St Mary's C of E Primary School

Data Protection Policy (including data security)

Reviewed by Governors: November 2016

1. Introduction and Scope

1.1 The Data Protection Act 1998 is the law that protects personal privacy and applies to any school which processes or has access to people's personal data. The Act helps ensure that the management of data held electronically and / or and in paper-based systems is processed correctly. Section 7 of the Act gives rights to the people about who the data relates.

1.2 Our school has a legal responsibility to comply with the Data Protection Act and the school, as a corporate body, is named as the 'Data Controller' under the Act. Data controllers are people / organisations who hold and process personal data and have a duty to establish workplace practices and policies that are in line with the Act.

2. Personal data

2.1 Personal data is any information which relates to a living individual who can be identified from that data either by itself or alongside any other information we hold (for example, name, address, date of birth, National Insurance number, bank account details etc). It also includes any expression of opinion about that individual and any indication of any intentions we have in respect of that individual and it also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

2.2 Personal data can also be 'sensitive' as defined by the Act. This is information about your racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, criminal offences, proceedings and convictions. We can only collect and hold this information for specific purposes (for example equal opportunities monitoring).

2.3 We are obligated to notify the Information Commissioner, who regulates the Data Protection Act, that information about individuals is being collected, processed and held. We are also obligated to follow the eight principles set out in the Act. The principles state that all personal information, or data, about individuals should be:

i. Processed fairly and lawfully

Either consent is required or there is an overriding necessity to process data however in any event, individuals should be made fully aware of why we are collecting their information, what we intend using it for, and who else we may be sharing it with.

ii. Processed for limited purposes
We will only process the information we've collected for the purposes we said we would when it was collected.

iii. Adequate, relevant and not excessive
We will only collect and process the information we need as opposed to any additional information that may be useful in the future for another purpose.

iv. Accurate and up to date
We will regularly review the information we hold to ensure that personal data is kept up to date.

v. Kept no longer than is necessary
Depending on the overriding need of any legislation, statutory or legal requirement, data will not be kept longer than is required for the purposes of processing.

vi. Processed in line with the individual's rights
The Data Protection Act creates rights for those individuals who have their data processed and responsibilities for our school which processes and records that data.

vii. Secure
We must ensure that appropriate measures have been taken to ensure your information is safe, secure and cannot be accessed by anyone that isn't authorised to do so.

viii. Not transferred to other countries that don't have suitable data protection controls.
We will not send personal information outside of the European Economic Area unless the individual whom it is about has consented or adequate protection is in place.

3. Information disclosure

3.1 Personal information cannot usually be released to anyone else without your consent or knowledge. There are, however, certain circumstances when a third party (such as a government agency or law enforcement agency) can request information about you and we may be obliged to disclose it to them (for example where the disclosure is required by law or by a court order).

3.2 If you ask for information about a person other than yourself, your request will likely be refused unless the person you are asking about has given their written consent allowing us to disclose their personal information to you.

4. Requesting Personal Data

4.1 To request access to personal data that the school may hold about you, a Subject Access Form can be completed and posted to us.

4.2 The person who the personal data is about is known as the *data subject* and the person who is making the request is known as the *applicant.* These can of course be the same person depending on the personal data sought. A common example of this relationship would be when a parent (*applicant*) is seeking personal information about their child (*data subject*).

4.3 Parents can generally request personal data about their child without their consent, however it should be noted that the Data Protection Act requires a data controller to assess the maturity and competency of a data subject which is not restricted to age. Therefore in some cases, consent of the child may still be required. There may also be occasions where someone is legally allowed to act on behalf of someone else (for example power of attorney).

4.4 A form to assist you making a request is available from the school office.

4.5 To protect your personal data when processing a request, we will also require copies of two forms of identification. These should be:

- one piece of photographic identification, such as a valid passport, valid driving licence or a valid EU national identity card.
- one piece of identification confirming your address and dated within the last three months such as a utility bill, council tax statement or bank statement.

4.6 If you do not want to post your application, you may book an appointment with the Head of School, who will accept your application and validate your identification. Whilst we may be able to confirm your identification in person, should you require any personal data be posted to you, we will always require proof of address to ensure that any data that we release is sent securely and to the correct address.

4.7 Remember that if you are applying on someone else's behalf, you must also enclose either their signed, written consent, or proof that you are legally entitled to act on their behalf.

4.8 There is also a £10 processing fee. Cheques and postal orders should be made payable to the school. Please note that in some very exceptional circumstances (for example the type and volume of manual files requested) there may be an additional fee required and we will advise you if this is the case.

4.9 Following receipt of your written request, identification and fee, you will receive a response within 40 days. However if we do not have enough information required to perform a search we will contact you and ask for more details (The 40 day period of response will begin from the day we receive sufficient information to enable a search).

4.10 The unlawful obtaining or disclosure of personal data without consent of the Data Controller is an offence under Section 55 of the Data Protection Act 1998.

5. Disclosing information

5.1 The information that you can expect to receive from us will usually be a copy in whatever format we hold it in.

5.2 Depending on what information has been requested we will explain any jargon or abbreviations, provide a summary sheet detailing what we have used the information for, and what information we have withheld and why (if applicable).

5.3 As per the Data Protection Act 1998, there are some instances where we may not be able to release some of the information we hold about you to you such as:

- personal information about other people (including family members), unless we receive their consent
- examination marks ahead of national release or examiners comments
- information provided by another person, such as a health visitor or the police, unless we receive their permission to do so
- information contained in adoption and parental order records
- legal advice provided by a legal professional
- information that would prejudice the prevention / detection of crime

5.4 In some exceptional circumstances we may also withhold information about you if we think that it might cause you serious harm or severe distress.

5.5 Occasionally your records may contain elements that it would not be appropriate for you to see (for example personal information about other individuals). Rather than withhold the whole record or document, we will redact or remove those sections, if we can, to make them anonymous

5.6 If you find incorrect information held about you then please write and tell us what is wrong and how you think it should be corrected. An assessment will be made and the information may be updated. Sometimes it may not be possible to amend historic information if it were key to decision making at the time.

6. Education Records

6.1 A parent has rights to their child's educational record under the Education (Pupil Information) (England) Regulations 2005.

6.2 Information kept by a teacher solely for their own use does not form part of the official educational record.

6.3 An education record will primarily consist of information that comes from a teacher or other employee of a local authority or school, the pupil or their parents (such as details of achievement and attainment). However, it may also include information from the child and their parents (such as information about the health of the child or correspondence from an educational psychologist).

6.4 To access your child's school records, you should submit your request in writing to the Head of School and we have a requirement to respond within 15 school days.

6.5 Whilst simply viewing an educational record is free of charge, if we receive a request from a parent who wants copy of their child's educational record then a fee may be charged at our discretion. This can range from £1.00 up to £50 for the reproduction of paper work depending on the volume or how many copies are produced.

6.6 Additionally it may not be possible for a parent to simply view the record if personal data subject to the Data Protection Act 1998 is contained within. If this is the case, this information will be disclosed with regards to the principles and requirements of the Data Protection Act 1998 and in line with those timescales as outlined in section 1 – 5 above.

Data Protection / Security

1. Scope

1.1 The Data Protection Act 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data. This policy does not seek to re write the legislation, rather to familiarise individuals with the key provisions and to demonstrate that our school has a commitment to them.

1.2 This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1.3 This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the school from time to time. Any failures to follow the policy may result in disciplinary proceedings.

1.4 The school processes a large amount of personal data such as staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection etc. In addition, the school may be required by law to collect and use certain types of information to comply with statutory obligations of the local authority, government agencies or other bodies.

1.5 Personal data is any information which relates to a living individual who can be identified from that data either by itself or alongside any other information we hold (for example, name, address, date of birth, National Insurance number, bank account details etc) and it also includes any expression of opinion about that individual and any indication of any intentions we have in respect of that individual. Personal data can also be held visually or as sound recordings (e.g. this includes but is not limited to CCTV recordings, photographs, video clips, smart / mobile phones, tablets, cameras and other portable media devices).

2. School Responsibilities

2.1 As per the Data Protection Act 1998 and as corporate body, the school is the Data Controller of the personal data it processes and Governors are therefore ultimately responsible for ensuring the school's compliance, however designated officers will deal with day to day matters.

2.2 Our school will ensure that all personal data is accessible only to those who have a valid reason for using it and not disclosed to any unauthorised third parties. Any member of staff, parent or other individual who considers that the policy has not been followed in respect of personal data should raise the matter with the appropriate designated officer.

2.3 The School has two designated officers and they are

The Head of School

The Executive Headteacher

2.4 In addition the school will put in place appropriate measures for the deletion of personal data. Manual records will be shredded or disposed of as '*confidential waste'*, CDs / DVDs / Disks should be cut into pieces, Audio / Video Tapes and (where applicable) Fax rolls should be dismantled / shredded. Hard drives of redundant PCs will be wiped clean before disposal, or, if that is not possible, destroyed physically.

2.5 Appropriate contract terms will be put in place with any third parties undertaking this work on the schools behalf.

2.6 The Freedom of Information Act 2000 requires that a log should be kept of the records destroyed and who authorised their destruction.

3. Staff Responsibilities

3.1 All members of staff are responsible for ensuring that:-

3.1.1 Any personal data which they hold is kept securely.

3.1.2 Any information provided to the school in connection with their employment is accurate and up to date including informing of any changes to information which has been provided (for example changes of address) or any errors spotted.

3.1.3 Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party. (Unauthorised disclosure may result in disciplinary proceedings)

3.1.4 Any personal data held about other people or collected as part of their responsibilities (for example opinions on reports, references, marks, details of personal circumstances) is kept securely.

3.1.5 Personal data that is written, printed or in electronic format held on an unencrypted disk, USB / portable data transfer device or other removable storage media should be kept in a locked filing cabinet, locked drawer, safe or in a lockable room with key-controlled access. Records containing personal data must never be left where unauthorised personnel can read or gain access to them.

3.1.6 Personal data that is computerised should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up.

3.1.7 Computer screens, terminals, CCTV camera screens or any Visual Display Unit (VDU) that shows personal data should be placed so that they are not visible except to authorised staff. PC screens will not be left unattended without a password protected screen saver being used.

3.2 This policy also applies to staff and pupils who process personal data 'off-site' (for example when working at home). Staff are still responsible in such circumstances and additional care must be taken regarding the security of the data. Any personal data, in any format, will not be taken off the school premises without approval of the Head of School.

3.3 Under the Data Protection Act 1998 any employee may be personally liable in a court of law for unauthorised disclosure of personal data.

3.4 It is also a criminal offence to gain access to unauthorised information on a computer system under the Computer Misuse Act 1990.

4. Closed Circuit Television

4.1 Our school uses Closed Circuit Television (CCTV) and complies with the Information Commissioner's CCTV Code of Practice.

4.2 As a data controller our school must let people know we are using CCTV. This is achieved by signs around the premises which are clearly visible and readable.

4.3 CCTV will only be used be in areas where privacy is normally expected in exceptional circumstances (such as in changing rooms or toilets), and will only be used to deal with very serious concerns. If this is the case, extra effort will be made to ensure that you are aware that cameras are in use.

4.4 We will make sure that someone at the school has responsibility for the CCTV images, deciding what is recorded, how images should be used and clear procedures on how to use the system. Regular checks will be made to ensure that the procedures are followed.

4.5 We will only keep the images for as long as necessary to meet the purpose of recording them.

4.6 Any disclosure of images will be in line with the Data Protection Act 1998 including any requests for personal data. Any such requests will be processed in line with our data protection policy however in addition to those requirements we will likely require details which will assist us establish your identity as the person in the pictures, and to help find the images on their system if they are still retained.

4.7 Our school may need to disclose CCTV images for legal reasons (for example to the police for crime detection or at the behest of a court order). Once we have given the images to another organisation, then that organisation must also adhere to the Data Protection Act 1998 in their handling of the images. We will not disclose images of identifiable people to the media or post them on the internet. Images released to the media to help identify any person are usually disclosed by the police.

5 Reviewing and disposing of records

5.1 Most expired records would be disposed of confidentially. These records must be kept secure until it has been destroyed. Confidential waste sacks are available by contacting the Head of School.

5.2.1 Personal and sensitive personal data stored on computers or computer media, such as USB keys, CDs, cannot be securely removed by simple deletion or reformatting. The school IT Helpdesk at Camden LA would be contacted to ensure the safe disposal of these devices.

6 Data Security Breach Management

6.1 Appropriate measures are taken against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data by the school. In the event of a data security breach for the following reasons (*this is by no means an exhaustive list):*

• Loss or theft of data or equipment on which data is stored on school premises or outside
• Inappropriate access controls allowing unauthorised use
• Equipment failure
• Human error - correspondence with personal data sent to the wrong email address
• Unforeseen circumstances such as a fire or flood
• Hacking attack
• ‘Blagging’ offences where information is obtained by deceit from the school

6.2 The school will follow the following steps if a data security:

1. **Containment and recovery**

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- Where appropriate, inform the police

Assessment of ongoing risk

The following points are also likely to be helpful in making this assessment:

- What type of data is involved – staff or pupil sensitive personal data
- Where personal data has been lost or stolen, are there any protections in place such as encryption?
- How many staff and/or pupils personal data are affected by the breach?
- What harm can be done to these individuals – risks to physical safety, reputation etc.

2. **Notification of breach**

The Information Commissioner (ICO) believes serious breaches should be brought to the attention of his Office. The school's notification to the ICO would include a description of how and when the breach occurred and what data was involved. It will also include details of what have been done to respond to the risks posed by the breach.

3. **Evaluation and response**

It is important the school investigates the causes of the breach and also evaluate the effectiveness of our response to it. If necessary, the school would update its policies and procedures accordingly.