WHISTON JUNIOR AND INFANT SCHOOL

DATA PROTECTION POLICY

Reviewed:	September 2014
Approved by Governors:	.....
Review:	September 2017

CONTENTS

Page

1. Introduction 4

2. Commitments 4

3. Definitions 5

4. Responsibilities 5

5. Training 6

6. Notification 6

7. The Eight Data Protection Principles 6

7.1 Processing Information Fairly and Lawfully 6
7.2 Processing only for specified purposes 7
7.3 Adequacy and relevance 7
7.4 Accuracy and timeliness 7
7.5 Retention of information 7
7.6 Individuals' Rights 8
7.7 Security 9
7.8 Overseas Transfers 9

8. Disclosures of Information 9

8.1 When personal information must be disclosed 9
8.2 When personal information can be disclosed 10
8.3 Other cases 10

9. The Non-Disclosure Exemptions 11

9.1 Crime and Taxation - Section 29(3) 11
9.2 Information Made Available to the Public by or under Enactment – Section 34 11
9.3 Required by Law or in Connection with Legal Proceedings - Section 35 11

10. Offences 11

10.1 Notification 12
10.2 Powers of the Commissioner 12
10.3 Unlawful Obtaining etc of Personal Data 12
10.5 Enforced Subject Access 12

11. Rules for Certain Types of Records 12

11.1 Adoption, Statements of Special Educational Needs and Parental Order Records and Reports 12
11.2 Educational Records 13
11.3 Health Information 13
11.4 Social Work Records 14
11.5 Protection for people who may be at risk if information is disclosed 14
11.6 Employee Records 14

12. Notices and Wording on Application Forms, Leaflets etc. 15

12.1 Examples of notices 15

13. E mail and the Internet 16

13.1 E mail 16
13.2 The Internet 17

14. System or Database Design and Development 17

15. Further Advice 17

Annex A - Relevant Sections of the Data Protection Act 1998 18

Annex B - Financial Services Retention of Data Internal Audit Guidelines 19

Annex C - Data Subject Access Procedure 22

DATA PROTECTION POLICY

1 Introduction

- Whiston J & I needs to collect and use information about people it deals with. This information may be about pupils, parents, members of staff, contractors and others.
- Computers, paper records, e-mails, microfilm, CDs, audio tapes, CCTV footage etc can all hold personal information.
- The Data Protection Act 1998 and other laws (such as Human Rights Act, the Law of Confidence etc) require the proper handling of personal information.
- People who give school their personal information should be confident that information will be handled lawfully, fairly and with due regard to their rights at all times.
- People giving personal information to Whiston Junior & Infant School need to be confident that it will be properly used. This confidence will enhance the success of school operations.
- This policy spells out the commitments to everyone whose personal information is used by us. All employees will be made aware of this policy as part of their induction to the school and periodically thereafter.

2 Commitments

Whiston Junior & Infant School will ensure that it:

- complies with all applicable legislation relating to the handling of personal information
- adopts best practice in handling personal information
- collects and uses personal information fairly and lawfully
- clearly specifies the purposes for which personal information is to be used
- collects and uses personal information only to the extent needed to discharge its responsibilities
- checks (where possible) the accuracy of the personal information it handles
- holds personal information for the minimum necessary time
- respects the rights of people whose personal information is held
- takes appropriate security measures to safeguard personal information
- only transfers personal information outside the European Economic Area in accordance with the law
- has a nominated Data Protection Officer
- implements a system of regular reviews and audits of the management and use of personal information.

3 Definitions

The following definitions are used throughout this policy:

- **Data Controller**
  The person or organisation who determines how information will be used and for what purpose (i.e. Whiston Junior & Infant School)

- **Data Processor**
  A third party who processes information on behalf of the data controller and under their instruction (not an employee). For example will use an agency to provide payroll services to the school on a monthly basis Whiston Junior & Infant School. As they will only process information under instruction from the school, the agency will be the data processor and Whiston Junior & Infant School will remain the data controller for that processing.

- **Data Subject**
  A living individual about whom you hold personal information.

- **Information Commissioner**
  The Government Regulator for the Data Protection Act 1998 and Freedom of Information Act 2000.

- **Personal Data or Personal Information**
  Information relating to a living individual who can be identified from that data, or from that data and other information in the possession of, or likely to come into possession of, the data controller.

- **Sensitive Data or Sensitive Information**
  Data such as that relating to an individual's race, religious or similar beliefs, health, sexual life, political opinion, trade union membership, anything relating to criminal offences or proceedings.

- **Processing**
  Obtaining, recording, holding, altering, disclosing, merging, deleting, destroying, retrieving, consulting or using information.

- **Parent**
  The meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

4 Responsibilities

- Each individual member of staff is responsible for making sure that personal information is properly handled.
- School Governors, in coordination with the Headteacher, are responsible for ensuring that school staff are properly trained and aware of relevant policies.
- The Leadership Team must ensure that school staff are adequately supervised with regard to the handling of personal information.
- Quality control checks should be carried out by the School Governors and Headteacher.
- Internal Audit will check compliance with this policy.

5 Training

- Everyone who handles personal information needs to be aware of this policy and to receive training.
- School Governors, in coordination with the Headteacher, must ensure that employees receive appropriate training.
- Training will be available to employees as part of the induction process and the Leadership Team must ensure that employees are made aware of this policy during their initial induction.
- Further advice and guidance is available from the school's Data Protection Officer.

6 Notification

- It is a requirement of the Data Protection Act 1998 that individual statutory bodies must notify the Information Commissioner of the purposes for which they process information. For example, the school's notification will include using information for Education, Personnel Administration etc.
- If you set up a new system, you must advise the school's Data Protection Officer, who will ensure that the notification is updated to cover that processing.

7 The Eight Data Protection Principles

7.1 Processing Information Fairly and Lawfully

We all expect our personal information to be handled properly by organisations. This guide outlines the law and identifies best practice when handling personal information.

- **Process information fairly**
  - Tell the person whose information you have who you are (i.e. Whiston Junior & Infant School) as soon as contact is made.
  - Tell them what the information will be used for (e.g. monitoring of performance and achievements).
  - Give them any other information they might need to understand how their information will be used (e.g. compliance with statutory obligations of LEA)
  - Tell them who they can ask about the processing of their information (i.e. the school's Data Protection Officer).

- **Process information lawfully**
  - Know the law you are working under, i.e. what gives Whiston Junior & Infant School the legal right to carry out a particular activity.
  - Do not do anything which the Whiston Junior & Infant School does not have the legal power to do.

- **Wherever possible, process information with consent**
  - Where people may give personal information voluntarily, ask them to agree that you can use it.
  - Where people must give personal information (i.e. it is illegal for them not to), explain this and the reasons for the requirement
  - If individuals do not give their consent, contact the school's Data Protection Officer for advice.

- **Sensitive Data**

Under the Data Protection Act 1998 there are conditions to be met prior to processing sensitive data.

- If you have explicit consent from an individual you may process their sensitive data.
- Explain the reasons for asking about sensitive information.
- Ask people to give a clear consent to your use of the information.
- Respect their wishes if they do not give consent. If you still need to process this information, contact the school's Data Protection Officer for advice.
- Where people must give sensitive personal information (i.e. a statutory service cannot be provided without it), explain this and the reasons for the requirement.

7.2 Processing only for specified purposes

- Tell people whose information is to be used exactly what it will be used for.
- Process personal information only for the purposes you have specified.
- Do not use information for purposes significantly different from those it was collected for.
- Do not disclose information for other purposes unless an exemption applies (refer to 9. The Non-Disclosure Exemptions).

7.3 Adequacy and relevance

- Make sure that the information is adequate, relevant and not excessive for the purpose for which it is collected.
- Decide on the minimum amount of personal information required for your purpose and collect that (e.g. you do not usually need to know someone's date of birth to deal with a complaint from them about the condition of a classroom).
- Only collect personal information which is relevant to your purpose.
- Do not collect personal information just because it is usual to do so.
- Review at intervals what information is collected and why.

7.4 Accuracy and timeliness

- Students/parents/staff members must ensure that all personal data provided to the school is accurate and up-to-date.
- Whiston Junior & Infant School cannot be held responsible for any errors in accuracy unless the member of staff or student/parent has informed the school about them.
- Correct any inaccuracies you find.
- Where new information is available, update the records as soon as possible (e.g. when someone tells you of a change of address).

7.5 Retention of information

- Make sure that information is kept no longer than necessary.
- Check whether there is a retention policy in place for the information you are processing. If not, contact the school's Data Protection Officer to ensure a relevant policy is developed.

- The Data Protection Act requires that information be kept no longer than necessary. If no current retention policy exists, establish a policy which defines retention periods, taking into account any legislative requirements and what the information may be needed for.
- Further advice on the storage of records can be obtained by visiting the National Archives website at www.nationalarchives.gov.uk
- When information is no longer required for any purpose, destroy it (e.g. when someone asks for a job application form to be sent to them, their name and address details can usually be destroyed immediately). Ensure that it is destroyed in a secure manner (refer to the Information Security Policy).

7.6 Individuals' Rights

- **Right of access to personal data (Data Subject Access)**
  - School staff, students/parents and other data subjects have the right
    - to be told whether personal information about them is processed
    - to be given details about what personal information is processed, and for what purpose
    - to be told who the personal information may be disclosed to and where it was obtained from (if known)
    - to obtain a copy of their personal information (follow the procedure at Annex C):
      - If no information can be traced, the individual must be informed.
      - There are a number of exemptions to this right. Please contact the school's Data Protection Officer for further advice where necessary.
      - If the individual is not happy with the response or with any of the information provided, refer to the school's Data Protection Officer.
    - to have explained (if significant decisions are made solely by automatic means) the decision making processes involved. (For example, some psychometric tests for job applications involve significant decisions made by automatic means)

- **Right to prevent processing likely to cause damage or distress**
  - In certain cases school staff, students/parents and other data subjects have the right to require the school not to process personal information if this would cause substantial and unnecessary damage or distress to them. Any individual who wishes to register an objection must do so in writing, by letter addressed to the Headteacher.

- **Right to prevent processing for the purposes of direct marketing**
  - Individuals have the right to require Whiston Junior & Infant School not to process their personal information for the purposes of direct marketing.

- **Rectification, blocking, erasure and destruction**
  - Individuals have the right to ask a Court to order Whiston Junior & Infant School to rectify, block, erase or destroy personal information which is inaccurate.

- **Compensation for failure to comply with certain requirements**
  - Individuals have the right to compensation (damages) if Whiston Junior & Infant School gets things wrong and damage or distress is caused as a result.

- **Rights in relation to automated decision making**
  - Individuals have the right to require the data controller not to make decisions which significantly affect the individual, solely by automatic means.

Note: There are exemptions and limitations to these rights.

7.7 Security

- Ensure that technical and organisational measures are in place to prevent unauthorised or unlawful processing of the information or the accidental loss, destruction, or damage of the information.
- Security measures which prevent the obtaining, holding, recording, or any use of personal information other than for purpose(s) specified, should be in place.
- Members of staff who process personal information should know what they are authorised to do.
- Computer systems should have built-in security measures, such as password protection, to prevent unauthorised processing.
- Disclosures of personal information must be strictly controlled. In some cases it may be advisable to log disclosures. Refer to the school's Data Protection Officer for further advice.
- School staff must be reliable and there is a continuing leadership responsibility to monitor employees.

7.8 Overseas Transfers

- The Act requires that information is not passed outside the European Economic Area (where there may be less stringent Data Protection laws) unless certain criteria are met.
- In practice, it is advisable not to send personal information outside the United Kingdom (e.g. via the Internet, e-mail, ordinary post, etc.) without the consent of the member of staff or student/parent involved.
- There are some circumstances in which this can be done without consent - please ask the schools Data Protection Officer for advice before doing this.

8 Disclosures of Information

People or organisations sometimes try to obtain information about other data subjects.

8.1 When personal information must be disclosed

- A Court can order information be disclosed.
- Various statutory bodies and the Police can obtain warrants etc to require disclosure.
- Various statutory bodies can require disclosure in limited circumstances (e.g. pupil data is disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations).
- It is sometimes a legal duty to disclose (e.g. disclosure of information to Connexions under the Learning and Skills Act 2000, sections 114-122).

The personal information required must be disclosed. In each case you should request full details of the legal basis for the request and take further advice if necessary. Make clear file notes of what happens, except when public registers are accessed.

8.2 When personal information can be disclosed

There are also bodies and people that can ask for personal information (also refer to 9. The Non-Disclosure Exemptions):

- A body involved in the prevention/detection of crime, the apprehension/ prosecution of offenders, or the assessment/collection of any tax or duty may ask for information under Section 29(3) of the Data Protection Act 1998 (refer to Annex A for details). These requests should be in writing and clearly state the basis for the request. If it is appropriate, personal information may be disclosed (you are not compelled to disclose information).
- Data subjects may appoint others to help them - for example, welfare rights workers, family members, friends, MP's, Councillors, professionals (e.g. Solicitors) etc. It is not always necessary to obtain written consent but you must be certain that consent has been given before any information is disclosed. Their representative can then be treated as if they were the data subject to the extent of their authority.
- Requests for personal information may come from someone who has been specially appointed by law (for example, Receivers appointed by the Court of Protection, Attorneys acting under Enduring Powers of Attorney etc.) to look after the data subject's affairs. After checking the relevant documentation, they should be treated as if they are the data subject.
- Where an Enduring Power of Attorney applies but the donor has become incapacitated, the details need to be registered with the Court of Protection. Confirmation of this should be sought. Refer to RMBC Legal Services for further advice if necessary.

8.3 Other cases

In all other cases the person making the enquiry may have no right to personal information about other people. The disclosure will need to be carefully considered, taking into account the following:

- Whiston Junior & Infant School holds a lot of personal information and any disclosure of personal information must comply with the law.
- If individuals are found to have permitted an unlawful disclosure, they, as well as the data controller, can be prosecuted.
- Has the data subject consented to the disclosure of personal information? If so, personal information can be disclosed in line with that consent.
- Personal information about "third parties" (someone other than the data subject) or information that could identify them, should not normally be disclosed.
- Where personal information is held for the prevention/detection of crime, the apprehension/prosecution of offenders, or the assessment/collection of any tax or duty, it should not be disclosed where to do so would prejudice those purposes.
- If the information relates to adoption, special educational needs, health, educational records, or social work (refer to 11. Rules for Certain Types of Records).

- All disclosures of information must be in line with Whiston Junior & Infant School policy and instructions to school staff. School Governors, working with the Headteacher, must set out clear instructions for school staff on the disclosure of personal information.

9 The Non-Disclosure Exemptions

Where information is required by other organisations for certain purposes, we may be able to disclose the information without breaching the Data Protection Act (refer to Annex A for details of the relevant sections of the Act). Please note that you are not obliged to disclose information and can refuse to do so. The following are a summary of the exemptions most likely to be referred to:

9.1 Crime and Taxation - Section 29(3)

- Where information is required for the prevention or detection of crime, the prosecution or apprehension of offenders or the collection of tax or duty.
- The exemption only applies where the enquiry would be prejudiced if the information was not supplied.
- In practice, this means that organisations who prosecute for criminal offences can ask for information as part of the criminal enquiry, if it would prejudice the enquiry not to get the information. Agencies likely to use this exemption are the Inland Revenue, Benefits Agency Fraud, Police etc.

9.2 Information Made Available to the Public by or under Enactment – Section 34

- Where information must be made available to the public by or under any law.
- In practice, this means that if you are obliged by law to make information available you won't breach the Act by publishing the information.
- This exemption only applies to the information you are obliged to make public, not to any further information you may hold about the individual.

9.3 Required by Law or in Connection with Legal Proceedings - Section 35

- Where disclosure is required by law, under any Act or by order of the Court, in connection with legal proceedings (including prospective legal proceedings) or for protecting or defending legal rights or obtaining legal advice.
- Requests for information may be made by departments involved in taking legal proceedings, such as RMBC Legal Services.
- This exemption needs to be carefully considered with due regard to the school's legal powers and whether the conditions for processing information are met. Refer to the school's Data Protection Officer for further advice.

10 Offences

There are a number of offences under the Data Protection Act. For details of all offences please contact the school's Data Protection Officer. The following are a summary of offences which may be relevant for Whiston J & I School staff.

10.1 Notification

- Processing without being notified to the Information Commissioner.
- Failure to notify changes of processing to the Information Commissioner.
- Failure to comply with a request for notification particulars from the Information Commissioner.

10.2 Powers of the Commissioner

- Failure to comply with an enforcement notice, information notice or special information notice.
- Making a false statement in replying to an information notice or special information notice.
- Obstruction of, or failure to give reasonable assistance in, execution of a warrant (obtained in accordance with the Commissioner's powers).

10.3 Unlawful Obtaining etc of Personal Data

- Where a person, knowingly or recklessly, without the consent of the data controller,
    - obtains or discloses personal data
    - procures the disclosure of personal data (i.e. tries to get information they have no right to)
- UNLESS they can show
    - it was necessary to prevent/detect crime or was authorised by law
    - they had reasonable belief they had a legal right to obtain, disclose or procure information
    - they had reasonable belief the data controller would have consented to the obtaining, disclosing or procuring
    - that the obtaining, disclosing or procuring was in the public interest

10.4 Unlawful Selling of Personal Data

- Selling, or offering to sell personal data, unlawfully obtained.

10.5 Enforced Subject Access

- To request potential or existing employees to access their own personal information to obtain from the police a report of convictions/cautions recorded against them (there are some limited exemptions).

11 Rules for Certain Types of Records

11.1 Adoption, Statements of Special Educational Needs and Parental Order Records and Reports

Personal information covered by one or more of the following Statutes/Regulations are exempt from Section 7 (Right of access to personal data) of the Data Protection Act and should not be disclosed in the event of a subject access request.

- Sections 31 and 33 of the Human Fertilisation and Embryology Act 1990.
- Sections 50 and 51 of the Adoption Act 1976.

- Regulations 6 and 14 of the Adoption Agencies Regulations 1983 - so far as they relate to records or other information in the possession of local authorities.
- Rules 5, 6, 9, 17, 18, 21, 22 and 53 of the Adoption Rules 1984.
- Rules 5, 6, 9, 17, 18, 21, 22 and 32 of the Magistrates' Courts (Adoption) Rules 1984.
- Regulation 19 of the Education (Special Educational Needs) Regulations 1994 - Statements of Special Educational Needs (SSEN's).
- Sections 50 and 51 of the Adoption Act 1976 as modified by paragraphs 4(a) and (b) of Schedule 1 to the Parental Orders (Human Fertilisation and Embryology) Regulations 1994 in relation to parental orders made under section 30 of the Human Fertilisation and Embryology Act 1990.
- Rules 4A.5 and 4A.9 of the Family Proceedings Rules 1991.
- Rules 21E and 21I of the Family Proceedings Courts (Children Act 1989) Rules 1991.

11.2 Educational Records

- Records about pupils at a school, used by the governing body or teachers at the school, may be exempt from all or part of the subject access provisions where:
    - providing access may be likely to cause serious harm to the mental or physical health or condition of any individual
    - providing access would reveal if the subject is (or has been, or may be) at risk of child abuse, to the extent that disclosure would not be in the best interests of that individual
- Take further advice if such a request is received.

11.3 Health Information

Information about the physical or mental health or condition of a person (the data subject) is very sensitive and needs to be treated with proper care. If the data subject wants to see the personal information, he or she has a general right to do so but in the following cases, that right is restricted.

- Where in the opinion of the appropriate health professional (usually the person responsible for the care of the data subject) the disclosure of part (or all) of the personal information would be likely to cause serious harm to the physical or mental health or condition of anyone, that part of the personal information or all of it should be withheld.
- Where evidence containing personal health information is given in certain Court proceedings involving children it may be withheld from the data subject - ask the Solicitor handling the case for advice.
- A person who has parental responsibility for a data subject or a person who has been appointed by the Court to manage a data subject's affairs, can ask for health information about the data subject. That personal information should be withheld if:
  (a) the person asking for the personal information does not have lawful authority to do so; or
  (b) the data subject did not and still does not, expect the personal information to be disclosed; or
  (c) the data subject does not want the personal information disclosed.
- Health information held as part of an adoption record or as a Statement of Special Educational Needs will usually be withheld. Refer to 12.1 and take further advice if necessary.

11.4 Social Work Records

Very sensitive personal information about people is often collected while carrying out social work. It is vitally important that this personal information is properly handled so as not to prejudice social work objectives, the health of any person or the legal situation of the school.

- Evidence containing social work personal information is given in Court proceedings involving children. In all cases you should take further advice if you get a request for personal information. Usually, information can only be released with the consent of the Court.
- The data subject has no access to social work personal information under the data protection legislation, if the disclosure of that personal information would be likely to cause serious harm to the physical or mental health or condition of any person. The data subject, however, must be told (if a request for personal information is made) that personal information is being processed about them. A person who has parental responsibility for a data subject or a person who has been appointed by the Court to manage a data subject's affairs, can ask for personal information. That personal information should be withheld if:
  (a) the person asking for the personal information does not have lawful authority to do so; or
  (b) the data subject did not and still does not, expect the personal information to be disclosed; or
  (c) the data subject does not want the personal information disclosed.
- Sometimes personal information is requested for use in criminal proceedings. In all cases you should take further advice if you get such a request.

11.5 Protection for people who may be at risk if information is disclosed

This protection applies usually to people who have contributed to personal information about someone in a health or social services context. Such people may be at risk of serious harm to their physical or mental health if personal information is disclosed. The risk might be from the data subject or from another source.

- Any person who feels that Whiston Junior & Infant School is about to comply with a data subject's request for personal information may apply to the Court. The Court can order that the personal information is not disclosed.
- The Court must be satisfied that the person making the application is at risk of serious harm to their physical or mental health if the personal information was disclosed.

11.6 Employee Records

- Employment files, which may contain sensitive information relating to sickness, disciplinary proceedings etc must be kept secure (refer to Information Security Policy).
- Disciplinary notices and warnings should be kept in a sealed/signed envelope within the employment file.
- Access must be restricted to persons with a 'need to know' and only for employment purposes.
- Recruitment files for unsuccessful applicants should only be retained for 9 months.
- School staff should be aware that references requested will include details of sickness and/or disciplinary proceedings.

12 Notices and Wording on Application Forms, Leaflets etc.

We should tell staff, students and parents clearly what we want their personal information for and how we intend to use it. When we ask for personal information, we must:

- Say clearly who is in charge of that personal information (usually Whiston Junior & Infant School).
- Ask for consent to use personal information wherever possible.
- Explain exactly what the information will be used for and the consequences of that use.
- If you want to use the personal information for any purpose subsidiary to the main purpose explain this and give individuals the chance to opt out. For example, when completing complaints forms, individuals would expect that the personal information they supply will be used to investigate their complaint. If you want to use that personal information for further work, an explanation should be given.
- Explain any further disclosures (for example, disclosure to the LEA).
- If the information will be used for marketing purposes (i.e. sending details of future events) individuals must be given the chance to opt out, for example "tick this box if you do not want to receive further information".
- Give people a contact point at which to make enquiries about the handling of their information and say that the school has a Data Protection Officer (give contact details if requested).

12.1 Examples of notices

Where giving personal information is compulsory

"By law you must give us ([school name]) the information requested [on this form]. We will use it for: [list all the purposes you are going to use the information for].

If you want to make any further enquiries about [specific subject / topic] please contact [provide contact details].

We have a Data Protection Officer, who can be contacted at: [school name, school address, contact telephone number]. "

Where giving some personal information is compulsory and some is voluntary

"By law you must give us ([school name]) the information [marked ***** / requested on this form]. We will use it for: [list all the purposes you are going to use the information for]. We will use the other information for [the same purposes? - provide as much detail as necessary for the individual to understand how their information will be used].

If you want to make any further enquiries about [specific subject / topic] please contact [provide contact details].

We have a Data Protection Officer, who can be contacted at: [school name, school address, contact telephone number]. "

Where giving all personal information is voluntary

"By signing this form, you consent to us ([school name]) using your information for: [list all the purposes you are going to use the information for - provide as much detail as necessary for the individual to understand how their information will be used].

If you want to make any further enquiries about [specific subject / topic] please contact [provide contact details].

We have a Data Protection Officer, who can be contacted at: [school name, school address, contact telephone number]. "

- The words in square brackets [ ] contain advice on text that will need to be tailored to your school.
- These notices cannot cover every situation. If you would prefer to use different wording, or need any further advice, please contact the school's Data Protection Officer.

Front line employees who deal with responses to these notices need to know:

- what personal information is held
- what it is processed for
- how someone can get a copy their personal information.

13 E mail and the Internet

13.1 E mail

The Data Protection Act 1998 controls the use of personal information. Therefore, if you include any personal information in an e-mail, you must comply with the Act.

- Ensure that you use information fairly and lawfully (refer to 7.1).
- Do not process personal information unless this is consistent with the purpose for which it was collected.
- Ensure that personal information is accurate and up to date.
- Destroy e mails which are no longer required.
- Do not send personal information outside the European Economic Area unless the relevant criteria are met (refer to 7.8).
- Refer to the school's Electronic Communications Policy for full details of how you may use the e-mail system.
- Remember that a data subject can request copies of information held about them on the e-mail system, can require the correction, blocking or erasure of damaging information, and can claim compensation for damage caused by inaccurate information.
- Be aware that all e-mail messages can be recorded. Management do not routinely monitor the content of messages but may, under certain circumstances, monitor specific usage and gain access to mailboxes.

13.2 The Internet

- The Internet is a very large network of computers which is unregulated. It is not secure except when special software is used.
- Anyone, anywhere in the world with a connection to the Internet can view information on it.
- If personal information is put on a website, the individual involved must have given their consent. There are some exemptions to this – refer to the school's Data Protection Officer for advice.
- Refer to the Electronic Communications Policy for full details of how you may use the Internet.
- Remember that your use of the Internet can be monitored.
- Do not access or disseminate website material containing any of the following: pornography/adult material, gambling, share dealing, drugs, racism/hate, terrorism, paedophilia, unless specific approval has been obtained for work purposes.

14 System or Database Design and Development

Many potential data protection problems can be overcome by good system design. When planning a new manual or electronic system, consider the following:

- Notification (refer to 6).
- What personal information do I need to use and why?
- Do I need to collect sensitive personal information? (refer to 7.1)
- What will I be using the information for?
- How long do I need to retain personal information?
- Do I have the legal right to use this personal information in this way?
- Wherever possible get consent to use information from the data subject.
- How will I communicate the purposes of the system to data subjects (e.g. by telling them when they phone or adding a notice to an application form)?
- How can I ensure that the personal information is accurate?
- How will I keep information up to date?
- How can I make sure that data subjects' rights are protected? How will I provide information in the event of a subject access request? (refer to 7.6).
- Who will have access to the personal information?
- What security measures are planned to ensure that there is no unauthorised access to personal information?

15 Further Advice

- The Information Security Policy and the Electronic Communications Policy
- Your line manager
- [school name] Data Protection Officer
- The Data Protection & Information Security Officer, Legal and Democratic Services, Rotherham Borough Council, Civic Building, Walker Place, Rotherham, S65 1UF (01709 823566)

Annex A - Relevant Sections of the Data Protection Act 1998

Section 28

(1) Personal data are exempt from any of the provisions of:-

(a) the data protection principles

(b) Parts II, III and V, and

(c) section 55

if the exemption from that provision is required for the purpose of safeguarding national security.

Section 29

(1) Personal data processed for any of the following purposes:-

(a) the prevention or detection of crime

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of any tax or duty or of any imposition of a similar nature,

are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

(3) Personal data are exempt from the non-disclosure provisions in any case in which:-

(a) the disclosure is for any of the purposes mentioned in subsection (1), and

(b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.

Section 34

Personal data are exempt from:-

(a) the subject information provisions,

(b) the fourth data protection principle and section 14(1) to (3), and

(c) the non-disclosure provisions

if the data consist of information which the data controller is obliged by or under any enactment to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.

Section 35

(1) Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

(2) Personal data are exempt from the non-disclosure provisions where the disclosure is necessary:-

(a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or

(b) for the purpose of obtaining legal advice,

or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Annex B - Financial Services Retention of Data Internal Audit Guidelines

Need for Guidelines

Internal Audit receives many informal requests from other departments who wish to dispose of data, owing to pressures on storage space available.

These requests have tended to be dealt with on an ad hoc basis, which does not encourage consistency of policy in this area.

Introduction of common guidelines would be beneficial in that:

(i) departments would be less likely to inadvertently dispose of data which was required.
(ii) departments would be less likely to needlessly accumulate data.
(iii) decision making in this area would be facilitated and should reduce the need for consideration of this same area by officials in departments and Finance at regular intervals.

Basis of Guidelines

1. Minimum periods of retention have been specified, as it is recognised that individual departments within the school will have differing needs/resources available in respect of retention of data and any decisions relating to the usefulness of retaining data beyond the minimum retention period are best taken by individual departments.

2. It is not practical to anticipate every particular need in this area, but it is hoped that the main sources of usual queries are covered.

3. It is recognised that departments may be desirous of keeping documents other than in their original format, e.g. computerised document imaging. However, it is important that departments who do so take due account of all legal considerations. Further advice is available from RMBC Legal Services or Internal Audit on this issue.

Internal Audit Guidelines – Retention of Financial Data

RECORD	MINIMUM PERIOD TO BE RETAINED
Cash Income	
Receipt Books	6 years (VAT requirement)
Records relating to the issue of tickets	As Above
Till Rolls	As Above
Paying-in Books	As Above
Supporting Records:-	
Records of Remittances Received	As Above
Daily Income Records, e.g. Catering Salesheets	As Above
Records of Overs and Shorts	As Above
Scales of Charges	As Above
Credit Income	
Debtor Accounts (Inclusive of VAT)	6 years
Debtor Accounts (Non-VAT)	Last financial year signed off by District Auditor plus the preceding financial year
Primary Debtors Records:-	Reason for raising debt / cost calculation
Raised Credit Notes	Last financial year signed off by District Auditor plus the preceding financial year
Expenditure	
Requisitions for supplies / works) Official Copy Orders) Delivery Notes)	Last financial year signed off by District Auditor plus the preceding financial year
Paid Invoices	6 Years
Paid Cheques	6 Years
Petty Cash Voucher) Cheque Requisition Books)	Last financial year signed off by District Auditor plus the preceding financial year.
Stores Prime Records Stores Ledger	Last financial year signed off by District Auditor plus the preceding financial year.

RECORD	MINIMUM PERIOD TO BE RETAINED
Issues, Transfer and Return Notes	As Above
Goods Received Notes	As Above
Stock Adjustment Notes	As Above
Transport Prime Records	As Above
Other	
School Registers	
Dinner Register Summary	6 Years
Pupil Dinner Registers	Last financial year signed off by District Auditor plus the preceding financial year
Attendance Registers/Records	Three years
PLASC Return (Formerly Form 7 Return)	6 years + Census years (1991&2001)
Contracts	
Contracts Register	Indefinitely
Register of Tenders and Quotations	Indefinitely
Contract documents (where contract is under seal)	12 years
Contract documents (where contract is not under seal)	6 years
Contract final account documents	12 years
Ledgers and Supporting Information	Indefinitely
Insurance Policies	Indefinitely
Bank Statements	6 years
Timesheets/Clock Cards inc. Bonus Sheets	Last financial year signed off by District Auditor plus the preceding financial year.
Other Staff Returns, e.g. (Overtime/ Allowances)	As Above
Copy Payroll	As Above
Details of Appointments, changes Leavers, etc.	As Above
Personal Records	Indefinitely
PAYE	6 years
Monthly Summary of Tax Paid to Revenue	Last financial year signed off Inland by District Auditor plus the preceding financial year.
P45's, P6's	As Above

Annex C - Data Subject Access Procedure

In accordance with Section 7 of the Data Protection Act 1998, any individual has a right to be told whether the [school name] is processing their personal information and to access that information.

- A copy of all information must be provided to the data subject unless an exemption applies.
- Information about other persons should be removed.
- We have a maximum period of 40 days to provide the information.
- The information should not be altered in order to make it acceptable to the data subject, although routine updating may continue.

Procedure

1. Request Received

The individual must provide identity details, an identification document and enough detail to find the information required. A standard request form and letter is attached at Appendix A, but if a clear written request containing all the information required is received, a form is not always necessary. A person can apply on behalf of someone else if they have written authorisation from that person.

2. Identify what is required

Although an individual does have the right to ask the school for ALL the information we hold, you can ask them what they want and limit the search to those records.

3. Acknowledgement

Acknowledge the request in writing (Appendix B) and advise when you will provide the information. The maximum time period allowed is 40 days.

4. Other Information

When an individual makes a subject access request, we should also inform them what we use their information for, where we obtained the information (if known), and who we may disclose information to.

5. Provision of E-mails

If the individual asks for e-mails, ask them to specify who the e-mails may have been sent to / received from. You can then ask the named individuals / departments to check their e-mail system and print off any e-mails containing personal information about the data subject. Remember that there may be e-mail back-ups and you may need to seek IT assistance [from whom] to retrieve them, if required by the applicant.

6. Extract the information

Extract information about the data subject for the areas specified. Remember that the data subject is entitled to copies of both electronically held and manual records. If no information is found you must advise the applicant of this (Appendix C).

7. Edit information where Exemptions apply

There are a number of exemptions within the Act, where we can withhold certain information. Check whether any of the exemptions apply when deciding what to provide to the data subject.

8. Edit information about other people
You must edit out any information about somebody else, unless the applicant would already know this information. However, don't assume they would know information about their partner or other family members. The best way to edit documents is to tippex out the information on one copy, then provide a photocopy of this to the applicant.

9. Explain codes and abbreviations
You must explain any coded items or abbreviations to the applicant.

10. Take a Copy
Keep a full copy of the information you send so that we can identify what has been edited in the event of a complaint.

11. Respond
Send the response by recorded delivery (see Appendix D).

The Subject Access Exemptions

Crime & Taxation – personal data processed for the prevention/detection of crime, the apprehension/prosecution of offenders or the assessment/collection of tax are exempt from subject access, only to the extent where disclosure of the information would prejudice those purposes.

Adoption, Statements of Special Educational Needs and Parental Order Records and Reports – personal information covered by several Statutes/Regulations are exempt from subject access. Refer to Page 12 of the Policy for full details

Educational Records – Records about pupils at a school, used by the governing body or teachers at the school may be exempt from all or part of the subject access provisions where providing access may be likely to cause serious harm to the mental or physical health or condition of any individual or providing access would reveal if the subject is (or has been, or may be) at risk of child abuse, to the extent that disclosure would not be in the best interests of that individual. Take further advice if such a request is received.

Health Records - information about the physical or mental health or condition of the data subject is very sensitive and needs to be treated with proper care. If the data subject wants to see the personal information, he or she has a general right to do so but in some cases, that right is restricted. Refer to Page 13 of the Policy for full details.

Social Work Records - very sensitive personal information about people is often collected while carrying out social work. Some of this information will be exempt from subject access. Refer to Page 14 of the Policy for full details.

Health and/or Social Service Records – if persons may be at risk if information is disclosed. This protection applies usually to people who have contributed to personal information about someone in a health or social services context. Such people may be at risk of serious harm to their physical or mental health if personal information is disclosed. The risk might be from the data subject or from another source. Any person who feels that the school is about to comply with a data subject's

request for personal information may apply to the Court. The Court can order that the personal information is not disclosed. The Court must be satisfied that the person making the application is at risk of serious harm to their physical or mental health if the personal information was disclosed.

Regulatory Activity – personal data processed for certain functions for the purposes of protecting members of the public against dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity, are exempt from the subject access provisions where disclosure would prejudice the proper discharge of these functions. These functions include functions conferred by enactment or other functions of a public nature exercised in the public interest.

Research, History & Statistics – personal data processed only for research purposes are exempt from subject access if they are not processed to support measures or decisions with respect to particular individuals, the data are not processed in such a way that substantial damage or distress is, or is likely to be, caused to any data subject and the results of the research or any resulting statistics are not made available in a form which identifies any data subject

Information made available to the public by or under enactment – personal data are exempt from the subject access provisions if the data consist of information which the data controller is obliged by or under any enactment to make available to the public, whether by publishing or making available for inspection.

References – a confidential reference given or to be given by the data controller for Whiston Worrygoose the purposes of education/training/employment, appointment to office, or for provision of a service, is exempt from subject access (Note this does not apply to references received).

Management Forecasts & Planning – personal data processed for these purposes are exempt from subject access if it would prejudice the conduct of the data controllers business or other activity.

Negotiations – records of the intentions of the data controller (Whiston Worrygoose) relating to negotiations with the data subject are exempt from subject access where the disclosure would prejudice the negotiations.

Examination Scripts – personal data consisting of information recorded by candidates during an academic, professional or other examination are exempt from subject access.

Examination Marks – are exempt from subject access for certain periods prior to publication of the results. Take further advice where such a request is received.

Legal Professional Privilege – personal data are exempt from subject access if the data consist of information where a claim to legal professional privilege could be made in legal proceedings (i.e. the data consists of confidential discussions between a legal advisor and a client).

DATA PROTECTION ACT 1998
SUBJECT ACCESS REQUEST FORM
Whiston J & I School

To enable us to process your request, please complete and return this form to the address below.

1. Your Details

Name	Surname	Forename(s)	Title
Address	Postcode		
Date of birth		Contact Telephone Number	

2. Please provide any identity or file numbers (if known) and National Insurance number if this would be included within the records you are requesting.

Identity or File Numbers		National Insurance Number	

3. Information required

Please state below what information you require and the reasons why [Whiston J & I school] would have personal information about you in its files. Details of any reference numbers, pupil identification references, payroll numbers etc will assist us to process your application.

Note that we may have a large amount of information to send you including computer screen prints and paper records. If you are looking for a particular document or set of documents, you may prefer to specify exactly what you require. This will speed up your request and ensure you receive the correct information.

4. CCTV Images

If you require CCTV images we will need to know the dates and times that your images will have been recorded and where you passed a camera under our control. Please give details of these below. You will also need to provide us with a copy of a recent photo of yourself so we can identify you.

5. Your consent

I require the information requested on this form.

Your Signature		Date	

If you are applying on behalf of someone else, complete their details in Sections 1 – 4 above, sign the form in Section 5 and provide your details below. You must indicate why you are acting on their behalf and, in most cases, written consent will be required.

If you are applying on behalf of a child, please explain below why this is in the interests of the child. If a child is able to understand the request for information, they should complete the form themselves.

6. Identity Documents

We need to check your details to ensure that we are disclosing information to the correct person. Please provide an identification document containing your name and address, such as a driving license or medical card. If you do not want to send the original, send a certified copy or visit one of our offices where your details will be checked and the document returned to you.

Please send this form and the appropriate identity documents to:

Data Protection Officer
Whiston J & I School
Saville Road
Whiston
Rotherham
S60 4DX

For office use only:

	Date	Signature
Form Received		
Identity Documents Checked		
Acknowledgement Sent		
Information or No-trace Letter Sent		

[Applicant's name]
[Applicant's address]
[Applicant's postcode]

22 March 2016

Dear [insert name]

Data Protection Act 1998 – Subject Access Request

I acknowledge receipt of your request to access [your / your child's] personal information in relation to [insert subject of request].

Unfortunately I am unable to progress your request as I do not have enough information to be able to locate the records. Please complete the attached application form giving details of any reference numbers or other information which would enable me to trace the information.

Please contact me on the above telephone number if you wish to discuss this matter.

Yours sincerely

[Name]
[Designation]

Enc

Appendix B

[Applicant's name]
[Applicant's address]
[Applicant's postcode]

22 March 2016

Dear [insert name]

Data Protection Act 1998 – Subject Access Request

I acknowledge receipt of your request to access [your / your child's] personal information in relation to [insert subject of request].

In accordance with the terms of the Data Protection Act 1998, [school name] will provide the information requested by [insert date].

I will contact you again to inform you of further progress.

Yours sincerely

[Name]
[Designation]

[Applicant's name]
[Applicant's address]
[Applicant's postcode]

22 March 2016

Dear [insert name]

Data Protection Act 1998 – Subject Access Request

Further to my letter dated [insert date], in relation to your request for information concerning [insert subject of request], I confirm that a search for information has been completed.

I have been unable to locate any information which relates to [you / your child].

Please contact me on the above telephone number if you wish to discuss this matter.

Yours sincerely

[Name]
[Designation]

[Applicant's name]
[Applicant's address]
[Applicant's postcode]

22 March 2016

Dear [insert name]

Data Protection Act 1998 – Subject Access Request

Further to my letter dated [insert date], please find enclosed the information requested in relation to [insert subject of request].

In accordance with the terms of the Data Protection Act 1998, information has been removed where an exemption applies or where information relates to other individuals.

Yours sincerely

[Name]
[Designation]

Encs