Amesbury CE Primary School

Secure Data Handling Policy for Amesbury Primary School

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 treated securely, i.e.

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

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).

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 will be aware of **all** the sensitive data it holds, be it electronic or paper.

- All details of auditing of sensitive information are stored within the Business Manager's data protection file. Any audits will be completed by the member of staff responsible for data protection.

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

[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

protected 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. safe / fire safe / remote backup.

All staff computers will be used in accordance with the Online Safety Policy and Staff usage Policy.

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.

---

[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.

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].

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

References:

The Data Protection Act 1998:
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

Becta: Data handling security guidance for schools
http://schools.becta.org.uk/index.php?catcode=ss_lv_saf_dp_03&rid=14734&section=lv

Information Commissioner's Office
www.ico.gov.uk

Information Sharing: Guidance for Practitioners and Managers HM Govt. Oct 2008
http://publications.everychildmatters.gov.uk/default.aspx?PageFunction=productdetails&PageMode=publications&ProductId=DCSF-00807-2008&

Records Management Society – Tool Kit for Schools:
http://www.rms-gb.org.uk/resources/848

Date produced: September 2015

Date of review: September 2017

Agreed by the governing body

Date ……

Signed ……