THE STONEHENGE SCHOOL
Data Protection Policy

A Statutory Policy

INTRODUCTION

1. The policy for data protection is to comply with the Data Protection Act. The main elements of the Act which are of relevance to schools are summarised below. This summary should be sufficient for most but, if there is any doubt, the *Data Controller* is to be consulted.

DEFINITION OF DATA

2. **General.** The Act regulates the use of "personal data". This is defined in the Sub-paragraphs below. Data means information which is:

a. Being or may be in the future processed by equipment (eg a computer).

b. Recorded for, or in the future for, a filing system that is structured so that record relating to individuals (such as personnel records) are held in a sufficiently systematic way as to allow ready access to specific information about those individuals.

c. A health record of information about the physical or mental health or condition of an individual,

c. An educational record of information about a pupil.

d. Any recorded information held by a public authority eg a school.

f. An accessible public record that consists of information held by a local authority for housing or social services purposes.

3. **Personal Data.** Personal data means data which relate to a living individual who can be identified from the data (a 'data subject') or from those data and other information which 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 any person in respect of the individual.

4. **Sensitive Personal Data.** Sensitive personal data means personal data consisting of information on a data subject as to:

a. Racial or ethnic origin.

b. Political opinions.

c. Religious beliefs or other beliefs of a similar nature.

d. Membership of a trade union (within the meaning of the Trade Union and Labour
Relations (Consolidation) Act 1992).

e. Physical or mental health or condition.

f. Sexual life.

g. The commission or alleged commission of any offence.

h. Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

5. **Other Definitions.** Other definitions are at Annex A and words/ phrases that are in italics are there defined.

THE EIGHT DATA PROTECTION PRINCIPLES

6. **Principle One.** Personal data (definition at Paragraph 3 above) is to be *processed fairly* and lawfully and, in particular, is not to be processed unless at least one of the conditions in Paragraph 14 is met and, for sensitive personal data, (definition at Paragraph 4 above) at least one of the conditions in Paragraph 15 is also met. Many (but not all) of these conditions relate to the purpose or purposes for which the information is intended to be used. In practice, it means that there must be:

a. Legitimate grounds for collecting and using the personal data.

b. The data is not used in ways that have unjustified adverse effects on the individuals concerned.

c. There must be transparency about the data that is to be used and individuals must be given appropriate privacy notices when their personal data is collected.

d. People's personal data must be handled only in ways that they would reasonably expect.

e. The data is not to be used for anything unlawful.

7. **Principle Two.** Personal data is to be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. (ie personal data must not be processed for any purpose that is incompatible with the original purpose and all *processing* is to be 'fair').

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

9. **Principle Four.** Personal data shall be accurate (ie are not accurate if they are incorrect or misleading as to any matter of fact) and, where necessary, kept up to date.

10. **Principle Five.** Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. (ie data is to be deleted when no longer required for the purpose for which it was obtained).

11. **Principle Six.** Personal data shall be processed in accordance with the *rights of data subjects* under this Act.

12. **Principle Seven.** Appropriate technical and organisational measures are to be taken against unauthorised or unlawful *processing* of personal data and against accidental loss or destruction of, or damage to, personal data. Rules for data security at The Stonehenge School are at Annex B.

13. **Principle Eight.** Personal data is not to 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.

PRINCIPLE ONE CONDITIONS

14. **For Personal Data.** At least one of the following conditions must be met whenever personal data (definition at Paragraph 3 above) is processed:

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

b. The *processing* is *necessary*: in relation to a contract which the individual has entered into or because the individual has asked for something to be done so they can enter into a contract.

c. The *processing* is *necessary* because of a legal obligation that applies to the processor (except an obligation imposed by a contract).

d. The *processing* is *necessary* to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.

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

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

15. **For Sensitive Personal Data.** When sensitive personal data (definition at Paragraph 4 above) is *processed* then, in addition to at least one of the conditions at Paragraph 13, at least one of the following conditions must also be met:

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

b. The *processing* is *necessary* so that employment law can be complied with.

c.

c. The *processing* is *necessary* to protect the vital interests of: the individual (if the individual's *consent* cannot be given or reasonably obtained) or another person (if the individual's *consent* has been unreasonably withheld).

d. 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*. Extra limitations apply to this condition.

e.The individual has deliberately made the information public.

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

g. The *processin*g is *necessary* for administering justice, or for exercising statutory or governmental functions.

h. 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.

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

j. There are several other conditions for *processing* sensitive personal data which permit such processing 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. Examples of such purposes include preventing or detecting crime and protecting the public against malpractice or maladministration.

16. **Subject Access.** One of the main rights which the Data Protection Act gives to individuals is the right of access to their personal information. An individual may request details of the personal information held about them and for a copy of that information. In most cases a response must be made to a valid request within 40 calendar days of receiving it. A fee may be charged of up to £10 except for educational records where the maximum is £50. In detail: an individual who makes a written (unless disabled and unable to write) request and pays a fee (the School may waive the fee) is entitled to be:

a. Told whether any personal data is being processed.

b. Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.

c. Given a copy of the information comprising the data.

d. Given details of the source of the data (where this is available).

OTHER REQUIRMENTS

17. **Privacy Notices.** A Privacy Notice (sometimes called a Fair Processing Notice) is to be given to all individuals and is to cover:

a. The Data Controller's identity.

b. The purpose or purposes for which it is intended to process the information.

c. Any extra information it is needed to give individuals in the circumstances to enable the information to be processed fairly.

18. **Exemptions.** There are exemptions to granting subject access to personal data, to giving privacy notices and not to disclosing personal data to third parties but it should be noted that every case must be considered on its merits against the requirements of the Act. Most of these are unlikely to apply to schools and are summarised in Annex B. Exemptions that are or might be relevant are:

a. **Exemptions to Non-disclosure to Third Parties.**

1. Subject data requested by eg the police in relation to crime.

2. Subject data requested by HMRC in relation to taxation.

3. Information that has been enacted as publicly available (eg directors' details).

4. Information in connection with legal advice and proceedings.

5. Adoption records and reports, statements of a child's special educational needs and parental order records and reports.

b. **Exemptions to Access to Personal Data.**

1. Management plans containing personal data (eg for redundancies).

2. Confidential references.

3. Personal data that consists of educational records, examination marks or is contained in examination scripts.

STAFF TRAINING

19. The induction of new staff and refresher training is to include awareness of the importance of data protection and confidentiality as specified in this policy. The security requirements referring to staff at Annex B is also to be included.

STATEMENT OF PRACTICE

20. The statement of practice relating to the Act is at Annex D.

Annexes

A. Other Definitions.
B. Security of Data.
C. Other Exemptions.
D. Statement of Practice.

ANNEX A

TO DATA PROTECTION POLICY

OTHER DEFINITIONS

1. **Processing.** Processing broadly means collecting, using, disclosing, retaining or disposing of personal data. In detail this includes:

a. Organisation, adaptation or alteration of the information or data.

b. Retrieval, consultation or use of the information or data.

c. Disclosure of the information or data by transmission, dissemination or otherwise making available.
d. Alignment, combination, blocking, erasure or destruction of the information or data.

2. **Data Controller.** Data controller means a person who (either alone or jointly or in common with other persons) who determines the purposes for which and the manner in which any personal data are, or are to be, processed. A data controller must be a "person" recognised in law, that is to say:

a. An individual.

b. An organisation.

c. Other corporate and unincorporated bodies of persons.

3. **Fair Processing.** Processing personal data must above all else be fair, as well as satisfying the relevant conditions for processing and 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 has been met. Fairness generally requires transparency: to be 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. Information should be treated as being obtained fairly if it is provided by a person who is legally authorised, or required, to provide it.

4. **Necessary Processing.** Many of the conditions for processing depend on the processing being "necessary" for the particular purpose to which the condition relates. This imposes a strict requirement because the condition will not be met if the organisation can achieve the purpose by some other reasonable means or if the processing is necessary only because the organisation has decided to operate its business in a particular way. Eg outsourcing data processing overseas would not be 'necessary' but might require data subjects consent or be covered by '*legitimate interests*.'

5. **Consent.** 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 purposes in question. The circumstances of each case must be examined to decide whether consent has been given. In some cases this will be obvious, but in others the particular circumstances will need to be examined closely to decide whether they amount to an adequate consent. Consent is not defined in the Act but a suitable definition is: 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". Note that 'signify' implies active communication. Consent must also be appropriate to the particular circumstances of the case, eg if it is intended to continue to hold or use personal data after the relationship with an individual ends, then the consent should cover this. Even when consent has been given, in most cases it will last only for as long as the processing to which it relates continues and the individual may be able to withdraw consent, depending on the nature of the consent given and the circumstances in which the information was collected or is being used. Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given.

6. **Legitimate Interests Condition.** The Data Protection Act recognises that there may be legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The "legitimate interests" condition is intended to permit such processing, provided certain requirements are met:

a. The first requirement is that an organisation must need to process the information for the purposes of its legitimate interests or for those of a third party to whom the information is disclosed.

b. The second requirement, once the first has been established, is that these interests must be balanced against the interests of the individual(s) concerned. The "legitimate interests" condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. Where there is a serious mismatch between competing interests, the individual's legitimate interests will come before that of the organisation.

c. Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles.

7. **Rights of Data Subjects.** This is the sixth data protection principle, and the rights of individuals that it refers to are:

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

b. A right to object to processing that is likely to cause or is causing damage or distress.

c. A right to prevent processing for direct marketing.

d. A right to object to decisions being taken by automated means.

e. A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed.

f. A right to claim compensation for damages caused by a breach of the Act.

ANNEX B
TO DATA PROTECTION POLICY

SECURITY OF DATA

COMPUTER SECURITY

1. The Network Manager is to follow the guidelines below as appropriate.

a. A firewall, virus-checking, anti-spyware and spam filters are to be installed.

b. The operating system is to be set up to receive automatic updates.

c. Computers are to be automatically protected by the downloading of relevant critical and security updates to cover known vulnerabilities.

d. Permissions are to be set in order that staff may only access data appropriate to their job.

e. Securely remove all personal information before disposing of old computers (by using an appropriate program or physical destruction of the hard disk).

2. Staff are not to share passwords.

3. Staff are only to take data away from the School for specific purposes and are then responsible for the security of that data and, in particular, for any hardware device used to transport the data.

EMAIL SECURITY

4. Consider whether the content of the email should be encrypted or password protected.

5. As the name of the recipient is typed, some email software will suggest similar addresses you have used before. If several people have been previously emailed whose name or address starts the same way - eg "Dave" - the auto-complete function may bring up several "Dave"s. Ensure the right address is chosen.

6. If it is wanted to send an email to a recipient without revealing their address to other recipients, use blind carbon copy (bcc), not carbon copy (cc). When cc is used, every recipient of the message will be able to see the address it was sent to.

7. Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

8. If a sensitive email is sent from a secure server to an insecure recipient, security will be threatened. The recipient's arrangements must be checked to ensure they are secure enough before sending the message.

FAX SECURITY

9. Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Ensure only the information that is required is sent.

10. Check the fax number to be used. It is best to dial from a directory of previously verified numbers.

11. A sensitive fax is only to be sent to a recipient with adequate security measures in place. For example, the fax should not be left uncollected in an open plan office.

12. If the fax is sensitive, the recipient is to be asked to confirm that they are at the fax machine, are ready to receive the document and there is sufficient paper in the machine.

13. For sensitive data. a sender is to telephone or email to make sure the whole document has been received safely or use a cover sheet. The latter will inform who the information is for and whether it is confidential or sensitive, the contents having to be read.

OTHER SECURITY

14. All confidential paper waste is to be shredded.

15. The physical security of premises is to be appropriate.

16. All staff are to be aware of the following:

a. To be wary of people who may try to trick them into giving out personal details.

b. That they can be prosecuted if they deliberately give out personal details without permission.

c. That strong passwords should be used - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols.

d. That offensive emails are not to be sent about other people, their private lives or anything else that could bring your organisation into disrepute.

e. Not to believe emails that appear to come from eg a bank that ask for account, credit card details or passwords (a bank would never ask for this information in this way).

f. Not to open spam – not even to unsubscribe or ask for no more mailings. The email is to be deleted.

ANNEX C
TO DATA PROTECTION POLICY

OTHER EXEMPTIONS

1. The following exemptions do not apply or are unlikely to apply to schools but are summarised here for completeness. It should be noted that every case must be considered on its merits against the requirements of the Act.

2. **Exemptions from subject Access**:

a. Negotiations (eg on an insurance claim) may be exempt.

b. Personal data processed for, or in connection with, a corporate finance service involving price-sensitive information.

c. Personal data processed for the purposes of making judicial, Crown, or Ministerial appointments or for conferring honours.

3. Exempt from Non-disclosure:

a. Data kept by individuals for 'domestic purposes (eg Christmas card address lists, holiday photographs)

b. Data regarding national security and the armed forces.

c. Personal data that is processed only for journalistic, literary or artistic purposes.

d. Personal data that is processed only for research, statistical or historical purposes.

e. Personal data relating to an individual's physical or mental health. This applies only in certain circumstances and only if granting subject access would be likely to cause serious harm to the physical or mental health of the individual or someone else

f. Personal data that relates to social work.

g. Personal data relating to human fertilisation and embryology, adoption records and reports, statements of a child's special educational needs and parental order records and reports.

ANNEX D
TO DATA PROTECTION POLICY

STATEMENT OF PRACTICE

GENERAL

1. The Head and Governors of this school intend to comply fully with the requirements and principles of the Data Protection Act All staff involved with the collection, processing and disclosure of personal data have been made aware of their duties and responsibilities under the Act

2. The Data Protection Policy is on the School Website.

3. The Data Protection Registration entry for the School may be inspected by appointment. The Business Manager is the person nominated to deal with Data Protection issues in the school. Registered purposes covering the data held at the school are listed on the school's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subjects' consent.

DATA COLLECTION INTEGRITY USE AND DISCLOSURE

4. **Collection.** The School undertakes to obtain and process personal data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' rights of access.

5. **Data Integrity.** The School undertakes to ensure data integrity by the following methods:

    a. **Data Accuracy.** Data held will be as accurate and up to date as is reasonablypossible. If a data subject informs the school of a change in circumstances their record will be updated as soon as is practicable. Where a data subject challenges the accuracy of their data, the School will try to resolve the issue informally but, if this is not possible, any disputes will be referred to the Board of Governors and, if necessary by independent arbitration. Until resolved, all disclosures of the affected information will contain both versions of the information. In order to prevent such problem areas data subjects are able to check their data accuracy and request amendments.
    b. **Data Adequacy and Relevance.** Data held about people will be adequate, relevant and not excessive to the purpose for holding the data.
    c. **Retention of Data.** Data held about individuals will not be kept for longer than necessary for the purposes registered and thereafter will be destroyed.

6. **Subject Access.** In accordance with the Act, all individuals have a right of access to their own personal data. Requests will be logged and met within 40 days of the request or of the receipt of any clarification concerning the request. A fee of up to £10 (£50 for educational records) may be charged but may be waived if meeting the request takes no longer than 30 minutes of staff time. Where a request for subject access is received in respect of a pupil, the school's policy is that:

    a. A request from parents in respect of their own child will, provided that the child does not understand the nature of subject access requests, be met as a request made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

    b. Requests from pupils who can demonstrate an understanding of the nature of their request will be met and the copy will be given directly to the pupil.

    c. Requests from pupils who do not understand the nature of the request will be referred to the child's parents.

7. **Authorised Disclosures.** In general, the School will only disclose data about individuals with their consent. However, there are circumstances under which the school's authorised officer may wish to reveal data without express consent. These are:

    a. Pupil data disclosed to authorised recipients in respect of education and administration necessary for the school to perform its legitimate duties and obligations.

    b. Pupil data disclosed to authorised recipients in respect of their children's health, safety and welfare.

    c. Pupil data disclosed to parents in respect of their children's progress, attendance, attitude and general demeanour within, and in the vicinity of, the school.

    d. Staff data disclosed to the relevant authority in respect of payroll and schools' staff administration.

    e. Other disclosures as may prove unavoidable, for example where an incidental disclosure occurs when an engineer is fixing the computer systems. In such cases, the engineer will sign a document to promise NOT to disclose such data outside the school.

8. Only authorised and properly instructed staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff,

teachers and welfare workers must be made available only if the staff member need to know the information for their work within the school.

DATA AND COMPUTER SECURITY

9. The School undertakes to ensure security of personal data by the following general methods:

a. **Physical Security.** Appropriate building security measures are in place, such as alarms, window bars, deadlocks. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out and are, where appropriate, accompanied.

b. **Logical Security.** Security software is installed on all computers containing personal data, only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (ie. security copies are taken) regularly.

c. **Procedural Security.** In order to be given authorised access to the computer, staff will be properly checked and will sign a confidentiality agreement. All staff are trained and instructed in their Data Protection obligations and their knowledge updated as necessary. Computer printout and source documents are always shredded before disposal.

9. Overall security policy is determined by the Head and will be monitored and reviewed as appropriate and if a major security breach or loophole is apparent. Any queries or concerns about security of data within school should be brought to the attention of the Head.

10. Individual members of staff can be liable in law under the terms of this Act. They may also be subject to damages claims from persons harmed as a result of inaccuracy, unauthorised use or disclosure of their data. Any deliberate breach of this Data Protection policy will be treated as a disciplinary matter and serious breaches of the Act may lead to dismissal.

Adopted by Governors : September 2013
Review date : September 2015