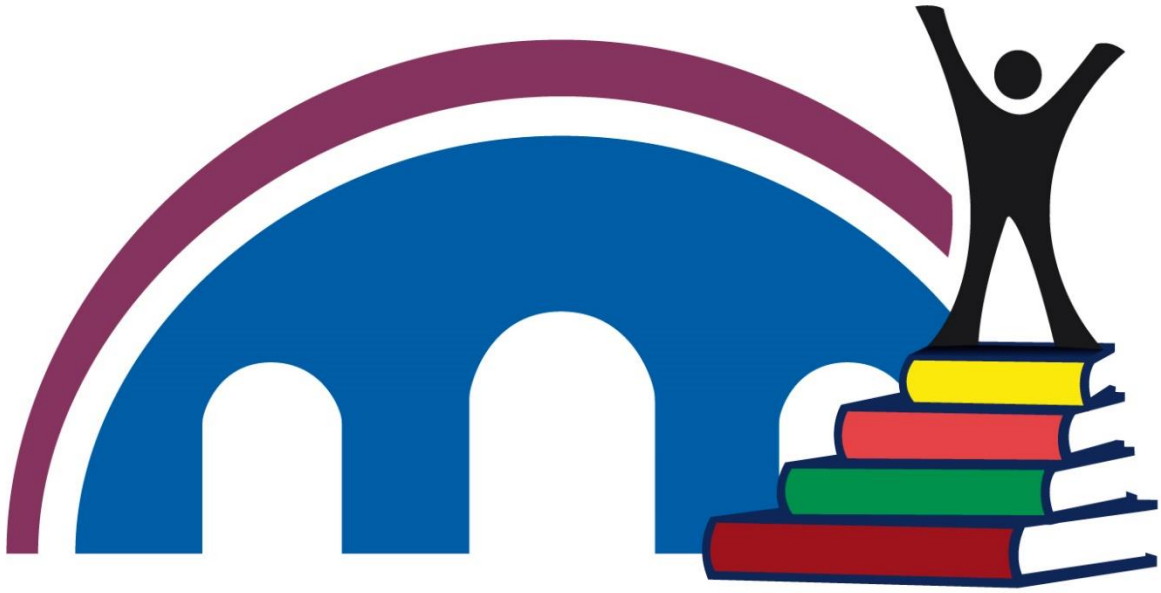

Bridge Academy Trust

DATA PROTECTION

June 2017

Date of Draft Policy:	June 2017	
Consultation with Staff Required	No	
Period of Consultation (if required)	From NA	To NA
Governing Body Committee Reviewing Document:	Policy Review committee 6th June 2017	
Date of FGB Meeting at which Policy Approved (if required)	NA	
Date of Adoption of Policy	7th June 2017	
Date Policy available on Central Area/www (if appropriate)		

Changes

NONE

Contents

DATA PROTECTION BASICS

1.1. The Data Protection Act 1988 establishes a framework of rights and duties that are designed to safeguard personal data. This framework balances the legitimate needs of an organisation to collect and use personal data against the right of individuals to respect for privacy of their personal details.

1.2. The Act applies to the particular activity of processing personal data. Failure to notify the Information Commissioner that the school is processing personal data would constitute a criminal offence. Notifying the ICO ensures transparency and openness as it is a basic principle of data protection that the public should know (or be able to find out) who is processing personal data and why this is being carried out.

1.3. Personal data refers to data that relates to a living individual who can be identified from the data or from the data and information that is in the possession of, or is likely to come into the possession of, the data controller. It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Where the ability to identify an individual depends partly on the data and partly on other information (not necessarily data), the data held will still be 'personal data'.

1.4. Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

1.4.1. organisation, adaptation or alteration of the information or data;

1.4.2. retrieval, consultation or use of the information or data;

1.4.3. disclosure of the information or data by transmission, dissemination or otherwise making available; or

1.4.4. alignment, combination, blocking, erasure or destruction of the information or data.

1.5. The definition of processing is very wide and it is unlikely that anything the school might do with data will not be processing.

1.6. Moulsham High School collects and uses personal information about staff, students, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

1.7. The school has a duty to be registered, as Data Controller, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are available on the ICO's website and will be updated when, and if, the school introduces any new purposes for processing information (e.g. installing CCTV). The school also has a duty to issue a Fair Processing Notice to all students/parents that summarises the information held on students, why it is held and the other parties to whom it may be passed on to.

1.8. Data Controllers determine the purposes for which, and the manner in which, any personal data are, or are to be, processed. Data controllers must ensure that any processing of personal data for which they are responsible complies with the Data Protection Act (DPA) – failure to do so risks enforcement action, prosecution, or compensation claims from individuals.

PURPOSE

2.1. This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

2.2. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

WHAT IS PERSONAL DATA?

3.1. Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. Greater legal restrictions are imposed on sensitive personal data.

3.2. Under the DPA, and other regulating acts, access to their own personal information is a statutory right for students. Parents (as defined in the Education Act 1996) may also request access to their child's personal data. School staff have a right of access to personal data on themselves.

3.3. The DPA covers four types of information that it refers to as data:

3.3..1. Information processed or intended to be processed, wholly or partly, by automatic means – i.e. information in electronic form, usually on computer.

3.3..2. Information processed in non-automated manner which forms part of, or is intended to form part of, a filing system – e.g. paper records in a filing system.

3.3..3. Information that forms part of an 'accessible record', e.g. educational records, regardless of whether the information is processed automatically or is held in a relevant filing system.

3.3..4. Information held by a public authority.

3.4. An expression of opinion about an individual is classed as their personal data and when recording information about an individual the school will record whether it is an opinion and, where appropriate, whose opinion it is.

3.5. The following questions will help determine whether the data held is 'personal data' for the purposes of the DPA.

3.6. **Can a living individual be identified from the data, or, from the data and other information in your possession, or likely to come into your possession?**

An individual is 'identified' if you have distinguished that individual from other members of a group. In most cases an individual's name together with some other information will be sufficient to identify them. Simply because you do not know the name of an individual does not mean you cannot identify that individual.

3.7. **Does the data 'relate to' the identifiable living individual, whether in personal or family life, business or profession?**

Data that identifies an individual, even without a name associated with it, may be personal data where it is processed to learn or record something about that individual, or where the processing of that information has an impact upon that individual. Therefore, data may 'relate to' an individual in several different ways.

3.8. **Is the data 'obviously about' a particular individual?**

Data 'obviously about' an individual will include medical history, criminal record, record of work, or achievements in a sporting activity.

3.9. **Is the data 'linked to' an individual so that it provides particular information about that individual?**

3.10. **Is the data used, or is to be used, to inform or influence actions or decisions affecting an identifiable individual?**

3.11. **Does the data have any biographical significance in relation to the individual?**

When considering 'biographical significance', what is important is whether the data goes beyond recording the individual's casual connection with a matter or event which has no personal connotations for him/her.

3.12. **Does the data focus or concentrate on the individual as its central theme rather than on some other person, or some object, transaction or event?**

It may be helpful to consider whether the information is being processed to record something about an individual or to record information about an object. Where information is linked to an individual is the key factor in determining whether information about an object is personal data.

3.13. **Does the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?**

Even though the data is not usually processed by the data controller to provide information about an individual, if there is a reasonable chance that the data will be processed for that purpose, the data will be personal data.

ROLES & RESPONSIBILITIES

4.1. The Business Manager is the named Data Protection Officer.

4.2. The Network Manager if responsible for the network security and is a Data Protection Champion along with the Logistics Manager, Office Manager/Headteacher's PA and the Deputy Business Manager.

4.3. All staff members, including members of the school governing body, will receive training in their responsibilities under the Data Protection Act as part of their HR induction.

4.4. Staff members and parents are responsible for checking that any information they provide to the school/academy in connection with their employment or in regard to a registered student is accurate and up to date.

4.5. The school/academy cannot be held accountable for any errors unless the employee or parent has informed the school / academy about such changes.

4.6. All the principles in this document apply to all staff and governors of Moulsham High School.

THE 8 DATA PROTECTION PRINCIPLES

5.1. The DPA establishes eight enforceable principles that must be adhered to at all times. The main purpose of the principles is to protect the interests of the individuals whose personal data is being processed. They apply to everything that is done with personal data, except where exemptions apply. The eight data principles are the key to striking the correct balance

in processing information so that the individual's privacy is respected where it needs protection and at the same time complying with the DPA.

PRINCIPLE 1

5.2. **Personal data shall be processed fairly and lawfully.**

5.2.1. The school must:

5.2.1.1. have legitimate reasons for collecting and using the personal data;

5.1.2.2. not use the data in ways that have unjustified adverse effects on the individuals concerned;

5.1.2.3. be open and honest (transparent) about how it intends to use the data, and give individuals appropriate privacy notices when collecting their personal data;

5.1.2.4. handle people's personal data only in ways they could reasonably expect; and

5.1.2.5. make sure that it does not do anything unlawful with the data.

Fairly

5.2.2. Processing personal data must above all else be fair, as well as satisfying the relevant conditions for processing. If any aspect of processing is unfair, there will be a breach of the first data protection principle, even if it can be shown that one or more of the conditions for processing have been met.

5.2.3. Fairness generally requires transparency, i.e. being clear and open with individuals about how their information will be used. Assessing whether information is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived or misled when the information is obtained, then this is unlikely to be fair.

5.2.4. The Data Protection Act states that information should be treated as being obtained fairly if it is provided by a person who is legally authorised, or required, to provide it.

5.2.5. Why and how personal data is collected and used will be relevant in assessing fairness. The school will make sure:

5.2.5.1. it is open and honest about its identity;

5.2.5.2. it tells people how it intends to use any personal data collected (unless this is obvious);

5.2.5.3. it usually handles personal data only in ways that would be reasonably expected; and

5.2.5.4. above all, it does not use information in ways that unjustifiably have a negative effect on the individuals concerned.

5.2.6. A decision to share personal data with another organisation does not take away the school's duty to treat individuals fairly. Before sharing personal data, the school will consider carefully what the recipient will do with it and what the effect on individuals is likely to be.

5.2.7. The school will control access to personal information, giving access only to people (staff and governors) who need particular information when doing their jobs, and only when they need it. This covers access to written and electronic staff and student records, and recorded CCTV images. Systems and procedures will be put in place to control access to paper and electronic records containing personal information. To ensure compliance, and as an important aspect of good information governance, the school will also monitor its controls.

Lawfully

5.2.8. The term lawful refers to statute and to common law, whether criminal or civil. An unlawful act may be committed by a public or private-sector organisation. If processing personal data involves committing a criminal offence, the processing will obviously be unlawful. However, processing may also be unlawful if it results in:

5.2.8.1. a breach of a duty of confidence;

5.2.8.2. the school exceeding its legal powers or exercising these powers improperly;

5.2.8.3. an infringement of copyright;

5.2.8.4. a breach of an enforceable contractual agreement;

5.2.8.5. a breach of industry-specific legislation or regulations;

5.2.8.6. a breach of the Human Right Act 1998 – the Act implements the European Convention on Human Rights, which gives individuals the right to respect for private and family life, home and correspondence.

PRINCIPLE 2

5.3. **Personal data shall be obtained only for one or more specified and lawful purposes.**

5.3.1. The school must:

5.3.1.1. be clear from the outset about why it is collecting personal data and what it intends to do with it;

5.3.1.2. comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;

5.3.1.3. comply with what the Act says about notifying the Information Commissioner; and

5.3.1.4. ensure that if it wishes to use or disclose the personal data for any purpose that is additional to, or different from, the originally specified purpose, the new use or disclosure is fair.

PRINCIPLE 3

5.4. **Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**

5.4.1. The school will ensure:

5.4.1.1. it holds personal data about an individual that is sufficient for the purpose it is holding it for in relation to that individual; and

5.4.1.2. it does not hold more information than is needed for that purpose.

5.4.2. The school will identify the minimum amount of personal data needed to properly fulfil its purpose and will hold that much information and no more. The data held will not include irrelevant details. This is part of the practice known as 'data minimisation'. Personal data should not be held on the off-chance that it might be useful in the future; however, it is permissible to hold information for a foreseeable event that may never occur, e.g. information needed in case of accident.

5.4.3. The school will take into account that the right amount of personal data may differ from one individual to another and where sensitive personal data is concerned will only collect or retain the minimum amount of information needed.

PRINCIPLE 4

5.5. **Personal data shall be accurate and, where necessary, kept up to date.**

5.5.1. The law recognises that it may not be practical to double-check the accuracy of every item of personal data received so the DPA makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties.

5.5.2. The school will:

5.5.2.1. take reasonable steps to ensure the accuracy of any personal data obtained;

5.5.2.2. ensure that the source of any personal data is clear;

5.5.2.3. carefully consider any challenges to the accuracy of the information; and

5.5.2.4. consider whether it is necessary to update the information.

5.5.3. The DPA does not define the word "accurate", but does say that personal data is inaccurate if it is incorrect or misleading as to any matter of fact. It is acceptable to keep records of events that happened in error, provided the records are not misleading about the facts – a note will be added to clarify if a mistake has happened.

5.5.4. If information is used for a purpose that relies on it remaining current, it should be kept up to date, for example employee payroll records should be updated when there is a pay rise. Where information is held only for statistical, historical or other research reasons, updating the information might defeat the purpose of holding it.

5.5.5. It may be impractical to check the accuracy of personal data someone else has provided. The school will not be considered to have breached the fourth data protection principle provided:

5.5.5.1. it has accurately recorded information provided by the individual concerned, or by another individual or organisation;

5.5.5.2. has taken reasonable steps in the circumstances to ensure the accuracy of the information; and

5.5.5.3. where an individual has challenged the accuracy of the information, this is clear to those accessing it.

5.5.6. In some circumstances it will be necessary to double-check information especially if inaccurate information could have serious consequences or if common sense suggests there may be a mistake. If an individual challenges the accuracy of the information held about him/her, the school will consider whether the information is accurate and, if it is not, will delete or correct it – in some circumstances it may be necessary for the individual concerned to provide convincing documentary evidence or the school may need to make its own checks. Where the accuracy of a record has been challenged by the individual it relates to, the school will mark the record as being in dispute until it is satisfied that the record is correct.

PRINCIPLE 5

5.6. **Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.**

5.6.1. The Data Protection Act does not set out any specific minimum or maximum periods for retaining personal data. In practice, the school will:

5.6.1.1. review the length of time it keeps personal data;

5.6.1.2. consider the purpose or purposes for holding the information when deciding whether (and for how long) to retain it;

5.6.1.3. securely delete information that is no longer needed for this purpose or these purposes; and

5.6.1.4. update, archive or securely delete information if it goes out of date.

5.6.2. Personal data held for longer than necessary will, by definition, be excessive and may also be irrelevant.

5.6.3. The school will regularly review the personal data it holds and delete anything no longer needed. Information that does not need to be accessed regularly, but which still needs to be retained, will be safely archived or put offline.

5.6.4. The retention period will depend on:

5.6.4.1. what the information is used for;

5.6.4.2. the surrounding circumstances;

5.6.4.3. any legal or regulatory requirements;

5.6.4.4. agreed industry practices.

5.6.5. At the end of the agreed retention period, or the life of a particular record, personal data will be reviewed and deleted, unless there is some special reason for keeping it. Records will be archived (rather than deleted) if the school still needs to hold it and the school will be prepared to give subject access to it, and to comply with the data protection principles. If it is appropriate to delete a record from a live system, it should also be deleted from any back-up of the information on the system.

5.6.6. School records for a student will be kept for 7 years after the student leaves the school, or until the student reaches 25 years of age (whichever is the greater) and examination records the same.

5.6.7. Employment records form part of a staff member's permanent record and will be retained for 7 years after the member of staff leaves the school. Interview records, CVs and application forms for unsuccessful applicants will be kept for 6 months.

5.6.8. All formal complaints made to the Headteacher or Governors will be kept for at least 7 years in confidential files, with any documents on the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection and to legal professional privilege in the event of a court case.

PRINCIPLE 6

5.7. **Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.**

5.7.1. The rights of individuals are:

5.7.1.1. a right of access to a copy of the information comprised in their personal data;

5.7.1.2. a right to object to processing that is likely to cause, or is causing, damage or distress;

5.7.1.3. a right to prevent processing for direct marketing;

5.7.1.4. a right to object to decisions being taken by an automated means;

5.7.1.5. a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;

5.7.1.6. a right to claim compensation for damages caused by a breach of the Data Protection Act.

PRINCIPLE 7

5.8. **Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

5.8.1. The school will ensure that it has appropriate security to prevent the personal data it holds being accidentally or deliberately compromised. It will:

5.8.1.1. design and organise its security to fit the nature of the personal data it holds and the harm that may result from a security breach;

5.8.1.2. be clear about who within the school is responsible for ensuring information security;

5.8.1.3. make sure it has the right physical and technical security, backed up by robust policies and reliable well-trained staff; and

5.8.1.4. be ready to respond to any breach of security swiftly and effectively.

5.8.2. The seventh data protection principle relates to the security of every aspect of the processing of personal data. The school will seek to ensure that:

5.8.2.1. only authorised people can access, alter, disclose or destroy personal data;

5.8.2.2. those people only act within the scope of their authority; and

5.8.2.3. if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

5.8.3. The school's security will be appropriate to:

5.8.3.1. the nature of the information in question; and

5.8.3.2. the harm that might result from it improper use, or from it accidental loss or destruction.

5.8.4. The school will regularly review security arrangements as technology advances and choose the appropriate level of security based on the risks. The information risk will be determined by reviewing the personal data held and the way it is used in order to assess how valuable, sensitive or confidential it is and what damage or distress could be caused to individuals if there were a security breach. The risk assessment should take account of factors such as:

5.8.4.1. the nature and extent of the school's premises and computer systems;

5.8.4.2. the number of staff;

5.8.4.3. the extent of their access to personal data; and

5.8.4.4. personal data held by a third party on its behalf.

5.8.5. Management and organisation security measures are likely to be equally important to physical and technological security in protecting personal data. The school will need to take account of:

5.8.5.1. coordination between key people in the organisation;

5.8.5.2. access to premises or equipment given to anyone outside the organisation and the additional security considerations this will generate;

5.8.5.3. business continuity arrangements that identify how to protect and recover any personal data the organisation holds; and

5.8.5.4. periodic checks to ensure that the organisation's security measures remain appropriate and up-to-date.

5.8.5.5. The school will put procedures in place to monitor when any personal information that could be considered in any way private or confidential is taken from the school premises in electronic or paper format.

Staff

5.8.6. It is essential that staff understand the importance of protecting personal data, that they are familiar with the school's security policy, and that they put the school's security procedures into practice. The school will provide appropriate initial training and refresher training that will cover:

5.8.6.1. the school's duties under the Data Protection Act and restrictions on the use of personal data;

5.8.6.2. the responsibilities of individual staff members for protecting personal data, including the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, information without authority;

5.8.6.3. the proper procedures to identify callers;

5.8.6.4. the dangers of people trying to obtain personal data by deception or by persuading staff to alter information when they should not do so; and

5.8.6.5. any restrictions the school places on the personal use of its computers by staff.

Physical Security

5.8.7. Physical security includes:

5.8.7.1. the quality of doors and locks;

5.8.7.2. whether premises are protected by alarms, security lighting or CCTV;

5.8.7.3. how the school controls access to premises;

5.8.7.4. how the school supervises visitors;

5.8.7.5. how the school disposes of waste paper; and

5.8.7.6. how the school keeps portable equipment secure.

5.8.8. Whenever possible, storage rooms, strong cabinets and other storage systems with locks will be used to store paper records. Papers containing confidential personal information should not be left on office and classroom desks, on staff room tables, or pinned to noticeboards where there is general access. Particular care should be taken if documents have to be taken out of school.

Computer Security

5.8.9. The school will consider the following guiding principles when deciding the technical side of information security:

5.8.9.1. computer security is appropriate to the size and use of the school's systems;

5.8.9.2. technological developments are taken into account (consideration will be given to costs when deciding what security measures to take).

5.8.10. All portable electronic devices will be kept as securely as possible on and off school premises. If they contain personal information, they should be kept under lock and key when not in use (this is a legal requirement if they hold personal information that could be considered confidential).

5.8.11. Strong passwords (i.e. at least eight characters long and containing special symbols) should be encouraged if any electronic equipment holds confidential personal information and, if possible, the school will set up a regular prompt to change passwords and use different passwords for separate systems and devices.

5.8.12. Encryption software will be used to protect all portable devices and removable media, such as laptops and USB devices (or another form of memory storage not part of the computer itself), which hold confidential personal information. This is particularly important if information is to be taken from school premises and to prevent access to information in cases where equipment is stolen. The school will ensure that solutions stay up to date and meet generally accepted standards. Where laptops containing

personal information have been stolen from workplaces, vehicles and houses, or left in public places and encryption software has not been used to protect the data, enforcement action by the Information Commissioner will usually follow.

5.8.13. If any of the school's personal information is held on private equipment and there is a breach of security from this equipment, the school will remain responsible unless it can prove it did everything reasonably possible to keep the information secure.

PRINCIPLE 8

5.9. **Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

5.9.1. Principle 8 will apply if a student's family moves outside the European Economic Area. Other principles of the Data Protection Act will also usually be relevant when sending personal data overseas.

5.9.2. Before making a transfer, the school will consider whether it can achieve the aims without actually processing personal data. The eighth principle will only apply if the information is moved to a country, rather than simply passing through on route to its destination. For a list of countries with adequate protection visit

http://www.ico.org.uk/for_organisations/data_protection/the_guide/principle_8#eea-countries.

(Although the USA is not included in the European Commission list, the Commission considers that personal data sent to the US under the "Safe Harbor" scheme is adequately protected)

5.9.3. Posting personal data on a website will often result in transfers to countries outside the EEA and consideration should be given to the likelihood that a transfer may take place and whether that would be fair for the individuals concerned. If it is intended that information on the website will be accessed outside the EEA then this is a transfer.

5.9.4. Before transferring data, the school will consider:

5.9.4.1. the nature of the personal data being transferred;

5.9.4.2. how the data will be used and for how long; and

5.9.4.3. the laws and practices of the country the data is being transferred to.

5.9.5. The school will decide whether there is enough protection for individuals in all the circumstances of the transfer by completing an assessment of adequacy that will look at:

5.9.5.1. the extent to which the country has adopted data protection standards in its laws;

5.9.5.2. whether there is a way to make sure the standards are achieved in practice; and

5.9.5.3. whether there is an effective procedure for individuals to enforce their rights or get compensation if things go wrong.

5.9.6. The Information Commissioner has the power to authorise transfers of personal data, but will only such authorise one-off arrangements in exceptional circumstances having satisfied itself that there is no other reasonable way for the school to comply with the eighth principle.

5.9.7. There are exemptions from the eighth principle, but the school will always ensure that there is adequate protection if it is possible to do so and will only rely on an exemption if it is not.

5.9.8. The school can transfer personal data overseas if it has the individual's consent, which should be given clearly and freely and may later be withdrawn by the individual. A consent will not be valid if the individual has no choice but to give his/her consent.

The individual must know and have understood what he/she is agreeing to. The school will specify the reasons for the transfer and, as far as possible, the countries involved, informing the individual of any particular risks involved in the transfer that it is aware of.

GENERAL STATEMENT

5.10. The school is committed to maintaining the above principles at all times. Therefore the school will:

5.10.1. Inform individuals why the information is being collected when it is collected.

5.10.2. Inform individuals when their information is shared, and why and with whom it was shared.

5.10.3. Check the quality and the accuracy of the information it holds.

5.10.4. Ensure that information is not retained for longer than is necessary.

5.10.5. Ensure that when obsolete information is destroyed that it is done so appropriately and securely.

5.10.6. Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.

5.10.7. Share information with others only when it is legally appropriate to do so.

5.10.8. Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests.

5.10.9. Ensure staff are aware of and understand the policies and procedures.

THE CONDITIONS FOR PROCESSING

6.1. Processing personal data covers collecting, storing, accessing, changing and even destroying any personal information about an individual.

6.2. The conditions for processing take account of the nature of the personal data in question. Being able to satisfy a condition for processing will not on its own guarantee that the processing is fair and lawful – fairness and legality must be looked at separately and the school will ensure that what it wants to do with personal data is fair and lawful before considering the conditions for processing set out in the DPA.

6.3. At least one of the following conditions must be met whenever personal data is processed (unless a relevant exemption applies – see Appendix 2).

6.3.1. The individual who the personal data is about has consented to the processing.

6.3.2. The processing is necessary:

6.3.2.1. in relation to a contract which the individual has entered into; or

6.3.2.2. because the individual has asked for something to be done so they can enter into a contract.

6.3.3. The processing is necessary because of a legal obligation that applies (except an obligation imposed by a contract).

6.3.4. The processing is necessary to protect the individual's "vital interests".

6.3.5. The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.

6.3.6. The processing is in accordance with the "legitimate interests" condition.

6.4. In the case of sensitive personal data, at least one of several other conditions must also be met.

6.4.1. The individual who the sensitive personal data is about has given explicit consent to the processing.

6.4.2. The processing is necessary so that the school can comply with employment law.

6.4.3. The processing is necessary to protect the vital interests of:

6.4.3.1. the individual (in a case where the individual's consent cannot be given or reasonably obtained), or

6.4.3.2. another person (in a case where the individual's consent has been unreasonably withheld).

6.4.4. The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents.

6.4.5. The individual has deliberately made the information public.

6.4.6. The processing is necessary in relation to legal proceedings, for obtaining legal advice, or otherwise for establishing, exercising or defending legal rights.

6.4.7. The processing is necessary for administering justice, or for exercising statutory or governmental functions.

6.4.8. The processing is necessary for medical purposes and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.

6.4.9. The processing is necessary for monitoring equality of opportunity and is carried out with appropriate safeguards for the rights of individuals.

6.5. A full list of the regulations for processing sensitive personal data for a range of other purposes, typically those that are in the substantial public interest and which must necessarily be carried out without the explicit consent of the individual, is set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000 and subsequent orders.

CONSENT

6.6. One of the conditions for processing is that the individual has consented to their personal data being collected and used in the manner and for the purpose in question. The school should not infer consent if an individual does not respond to a communication. Consent must also be appropriate to the age and capacity of the individual.

6.7. In most cases consent will last for as long as the processing to which it relates continues, but the individual may be able to withdraw consent depending on the nature of the consent given and the circumstances in which the personal data is collected or used. Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given. If the school intends to continue to hold or use personal data after its relationship with an individual has ended then the consent should cover this.

6.8. The school should review whether a consent that has been given remains adequate as its relationship with the individual develops or as the individual's circumstances change.

6.9. Consent should cover the specific processing details, the type of information (or even the specific information), the purposes of the processing, and any special aspects that may affect the individual such as any disclosures that may be made.

6.10. A particular consent may not be adequate to satisfy the condition for processing and the school should not rely exclusively on consent to legitimise its processing, but should concentrate on making sure that individuals are treated fairly – each condition of processing provides an equally valid basis for processing personal data.

DISPOSAL OF DATA

6.11. The Data Protection Act 1998 does not provide any specific guidance on how to dispose of personal data, but disposal is a form of processing that needs to be done fairly and in line with the first and seventh principles.

6.12. When disposing of records in any form, the school will consider the nature of the information and the harm that may result from its unauthorised use. The method of destruction of personal data should take into account the nature of the information and, in all cases, the school will ensure that data is disposed of in a way that creates little risk of an unauthorised third party using it to the data subject's detriment. If confidential information is held on paper records, they will be shredded or pulped; electronic memories will be scrubbed clean or destroyed.

6.13. The ultimate responsibility for safely disposing of all electronic and paper records lies with the school.

SUBJECT ACCESS REQUEST

7.1. The DPA gives individuals the right of access to their personal data through a subject access request. The school will respond to a valid subject access request (SAR) within 40 calendar days of receiving it (see Appendix 1). The definition of personal data for this purpose extends to any personal information held on record anywhere in the school (with one or two exceptions – see Appendix 2) and not just that held electronically, in structured files and in educational records – this includes information in correspondence and in notes made by Governors, teachers and other staff.

7.2. A student can request access to his/her own data. The request is not charged and does not have to be in writing. Staff will judge whether the request is in the student's best interests and that the student will understand the information provided. Consideration will also be given as to whether the request has been made under coercion.

7.3. A parent can request access to, or a copy of, their child's school records and other information held about their child. The request must be made in writing. There is no charge for such requests on behalf of the child, but there may be a charge for photocopying records (see Appendix 1). Staff will check that no other legal obstruction (e.g. a court order limiting an individual's exercise of parental responsibility) is in force. Parents should be aware that all rights to do with information about their child rest with the child as soon as they are old enough to understand these rights – this will vary from one child to another, but, as a broad guide, it is reckoned that most children will have a sufficient understanding by the age of 12. Parents are encouraged to discuss and explain any request for information with their child if they are aged 12 or over.

(NB: The Education (Pupil Information)(England) Regulations 2005 provide a student's parents [regardless of the age of the student] with the right to view, or have a copy of, their child's educational record at the school. Parents who wish to exercise this right must apply to the school in writing.)

7.4. For educational records (unlike other personal data) access must be provided within 15 school days and if copies are requested these must be supplied within 15 days of payment.

7.5. A member of staff can request access to his/her own records at no charge, but the request must be made in writing. The member of staff has the right to see his/her own records and to ask for copies. There is no charge for copies of staff records.

7.6. All requests for personal information will be acknowledged in writing on receipt and access to records will be arranged as soon as possible. If awaiting third party consents, the school will

arrange access to those documents already available and notify the individual that other documents may be made available later.

7.7. The school will document all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes (e.g. letter requesting changes).

SHARING PERSONAL INFORMATION

8.1. Sharing personal information involves providing it to another organisation or person so that they can make use of it. It does not extend to the use of personal information within the school, including use by the governing body.

8.2. Personal data and school records about students are confidential to the child. The information can be shared appropriately within the professional working of the school to enable the school to make the best educational provision for its students. The law permits such information to be shared with other educational establishments when students change schools.

8.3. Data on staff is sensitive information and confidential to the individual and is shared, where appropriate, at the discretion of the Headteacher and with the knowledge, and if possible the agreement, of the member of staff concerned.

8.4. The main organisations that the school will share personal data with are:

8.4.1. local authorities;

8.4.2. other schools and educational bodies; and

8.4.3. social services.

8.5. Personal information can be shared with students once they are old enough to be considered responsible for their own affairs, although information can also be shared with their parents or guardians. Students old enough to make decisions for themselves are entitled to have their personal information handled in accordance with their rights under the DPA rather than the rights of their parents acting on their behalf. If information is shared with parents, sharing must be in line with the data protection principles.

8.6. The three most important aspects the school will consider when sharing data are:

8.6.1. making sure it is allowed to share it;

8.6.2. ensuring that adequate security (taking into account the nature of the information) is in place to protect it; and

8.6.3. providing an outline in a fair processing notice of who receives personal information form the school.

8.7. The school will consider how the personal information is provided. When sending by e-mail, the school will check that the recipient's arrangements are secure enough before sending the message and, if necessary, password-protect the details and send the password separately. Staff should check (and check again) that the message is being sent to the correct e-mail address and that they are sending only the information that needs to be sent. Similar consideration applies when sending confidential information by fax – staff must make sure it goes to the right recipient and is not left unattended on their equipment for others to see.

8.8. Secure methods, such as S2S, should be used when sharing information with other organisations.

8.9. When sharing paper copies of personal data, or providing it on disk or memory stick, the school will make every effort to minimise the risk of loss and will use appropriate systems to track packages to ensure they reach the intended recipient.

DATA SECURITY BREACH MANAGEMENT

9.1. The school will take appropriate measures against unauthorised or unlawful processing and against accidental lost, destruction or damage to personal data.

9.2. A data security breach can happen for a number of reasons:

9.2.1. Loss or theft of data or equipment on which data is stored.

9.2.2. Inappropriate access controls allowing unauthorised use.

9.2.3. Equipment failure.

9.2.4. Human error.

9.2.5. Unforeseen circumstances, such as fire or flood.

9.2.6. Hacking attack.

9.2.7. 'Blagging' offences where information is obtained by deceiving the organisation that holds it.

CONTAINMENT AND RECOVERY

9.3. Following a data security breach, the school will make an initial response to investigate and contain the situation and will then instigate a recovery plan, including, where necessary, damage limitation. This may involve specialists such as IT, HR and legal and, in some cases, contact with external stakeholder and suppliers. The school will:

9.3.1. Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.

9.3.2. 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.

9.3.3. Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause.

9.3.4. Where appropriate, inform the Police.

ASSESSING THE RISKS

9.4. Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Whilst these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of a database. Before deciding on what steps are necessary for immediate containment, the school will assess the risks that may be associated with the breach, including assessment of potential adverse consequence for individuals, how serious or substantial these are and how likely they are to happen again.

NOTIFICATION OF BREACHES

9.5. Informing people of a data security breach is an important element of the school's breach management strategy, but is not an end in itself. Notification will have a clear purpose to enable individuals who may have been affected to take steps to protect themselves, or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal

with complaints. Not every incident will warrant notification and in deciding whether to notify the school will consider:

9.5.1. If there are any legal or contractual requirements.

9.5.2. If notification would help meet security obligations with regard to Data Protection Principle 7.

9.5.3. If notification would help the individual, bearing in mind that he/she could act on the information provided to mitigate risks.

9.5.4. Whether the ICO should be informed as a large number of people are affected or there are serious consequences.

9.5.5. How notification can be made appropriate for particular groups of individuals, e.g. children or vulnerable adults.

9.5.6. The dangers of 'over notifying'.

9.6. Where notification is warranted, the school will decide who to notify, which people will be told and how the message will be communicated. This will depend on the nature of the breach and will take into consideration:

9.6.1. Requirement to notify the appropriate regulatory body.

9.6.2. The most appropriate way to notify those affected, bearing in mind the security of the medium as well as the urgency of the situation.

9.6.3. Inclusion of a description of how and when the breach occurred and what data was involved, as well as details of what has already been done to respond to the risks posed by the breach.

9.6.4. Specific and clear advice on the steps that should be taken for individuals to protect themselves and how the school is willing to help them.

9.6.5. Contact details for further information or to ask questions about what has occurred.

9.7. When notifying the ICO the school will provide details of the security measures in place, such as encryption, and, where appropriate, the security procedures in place at the time the breach occurred. The ICO will also be informed if the media are aware of the breach.

EVALUATION AND RESPONSE

9.8. It is important to not only investigate the causes of the breach, but also to evaluate the effectiveness of the school's response. Existing procedures could lead to another breach and the school will need to identify where improvements can be made.

COMPLAINTS

10.1. Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

10.2. Many data protection failures are caused by ignorance and the school will, therefore, promote awareness of information rights. Information governance is not optional and, as electronic systems become more complex, capable and extensive, it is increasingly important for staff to know how to safeguard the personal information they process.

REVIEW

11.1. This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years. The policy review will be undertaken by the Headteacher, or nominated representative.

CONTACTS

12.1. If you have any enquires in relation to this policy, please contact the headteacher who will also act as the contact point for any subject access requests.

12.2. Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113 or 01625 545745 between 9.00am and 5.00pm.

APPENDIX 1 – PROCEDURES FOR RESPONDING TO SUBJECT ACCESS REQUESTS MADE UNDER THE DATA PROTECTION ACT 1998

RIGHTS OF ACCESS TO INFORMATION

There are two distinct rights of access to information held by schools about students.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Student Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

ACTIONING A SUBJECT ACCESS REQUEST

1. Requests for information must be made in writing, including e-mail, and be addressed to The headteacher). If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
   - passport
   - driving licence
   - utility bills with the current address
   - Birth / Marriage certificate
   - P45/P60
   - credit card or mortgage statement

   (this list is not exhaustive)

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher, or his representative, should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for his/her records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependent upon the following:
   - should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.
   - should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
   - of the information requested it is only the educational record viewing that will be free, but a charge, not exceeding the cost of copying the information, can be made by the Headteacher.

5. The response time for subject access requests, once officially received, is 40 days (not working or school days but calendar days, irrespective of school holiday periods). However the 40 days will not commence until after receipt of fees or clarification of information sought. **NB:** For educational records (unlike personal data) access must be provided within 15 school days.

6. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40-day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the student or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

INFORMATION HELD ABOUT STUDENTS BY SCHOOLS

A student, or someone acting on his/her behalf, may make a SAR in respect of personal data held about the student by a school. If the school is in England, Wales or Northern Ireland, the SAR should be dealt with by the school. If the school is in Scotland, the SAR should be dealt with by the relevant education authority or the proprietor of an independent school.

There are two distinct rights to information held about students by schools. They are:

- the student's right of subject access under the DPA; and
- the parent's right of access to their child's 'educational record' (this right of access is only relevant to maintained schools – not independent schools, English academies or free schools).

Although this code is only concerned with the right of subject access, it is important to understand what is meant by a student's 'educational record'. This is because there is an overlap between the two rights mentioned above, and also because 'educational record' is relevant when ascertaining the fee you may charge for responding to a SAR.

Unlike the distinct right of access to the educational record, the right to make a SAR is the student's right. Parents are only entitled to access information about their child by making a SAR if the child is unable to act on his/her own behalf or has given his/her consent. If it is not clear whether a requester has parental responsibility for the child or is acting on their behalf, the school should clarify this before responding to the SAR.

In deciding what information to supply in response to a SAR, the school will need to have regard to the general principles about exemptions from subject access (see Appendix 2).

If a SAR is made for information containing, in whole or in part, a student's 'educational record', a response must be provided within 15 school days (if the school is in England, Wales or Northern Ireland). The maximum amount you may charge for dealing with the request depends on the number of pages of information to be supplied. The following table shows the maximum fees.

Number of pages of information supplied	**Maximum fee**
1-19	£1
20-29	£2
30-39	£3
40-49	£4
50-59	£5
60-59	£6
70-79	£7
80-89	£8
90-99	£9
100-149	£10
150-199	£15
200-249	£20
250-299	£25
300-349	£30
350-399	£35
400-449	£40
450-499	£45
500+	£50

If the SAR does not relate to any information that forms part of the educational record, then the usual 40-day time limit for responding applies. The maximum fee for dealing with the request is £10.

COMPLAINTS

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

CONTACTS

If you have any queries or concerns regarding this policy or the procedures then please contact Mr. M. Farmer, Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113 or 01625 545745 between 9.00am and 5.00pm.

APPENDIX 2 – EXEMPTIONS AND RESTRICTIONS

The Data Protection Act 1998 (DPA) recognises that in some circumstances the school might have a legitimate reason for not complying with a subject access request (SAR), so it provides a number of exemptions from the duty to do so. Where an exemption applies to the facts of a particular request, the school may refuse to provide all or some of the information requested, depending on the circumstances. It is a matter for the school to decide whether or not to use an exemption – the DPA does not oblige the school to do so, so it is free to comply with a SAR even if it could use an exemption.

Certain restrictions (similar to exemptions) are also built into the DPA's subject access provisions. For example, there are restrictions on the disclosure of personal data about more than one individual in response to a SAR.

Not all of the exemptions apply in the same way, and the school should look at each exemption carefully to see how it applies in a particular SAR. Some exemptions apply because of the nature of the personal data in question, e.g. information contained in a confidential reference. Others apply because disclosure of the information would be likely to prejudice a particular function of the organisation to which the request is made. The DPA does not explain what is meant by 'likely to prejudice', however, the Information Commissioner's view is that it requires there to be a substantial chance (rather than a mere risk) that complying with the SAR would noticeably damage the discharge of the function concerned.

If challenged, the school must be prepared to defend to the Information Commissioner's Office or a court its decision to apply an exemption. It is therefore good practice to ensure that such a decision is taken at a suitably senior level in the school organisation and that the school documents the reasons for it.

CONFIDENTIAL REFERENCES

The school may give or receive references about an individual, e.g. in connection with his/her employment, or for educational purposes. Such references are often given 'in confidence', but that fact alone does not mean the personal data included in the reference is exempt from subject access. The DPA distinguishes between references the school gives and references it receives.

References the school gives are exempt from subject access if they are given in confidence and for the purposes of an individual's education, training or employment or the provision of a service by them. There is no such exemption for references received from a third party. If the school receives a SAR relating to such a reference, it must apply the usual principles about subject access to decide whether to provide some or all of the information contained in the reference.

It may be difficult to disclose the whole of a reference to the individual it relates to without disclosing some personal data about the author of the reference – most obviously, their identity. If the reference was not provided in confidence, this difficulty should not prevent disclosure. However, if a question of confidentiality arises, the school should contact the author to find out whether they object to the reference being disclosed and, if so, why. Even if the provider of a reference objects to its disclosure in response to a SAR, the school will need to supply the personal data it contains to the requester if it is reasonable to do so in all the circumstances. The school will, therefore, need to weigh the referee's interest in having their comments treated confidentially against the requester's interest in seeing what has been said about them.

Relevant considerations are likely to include:

- any clearly stated assurance of confidentiality given to the referee;
- any reasons the referee gives for withholding consent;
- the likely impact of the reference on the requester;

- the requester's interest in being able to satisfy himself or herself that the reference is truthful and accurate; and
- any risk that disclosure may pose to the referee.

INFORMATION HELD BY SCHOOLS

The statutory definition of 'educational record' differs between England and Wales, Scotland and Northern Ireland. Broadly speaking, however, the expression has a wide meaning and includes most information about current and past students that is processed by or on behalf of a school. However, information kept by a teacher solely for their own use does not form part of the educational record. It is likely that most of the personal information a school holds about a particular student will form part of the student's educational record. However, it is possible that some of the information could fall outside the educational record, e.g. information about the student provided by the parent of another child is not part of the educational record.

Examples of information which (depending on the circumstances) it might be appropriate to withhold include:

- information that might cause serious harm to the physical or mental health of the student or another individual;
- information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- information contained in adoption and parental order records; and
- certain information given to a court in proceedings concerning the child.

INFORMATION ABOUT EXAMINATIONS

Special rules apply to SARs relating to information about the outcome of academic, professional or other examinations. These rules, which apply to requests for examination scripts, marks or markers' comments, are designed to prevent the right of subject access being used as a means of circumventing an examination body's processes for announcing results.

Information comprising the answers given by a candidate during an examination are exempt from the right of subject access. So a SAR cannot be used to obtain a copy of an individual's examination script. Although this exemption does not extend to an examiner's comments on a candidate's performance in an examination (whether those comments are marked on the examination script or recorded on a separate marking sheet), or to details of the marks awarded, there is a special rule governing the time limit for responding to a SAR for such information in cases where the SAR is made before the results are announced. In such cases, a response must be provided within the earlier of:

- five months of the date of the request; and
- 40 days of the date on which the results are announced.

Where a SAR is made for an individual's examination marks, a response may only be refused (or delayed) for reasons permitted by the DPA. So it would not be appropriate to refuse to provide details of examination marks in response to a SAR because the requester had failed to pay their tuition fees. Clearly, though, providing information about examination results is not the same as conferring a qualification.

PUBLICLY AVAILABLE INFORMATION

If an enactment requires an organisation to make information available to the public, any personal data included in it is exempt from the right of subject access. The exemption only applies to the information that the organisation is required to publish. If it holds additional personal data about an individual, the additional data is not exempt from the right of subject access even if the organisation publishes it.

CRIME AND TAXATION

Personal data processed for certain purposes related to crime and taxation is exempt from the right of subject access. These purposes are:

- the prevention or detection of crime;
- the capture or prosecution of offenders; and
- the assessment or collection of tax or duty.

However, the exemption applies, in any particular case, only to the extent that complying with a SAR would be likely to prejudice the crime and taxation purposes set out above.

Personal data that:

- is processed for the purpose of discharging statutory functions; and
- consists of information obtained for this purpose from someone who held it for any of the crime and taxation purposes described above

is also exempt from the right of subject access to the extent that providing subject access to the personal data would be likely to prejudice any of the crime and taxation purposes. This prevents the right applying to personal data that is passed to statutory review bodies by law-enforcement agencies and ensures that the exemption is not lost when the information is disclosed during a review.

MANAGEMENT INFORMATION

An exemption applies to personal data that is processed for management forecasting or management planning. Such data is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the business or other activity of the organisation.

NEGOTIATIONS WITH THE REQUESTER

Personal data that consists of a record of the school's intentions in negotiations with an individual is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the negotiations.

REGULATORY ACTIVITY

Organisations may use an exemption from subject access if they perform regulatory activities. The exemption is not available to all organisations, but only to those that have regulatory functions concerning the protection of the public or charities, or fair competition in business. Organisations that do have such functions may only apply the exemption to personal data processed for these core regulatory activities and then only to the extent that granting subject access to the information concerned would be likely to prejudice the proper discharge of those functions. For more detailed guidance on how this exemption applies, see ICO guidance on regulatory activity.

LEGAL ADVICE AND PROCEEDINGS

Personal data is also exempt from the right of subject access if it consists of information for which legal professional privilege (or its Scottish equivalent, ‘confidentiality in communications’) could be claimed in legal proceedings.

The English law concept of legal professional privilege encompasses both ‘legal advice’ privilege and ‘litigation’ privilege. In broad terms, the former applies only to confidential communications between client and professional legal adviser, and the latter applies to confidential communications between client, professional legal adviser or a third party, but only where litigation is contemplated or in progress.

Where legal professional privilege cannot be claimed, the school may not refuse to supply information in response to a SAR simply because the information is requested in connection with actual or potential legal proceedings. The DPA contains no exemption for such information; indeed, it says the right of subject access overrides any other legal rule that limits disclosure. In addition, there is nothing in the Act that limits the purposes for which a SAR may be made, or which requires the requester to tell you what they want the information for.

The Information Commissioner recognises that:

- the courts have discretion as to whether or not to order compliance with a SAR; and
- if a court believes that the disclosure of information in connection with legal proceedings should, more appropriately, be determined by the Civil Procedure Rules (the courts' rules on disclosure), it may refuse to order personal data to be disclosed.

Nevertheless, simply because a court may choose not to order the disclosure of an individual's personal data does not mean that, in the absence of a relevant exemption, the DPA does not require the school to disclose it. It simply means that the individual may not be able to enlist the court's support to enforce his or her right.

SOCIAL WORK RECORDS

Special rules apply where providing subject access to information about social services and related activities would be likely to prejudice the carrying out of social work by causing serious harm to the physical or mental health or condition of the requester or any other person. These rules are set out in the *Data Protection (Subject Access Modification) (Social Work) Order 2000 (SI 2000/415).* Their effect is to exempt personal data processed for these purposes from subject access to the extent that its disclosure would be likely to cause such harm.

A further exemption from subject access to social work records applies when a SAR is made by a third party who has a right to make the request on behalf of the individual, such as the parent of a child or someone appointed to manage the affairs of an individual who lacks capacity. In these circumstances, personal data is exempt from subject access if the individual has made clear they do not want it disclosed to that third party.