unattended even in locked vehicles especially overnight.
  If you can take personal information or mobile devices with you when you leave your vehicle.
- Aim to park in busy, well-lit areas or where there is CCTV coverage to discourage thieves.
- If leaving your vehicle even for a second, for example whilst paying for petrol or using a cashpoint, ensure your vehicle is secure and that doors, windows, the boot and sunroof are all locked.

4. Sharing Information Securely

By Post

If you are sending **personal information** by post, you must:

- confirm the name, department and address of the recipient;
- seal the information in a robust envelope;
- mark the envelope 'Private and Confidential – To be opened by Addressee Only' and place this inside a larger envelope with only the correct name and address on it - this adds an additional level of security as the package is not easily identifiable as 'valuable' and administrative staff should only open the outer envelope;

If you are sending **sensitive personal information** by post, you must also:

- send the information by recorded, registered or 'signed for' delivery or by courier where appropriate;
- ask the recipient to confirm receipt; and
- record the disclosure on the individual's file
- Registered post is the best way to send sensitive personal or confidential information on an encrypted USB memory stick.

Different levels of security can be used depending on the information being sent:

DRAFT

-

- Reliable transport couriers should be used at all times. Consult with your organisation.
- Packaging must be adequate to protect the contents from damage during transit.

By Telephone

If you have received a request to share personal information via the telephone, you must first confirm that the requestor is who they say they are and has a legitimate reason for access to the information.

Where possible ask for the request to be put in writing or if urgent ask for their contact details. Only accept the main switchboard number of their organisation and confirm with the operator the name, job title, department and organisation of the person with whom you wish to share information. Do not accept a mobile phone number.

Once you have confirmed this:

do not share information when a return telephone number cannot be supplied - call the requestor back via the switchboard;

- only provide the information to the person who has requested it - if they are not there you should leave a message for them to call you back;
- do not leave a detailed (disclosure) message with someone else or on a voicemail;
- be aware of who might overhear your call;
- keep a record of any personal information disclosed during the call; and
- record on the individual's file the time of the disclosure, the reason for it and if appropriate, who authorised it.

By Fax

Paper documents are somtimes sent by fax. Precautions must be taken when sending personal information by fax because the receiving machine may be sited in an open office, meaning the document is visible to other staff, contractors or visitors. Where possible any information should be shared via a dedicated fax (known as a 'safe haven' fax machine).

If you are sending information by fax to a machine that is NOT a safe haven one you must:

- remove any information that could identify an individual
- telephone the recipient of the fax to let them know you are about to send it;
- check the fax number. If the information is confidential ask them to wait by the fax;
- ask the recipient to confirm receipt of the fax; or call them to ensure the fax has arrived;
- use pre-programmed fax numbers where possible to reduce the chance of the fax being sent to the wrong machine;

DRAFT

•

- ensure that you use an appropriate fax cover sheet. Make sure your cover sheet states who the information is for, and mark it 'Private and Confidential';
- ensure you do not refer to the names of the person(s) concerned in the subject heading or on the cover sheet of the fax; keep a record that you have sent the fax on the service users file.

By email

Huge amounts of information are sent by email, within and across agencies. Whilst internal messages are generally secure (e.g. within organisations), those sent to external addresses are not considered secure enough for personal information.

Personal information must be sent by other methods, some of which are outlined in this section.

When sending **personal information** via email, you must:

- ensure all recipients need to receive the information - think twice before responding to a group email or copying others in;
- confirm the name, department and email address of the recipient;
- use a flag to mark the message 'confidential';
- do not include personal or confidential information in the subject field;
- ask the recipient to confirm receipt of the email;
  If sending any email to multiple recipients, consider using blind copy facility so recipients can't view other recipients' email addresses (which, depending on the subject of the email, could constitute personal information)

Using password protected files

Password protection and encryption are not necessary for information shared between staff within a secure platform (e.g. within the school) or where secure email is used.

If you have to send personal information to an external recipient you must:

- contain it within a password protected file.
- remember to use a different password to anything you may use for other tasks because you will have to share the password when you disclose the document.
- always save the password protected version of the document as a new file and retain the original safely. IT Services will not be able to open password protected or encrypted documents without the password.
- Do not send the password in the same email - preferably ask the recipient to confirm receipt of the information and then send the password in the reply to that email. Or give the password over the telephone.
- Record what information has been sent on the individual's file.

DRAFT

-

- After receiving a password protected file, re-save the information without the password in a new secure place. Do not rely on remembering the password.

Save an audit trail of your email communications. This could mean saving a copy of all sent and received emails in a separate folder.

Sending information by Secure Mail

When sharing information with other organisations, there are some secure methods available – for example Egress Switch and the S2S system.

The S2S system allows schools and local authorities to securely share information, for example to:

- transfer pupil records using the common transfer file protocol (CTF)
- update pupil details with the Learning Records Service (LRS)
- apply for and receive pupil unique learning numbers
- send and receive messages to and from other users within the S2S network.

To send information to another school or local authority, you must:

- use the CTF naming protocols
- save the data in an encrypted folder or file
- send the file as a compressed folder

Full instructions for saving, uploading and receiving files via S2S can be found in the guides for schools and local authorities.

DRAFT

In Person

Personal or confidential information may be delivered personally by members of staff. Such information may be held in paper or electronic form. Where laptops, mobile or other electronic devices are used precautions must be taken to ensure the security of systems as well as any data held on the device itself.

Personal information should only be taken off site where necessary, either in accordance with local policy or with the agreement of your line manager.

Staff must:

- Log any personal information you are taking off site and the reason why.
- Paper based personal information must be transported in a lockable box, sealed file or envelope.
- Electronic information must be protected by appropriate electronic security measures – password or encryption.
- If transferring personal information by car put the information in the boot and lock it, but DO NOT leave in the car overnight
- Ensure the information is returned back on site as soon as possible.
- Record that the information has been returned.

5. Use of Personal Devices

Where personal devices, such as laptops or tablets, are used to access personal data belonging to the Trust that data must be stored remotely on either:

- A secure cloud service; or
- A separate server within your IT network, accessible remotely through a virtual private network (VPN)

Storing data remotely allows you to:

- Update data whenever needed, rather than running the risk of copies of it becoming out of date or inaccurate over time
- Delete data when needed, to ensure it isn't retained on any devices for longer than necessary
- Restrict access when a staff member leaves the school or should no longer have access to the data
- Respond more quickly to subject access request and freedom of information requests

Staff must ensure that:

DRAFT

- Two-factor authentication is turned on. This is where, in addition to a username and password, something that only the user has is needed to log in. This could be a code sent via text or a further password
- Strong passwords are used and that these passwords are not stored or saved on your device. Strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special keyboard characters (e.g. an asterisk or currency symbols).
- Documents with personal data are password protected.
- Make and save changes in the remote version of any document containing personal data, do not make copies of data.
- Devices automatically lock if left inactive for a period of time
- Do not share any devices that store personal data among family or friends
- Set the operating system of the device to receive automatic updates. Downloading the latest 'patches' or security updates should cover vulnerabilities.

If personal data is stored on a device, or likely to be, the hard drive must be encrypted. Encryption means the data is converted into a code, and can only be converted back using 'the key' (such as a password). Only users with the key will be able to read it. This means that if the device is lost or stolen, someone cannot access the files stored on its hard drive by attaching the drive to a new device.

Automated back-up

Some devices may offer an automated back-up facility, where a back-up of data on the device is kept on a cloud-based account. You should ensure that, if this facility is enabled, the cloud-based service is secure and the back-up will not lead to data security issues.

6. Information Security Breaches

The Information Commissioners Office (ICO) has the power to issue monetary penalty notices of up to €20 million (or 4% of total worldwide annual turnover, whichever is higher) for serious breaches of the General Data Protection Regulation.

If despite the security measures you take to protect the personal information you hold a breach of security occurs, you must report it IMMEDIATELY to the KCSP Data Protection Officer, Michelle Boniface (dpo@kcsp.org.uk or 01622 232662 or 07718 424788).

The breach may arise from a theft, a deliberate attack on your systems, from the unauthorised use of personal information by a member of staff, or from accidental loss or equipment failure. However the breach occurs, **all staff have a responsibility to report it immediately**.

DRAFT