VERSION 1

# Kington St Michael CE Primary School
# Secure Data Handling Policy

**This policy should be read and understood in conjunction with the following policies and guidance:**

- The Data Protection Act 1998
- Becta: Information Risk Management and Protective Marking
- Information Sharing: Guidance for Practitioners and Managers HM Govt. Oct 2008
- Records Management Society – Tool Kit for Schools

**Principles**

Colleagues within schools have increasing access to a wide range of sensitive information[1]. There are generally two types of sensitive information; personal data concerning the staff and pupils and commercially sensitive financial data. It is important to ensure that both types of information are managed in a secure way at all times.

Personal data is the most likely form of sensitive data that a school will hold. Personal data is defined by the Data Protection Act as ***"Data relating to a living individual who can be identified from the data"*.** The Act gives 8 principles to bear in mind when dealing with such information. Data must:

1. be processed fairly and lawfully
2. be collected for a specified purpose and not used for anything incompatible with that purpose
3. be adequate, relevant and not excessive
4. be accurate and up-to-date
5. not be kept longer than necessary
6. be processed in accordance with the rights of the data subject
7. be kept securely
8. not be transferred outside the EEA (European Economic Area) unless the country offers adequate protection.

The Data Protection Act states that some types of personal information demand an even higher level of protection, this includes information relating to:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual life (orientation)
- the commission or alleged commission by them of any offence, or any proceedings for such or the sentence of any court in such proceedings.

The three questions below can be used to quickly assess whether information needs to be treated securely, i.e.

1. Would disclosure / loss place anyone at risk?
2. Would disclosure / loss cause embarrassment to an individual or the school?
3. Would disclosure / loss have legal or financial implications?

If the answer to any of the above is "yes" then it will contain personal or commercially sensitive information and needs a level of protection. (A more detailed assessment guide is contained with Appendix A).

[1] The terms, "Information" and "data" are treated as the same for the purposes of this policy.

## Procedures and practice

The following practices will be applied within the school:

- The amount of data held by the school should be reduced to a minimum.
- Data held by the school must be routinely assessed to consider whether it still needs to be kept or not.
- Personal data held by the school will be securely stored and sent by secure means.

## Auditing

The school must be aware of **all** the sensitive data it holds, be it electronic or paper.

- A register (Appendix B) will be kept detailing the types of sensitive data held, where and by whom, and will be added to as and when new data is generated.
- How long these documents need to be kept will be assessed using the Records Management Toolkit.
- Audits will take place in line with the timetable. (Appendix C).

This register will be sent to all staff each year to allow colleagues to revise the list of types of data that they hold and manage.

The audit will be completed by a member of staff responsible for data protection.

## Risk assessment

If it has not already been undertaken, the school will carry out a risk assessment to establish what security measures are already in place and whether or not they are the most appropriate and cost effective available.

Carrying out a risk assessment will generally involve:

- How sensitive is the data?
- What is the likelihood of it falling into the wrong hands?
- What would be the impact of the above?
- Does anything further need to be done to reduce the likelihood?

Once the risk assessment has been completed, the school can decide how to reduce any risks or whether they are at an acceptable level.

Risk assessment will be an on-going process and the school will have to carry out assessments at regular intervals as risks change over time.

## Securing and handling data held by the school

The school will encrypt[2] any data that is determined to be personal or commercially sensitive in nature. This includes fixed computers, laptops and memory sticks.

Staff should **not** remove or copy sensitive data from the organisation or authorised premises unless the media is:

- encrypted,
- is transported securely
- will be stored in a secure location.

This type of data should not be transmitted in unsecured emails (e.g. pupil names and addresses, performance reviews etc).

Data transfer should be through secure websites e.g. S2S, SecureNet Plus, common transfer files and school census data. If this is not available then the file must be minimally password protected

[2] Encryption of computers and memory sticks can be provided by the school's technical support. Guidance is available from http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

or preferably encrypted[3] before sending via email, the password must be sent by other means and on no account included in the same email. A record of the email should be kept, to identify when and to whom the email was sent, (e.g. by copying and pasting the email into a Word document).

Data (pupil records, SEN data, contact details, assessment information) will be backed up, encrypted and stored in a secure place – e.g. locked filing cabinet / fire safe / remote backup.

All staff computers will be used in accordance with the Teacher Laptop Policy (Appendix C)

When laptops are passed on or re-issued, data will be securely wiped from any hard drive before the next person uses it (not simply deleted). This will be done by a technician using a recognised tool, e.g. McAfee Shredder.

The school's wireless network (WiFi) will be secure at all times[4].

The school will identify which members of staff are responsible for data protection. The school will ensure that staff who are responsible for sets of information, such as SEN, medical, vulnerable learners, management data etc. know what data is held, who has access to it, how it is retained and disposed of. Appendix B details which members of staff are responsible for which data. This is shared with all staff concerned within the school.

Where a member of the school has access to data remotely (e.g. SIMS from home), remote access off the school site to any personal data should be over an encrypted connection (e.g. VPN) protected by a username/ID and password. **This information must not be stored on a personal (home) computer.**

Members of staff (e.g. senior administrators) who are given full, unrestricted access to an organisation's management information system should do so over an encrypted connection and use two-factor authentication, which is available to SIMS users from Capita. **This information must not be stored on a personal (home) computer.**

The school will keep necessary pupil and staff information in accordance with the Records Management Society's guidance (see references at the end of this document).

The school should securely delete commercially sensitive or personal data when it is no longer required as per the Records Management Society's guidance.

All staff will be trained to understand the need to handle data securely and the responsibilities incumbent on them this will be the responsibility of the headteacher.

When sensitive data is to be sent out of the school it must be done in a secure way. The Information About Children Education and schools (ICES) March Bulletin (no 41) contains a number of useful guidance sections and appendices that cover the issues of Information Sharing and details of how to securely transfer data between schools, LA and Government departments[5].

[3] The ICES bulletin has a useful guide explaining how WINZIP a free application can be used to encrypt files that need to be sent either through S2S, SecureNet or email: http://www.teachernet.gov.uk/_doc/14782/ICES%20Bulletin%20-%20issue%2041%20v1-0Final.pdf

[4] The school will use WPA2 (or WPA if WPA2 is not available). The older standard WEP will not be used.

[5] http://www.teachernet.gov.uk/_doc/14782/ICES%20Bulletin%20-%20issue%2041%20v1-0Final.pdf

**APPENDIX A:** Help sheet for assessing risk of sharing information

In deciding the most appropriate way to share information and the level of security required, you must always take into consideration the nature of the information and the urgency of the situation, i.e. take a risk based approach to determining appropriate measures.

The simplified process described below will help organisations to choose the appropriate level of security to consider when emailing information.

**Step 1**

Imagine a potential security breach (e.g. a confidential letter is left in a public area, a memory stick is lost or someone reads information on a computer screen while waiting to meet a member of staff), and consider:

1 Will it affect or identify any member of the school or community?
2 Will someone lose / be out of pocket by / more than £100?
3 Will it cause any kind of criminal case to fail?
4 Is there a risk of discomfort / slur upon professional character of someone?
5 Is anyone's personal safety at risk?
6 Will it embarrass anyone?

If you answered **NO** to all the questions, the document does not contain sensitive information. If you answered yes to any of the questions, the document with include some sensitive information and therefore requires a level of protection.

**Step 2**

Imagine the same potential security breach as above, and consider:

7 Will it affect many members of the school or local community and need extra resources locally to manage it?
8 Will an individual or someone who does business with the school lose / be out of pocket by £1,000 to £10,000?
9 Will a serious criminal case or prosecution fail?
10 Is someone's personal safety at a moderate risk?
11 Will someone lose his or her professional reputation?
12 Will a company or organisation that works with the school lose £100,000 to £1,000,000?

If you have answered **yes** to any of the above questions the document contains sensitive information and additional security should be considered, such as, password protecting the document before you email it to a colleague outside of your organisation. Further information about how to achieve this can be found on the ICES bulletin (number 41)[6].

However, if you think that the potential impact exceeds that stated in the question (for example, someone's personal safety is at high risk) think very carefully before you release this information.

**Step 3**

All documents that do not fit into steps 1 or 2 might require a higher level of protection / security; organisations should err on the side of caution.

[6] http://www.teachernet.gov.uk/_doc/14782/ICES%20Bulletin%20-%20issue%2041%20v1-0Final.pdf

## Appendix B: Register of sensitive data held by the school

| Type of data | Held on | Period to be retained | Type of protection | Who can access the data |
|---|---|---|---|---|
| Pupil SEN data | SENCO laptop | | Data is encrypted on laptop | SENCO and Headteacher |

## Appendix C: Timetable for Information Security Management

| Activity | Frequency | Lead |
|---|---|---|
| Audit of data held | Annually | Head and admin officer |
| Encrypting sensitive data | On-going | All staff |
| Reviewing data backup procedures | Annual | Admin officer |
| Identifying staff responsible for data security and keep log of names and roles. | Annual | Head |
| Wiping of laptop data when re-issued | Annual and then when necessary. | ICT Technician |
| Wiping of laptop data when discarded | As necessary | ICT Technician |

## Local Authority to update when appropriate

## Appendix D

**This policy is reviewed every two years or as necessary**

# Staff Computer Use Policy

- Passwords that I use to access school systems will be kept secure and secret – if I have reason to believe that my password is no longer secure I will change it.
- I acknowledge that the computer provided for me to use remains the property of the school and should only be used for school business.
- I will not access the files of others or attempt to alter the computer settings.
- I will not update web content or use pictures or text that can identify the school, without the permission of the Headteacher.
- I will not alter, attempt to repair or interfere with the components, software or peripherals of any computer that is the property of the school. I will seek permission with the school's technician / Network Manager should I need to install additional software.
- I will always adhere to the copyright.
- I will always log off the system when I have finished working.
- I understand that the school may, in line with South West Grid for Learning, monitor the Internet sites I visit.
- I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Network Manager / school technician / headteacher.
- Any e-mail messages I send will not damage the reputation of the school.
- All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be forwarded.
- I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material[7].
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Storage of e-mails and attachments should be kept to a minimum to avoid unnecessary drain on memory and capacity.
- I understand that I am responsible for the safety of school data that I use or access.
- In order to maintain the security of data I will take the following steps:
    - I will store data files in my user area only for as long as is necessary for me to carry out my professional duties.
    - I will not save data files to a PC or laptop other than that provided by the school.
    - If I need to transfer sensitive data files and no secure electronic option is available I will only do so using the encrypted USB key provided by the school.
    - Sensitive data will only be sent electronically through a secure method, e.g. SecureNet Plus. If this is not available then the minimum requirement is to password protect the document before attaching it to email.

7 Legislative guidance is available from the Internet Watch Foundation: http://www.iwf.org.uk/police/page.22.htm

Sensitive data includes:

- Pupil reports
- SEN records
- Letters to parents
- Class based assessments
- Exam results
- Whole school data
- Medical information
- Information relating to staff, e.g. Performance Management reviews.

If I am in any doubt as to the sensitivity of data I am using, I will consider these questions:

- Would disclosure / loss place anyone at risk?
- Would disclosure / loss cause embarrassment to an individual or the school?
- Would disclosure / loss have legal or financial implications?

If the answer to any of these questions is yes, then the data should be treated as sensitive.

I understand that if I do not adhere to these rules outlined in this policy, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow including notification to professional bodies where a professional is required to register. If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may be reference for investigation by the Police and could recorded on any future Criminal Record Bureau checks.

Name…….

Date……..