Fulford School Information Management Policy

POLICY DOCUMENT	Information Management Policy
Policy Status	Statutory
Lead Member of Staff	Lorna Savage, Headteacher
Publication /Revision Date	November 2017
Governor Committee	Full Governors
Full Governors Ratification Date	
Review Frequency	2 years
Date of next review	November 2019
Publication details: **School Website** **School intranet**	1 December 2017
Purpose	To ensure appropriate collection, processing, sharing, reporting, retention and deletion/destruction of personal / individual/ data subject records and that the school acts in accordance with the law on data protection, privacy and information management.
Supporting documents	Privacy Notices/Privacy Scheme – see Appendices 1 & 2 Record of Freedom of Information and Subject Access requests – see Appendix 3 Record of Data Breaches – see Appendix 4 Record retention schedule – see Appendix 5 Record of destruction of data sources – see Appendix 6 Disclosure Requests – Appendix 7

Fulford School Information Management Policy

Information Management Policy
Fulford School collects, processes, uses, shares, reports, retains and destroys personal information about students, staff, parents or carers and other individuals who come into contact with the school. This information is gathered to enable us to provide education and other associated functions in relation to our employment of staff and duty of care to young people. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing or Privacy Notice to all students/parents or carers and staff, this summarises the information held on students and staff, why it is held and the other parties it may be passed on to.

Purpose
This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act, and other related data protection and privacy 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.

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

What is Personal Information?
Personal information or data is defined as that which relates to a living individual who can be identified from that data, or other information held. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments, opinions or expressions of intentions about an individual and staff development reviews.

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. The difference between processing personal data and sensitive personal data is that there are greater legal restrictions on the latter. Sensitive personal data will be held in pupil and staff records and must be handled with extra care. The school will also contain some personal information that individuals would expect to be treated as private or confidential (whether or not legally classified as sensitive personal data).

For the GDPR:
'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
"special categories of personal data" are:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- data concerning health or sex life and sexual orientation;
- genetic data (*new*); and
- biometric data where processed to uniquely identify a person (*new*).

Data Protection Principles
The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

- Personal data shall be processed fairly and lawfully;
- Personal data shall be obtained only for one or more specified and lawful purposes;
- Personal data shall be adequate, relevant and not excessive;
- Personal data shall be accurate and where necessary, kept up to date;
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
- We must have in place organisational and technical measures to stop unlawful processing and accidental loss or damage to personal data

- Personal data shall be kept secure i.e. protected by an appropriate degree of security and it shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of data protection.

For the GDPR:

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The controller shall be responsible for, and be able to demonstrate compliance with, point 1 ('accountability').

General Statement

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

- Inform individuals why the information is being collected and who it is being shared with
- Take steps to ensure information is shared securely
- Audit the collection, nature, use and storage of personal information
- Check the quality, accuracy and appropriateness of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- 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
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to the rights of individuals such as requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures
- Have clear and robust procedures to minimise and deal with any data breach

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Fulford School Information Management Policy

Information Sharing

All schools share personal information with other organisations and usually with the same types of organisation. 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. The main organisations that schools share personal data with are:

- local authorities;
- other schools and educational bodies; and
- social services.

Personal information can be shared with pupils once they are old enough to be considered responsible for their own affairs, although information can also be shared with their parents or guardians. Pupils old enough to make decisions for themselves are entitled to have their personal information handled in accordance with their rights under the Data Protection Act rather than the rights of their parents acting on their behalf. So if this information is shared with parents, sharing must be in line with the data protection principles.

Information sharing is an important aspect of safeguarding children and vulnerable people. It is important however that information is only shared for this purpose legally and appropriately. Some of the legal or statutory requirements are from the following:

- Children Act 1989
- Children Act 2004 Section 11
- Duty to safeguard and promote the welfare of children
- Data Protection Act 1998 relevant sections such as 29, 35
- Duty to disclose in line with a defined category of public interest: The protection of vulnerable members of the community

When children are suffering or may be at risk of suffering significant harm, concerns must always be shared with children's social care or the police. Fulford School will make it clear to parents that we have general duty to share information with other agencies where we have safeguarding concerns. We will seek to act in line with best practice in sharing information with other agencies, including social services, with the parents' knowledge and consent. However seeking consent is not required, if to do so would:

- place a person at increased risk of harm (usually the child, but also a family member or another person);
- prejudice the prevention, detection or prosecution of a serious crime; or
- lead to an unjustifiable delay in making enquiries.

Information Sharing will be based on the Information Commissioner's Office (ICO) code of practice https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf and will follow the generally accepted guidelines:

- The Data Protection Act will be used as a framework to ensure that personal information about living persons is shared appropriately.
- Open and honest communication should occur with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and their agreement to share this should be obtained, unless it is unsafe or inappropriate to do so.
- Advice should be sought where there is doubt or concern about information sharing**,** without disclosing the identity of the person where possible.
- Information should be shared with consent where appropriate and, where possible, the wishes of those who do not consent to share confidential information should be respected. Information may be shared without consent if, it is judged, that lack of consent can be overridden in the public interest, for example, protection of a vulnerable child or adult. Judgement will be based on the facts of the case.
- Safety and well-being will be considered with information sharing decisions being based on considerations of the safety and well-being of the person and others who may be affected by their actions.
- Sharing must be necessary, proportionate, relevant, accurate, timely and secure: information shared will be necessary for the purpose for which it is shared, will be shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
- Sharing decisions relating to safeguarding should be recorded along with the reasons for information sharing – whether it is to share information or not. Where information is shared what has been shared, who it has been shared with and why it has been shared will be noted. Decisions not to share information relating to safeguarding will be similarly recorded.

Fulford School Information Management Policy

Sharing Child Protection and Safeguarding information with other schools
Child Protection information will be transferred as soon as possible to the pupil's new school, but kept separately from the main pupil file. It is important to transfer this information to prevent harm to a child. Parental consent is not required to transfer this data, since it is held to prevent harm to a child. Parents should be informed of this data transfer and where parents object, the fact should be recorded and the reasons to transfer should be noted.

Where students transfer to our school other than at the Year 6 transition point we will send a letter to the previous school asking for written confirmation whether there are Child Protection records or not.

Where Child Protection or Safeguarding Information is shared by post this will be done securely. The following security protocols, in line with DfE recommendations, will govern this process:
The name, department and address of the recipient will be confirmed.

- The information will be sealed in a double envelope, ensuring the packaging is sufficient to protect the contents during transit.
- The inner envelope will be marked 'Private and Confidential – To be opened by Addressee Only.
- There will be nothing on the outer envelope that would indicate that it contains personal information.
- A return address will be included on both the outer and inner envelopes in case it has to be returned for some reason.
- Where appropriate the information will be sent by recorded delivery or by locally approved courier;
- The recipient will be asked to confirm receipt and a form will be enclosed with the contents for the addressee to sign and return.

Sharing Data with the Police and Law Enforcement Agencies
These guidelines are intended to cover situations where the school receives requests from agencies connected with law enforcement for personal data about students, staff or other individuals whose information is in the school's custody. Usually, such requests will come from the police. However, other government agencies may also request data for law enforcement purposes, such as the Department for Work and Pensions, local authorities, HM Customs and Revenue and the Border and Immigration Agency.

Personal data held by the school has to be managed in accordance with the Data Protection Act 1998. In general, care should be taken to ensure that any disclosure meets the conditions for "fair and lawful" processing set down in the Act, and is done for a purpose which is covered by the School's Data Protection notification with the Information Commissioner.

However, the Data Protection Act includes exemptions which allow personal data to be disclosed to law enforcement agencies without the consent of the individual who is the subject of the data, and regardless of the purpose for which the data were originally gathered. In particular, personal data may be released if:

- The information is required for **safeguarding national security** (Data Protection Act section 28); or
- Failure to provide the data would prejudice the **prevention or detection of crime**, the **apprehension or prosecution of offenders**, or the **assessment or collection of any tax or duty** (Data Protection Act section 29(3)).

Personal data may also be disclosed without contravening the Data Protection Act where the disclosure is required by law. For example, the Social Security Fraud Act 2001 requires education institutions to provide any information to authorised officers of the Department for Work and Pensions or local authorities which they require for the investigation of fraud against the state benefit system. Refusal to provide the information can lead to prosecution of the institution.
Before we is released to a law enforcement agency, we need to ensure that the information is being provided to a genuine and properly authorised investigation.

The school seeks to co-operate with the police and other agencies in the prevention and detection of crime, and the maintenance of a safe environment for the school and the wider community. Personal data which is necessary for a legitimate investigation will normally be released. The points below set out the procedures that should be followed when responding to requests for data, to ensure there are adequate safeguards in place to protect the school against the claim that information has been released contrary to the Data Protection Act.

Responding to requests for information

The following points apply to routine requests for personal data.

Any member of staff who receives a request for personal data from a law enforcement agency must forward it as soon as possible to the Headteacher or Deputy Headteacher (Safeguarding). This applies to data relating to:

- Current or former students or those applying to become students or unsuccessful applicants.
- Current or former staff or job applicants.

The above staff will ensure that the request is handled in accordance with the remainder of these procedures.

Except in Emergency Situations, personal data will only be disclosed in response to an adequate and properly authorised written request.

Police forces have standard forms (known as section 28/section 29(3) forms) for requesting personal data, in accordance with guidance issued by the Association of Chief Police Officers (ACPO). The form should certify that the information is required for an investigation concerning national security, the prevention or detection of crime, or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by a failure to disclose the information. This provides us with a legal basis for supplying the data under the Data Protection Act exemptions. **All requests for personal data from the police, apart from emergency requests, should be required to be on a section 28/section 29(3) form.**

Other law enforcement agencies may not use standard forms. However, any request should:

- Be in writing, on headed paper, and signed by an officer of the agency.
- Describe the nature of the information which is required.
- Describe the nature of the investigation (e.g. citing any relevant statutory authority to obtain the information).
- Certify that the information is necessary for the investigation.

If a properly completed form or letter is received, the data should normally be disclosed. Copies of the form or letter used to request personal data, other correspondence with the law enforcement agency and a copy of any data released should be retained by the School for 6 years.

Emergency situations

An emergency situation is one where we have reason to believe that there is a danger of death or injury to a member of the school or any other person. The police and other emergency services may urgently require personal data from us, and may not have time to complete a formal written request (see Responding to Requests for Information). In these circumstances, any staff member who has access to the data can legally disclose the information, but the safeguards below need to be met:

- If possible, seek the authorisation of a senior manager before providing the data.
- If the request is received by telephone, ask the caller to provide a switchboard number, and call them back through the organisation's switchboard before providing the data. This provides a basic (though not foolproof) way of checking that the call is genuine.
- Ask the enquirer to follow up their request with a formal written request, so that we have this on file. Keep a record of the enquiry and your response, and pass details to the Headteacher or Deputy Headteacher (Safeguarding) as soon as possible.

Data must not be disclosed if you have any doubt as to the validity of the request. In any such instance, ask the enquirer to submit the request in writing, and refer the enquiry to the Headteacher or Deputy Headteacher (Safeguarding).

Records Management

The School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability.

This policy applies to all records created, received or maintained by staff or governors the school in the course of carrying out its functions. Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created or received, and then stored, in hard copy or electronically

The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Head of the School. Individual staff must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System. The pupil record should accompany the pupil to every school they attend and should contain information that is accurate, objective and easy to access. A pupil or their nominated representative have the legal right to see their -le at any point during their education and even until the record is destroyed (when the pupil is 25 years of age or 35 years from date of closure for pupils with special educational needs). This is their right of subject access under the Data Protection Act 1998. It is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner.

Fulford School Information Management Policy

Items which should be included on the pupil record:

- Admission form (application form)
- Fair processing notice [if these are issued annually only the most recent need be on the file
- Parental permission for photographs to be taken (or not)
- Reports to parents
- Assessment/results information
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (should be stored in the file in an envelope)
- Child protection reports/disclosures (should be stored in the file in an envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

The following records should be stored separately to the main pupil record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary weeding of the files once the pupil leaves the school.

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident).

The school which the pupil attended until statutory school leaving age (or the school where the pupil completed sixth form studies) is responsible for retaining the pupil record until the pupil reaches the age of 25 years. This retention is set in line with the Limitation Act 1980 which allows that a claim can be made against an organisation by a minor for up to 7 years from their 18th birthday. Child Protection records should be retained by the last school or college that the young person attends. The records should be kept until the person has their 26th birthday and then securely disposed of.

All pupil and staff records should be kept securely at all times. Paper records, for example, should be kept in lockable storage areas with restricted access, and the contents should be secure within the file. Equally, electronic records should have appropriate security. Access arrangements for records should ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it. Paper records should be checked out of the filing system with the location of the removed file being logged along with the name of the borrower.

The pupil record will be disposed of in accordance with the safe disposal of records guidelines.

Safe Destruction of Records

The Data Protection Act 1998 stipulates that records should be kept for no longer than necessary.

All records containing personal information, or sensitive personal information should be made either unreadable or unreconstructable.

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded

Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by a Senior Manager and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed. The schedule of destruction to record such actions is shown in Appendix 6.

The school needs to maintain a list of records which have been destroyed and who authorised their destruction. Members of staff should record at least:

- File reference (or other unique identifier);
- File title (or brief description);
- Number of files and date range
- The name of the authorising officer
- Date action taken

Fulford School Information Management Policy

Following this guidance will ensure that the school is compliant with data protection and privacy legislation and that we practice good records management.

Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media. It is essential to have procedures in place so that conversion is done in a standard way. This means that organisations can prove that the electronic version is a genuine original and could not have been tampered with in any way. Reference should be made to 'British Standard 10008:2008 'Evidential weight and legal admissibility of electronic information' when preparing such procedures.

Retention Guidelines
Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule listing the record series which the school creates in the course of its business. The retention schedule lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use. The retention schedule lays down the basis for normal processing under both the Data Protection Act 1998 and the Freedom of Information Act 2000.

Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems. The retention schedule refers to record series regardless of the media in which they are stored.

Managing records against the retention schedule is deemed to be "normal processing" under the Data Protection Act 1998 Provided members of staff are managing records in line with the retention schedule they cannot be found guilty of unauthorised tampering with files once a freedom of information request or a data subject access requests has been made.

This retention schedule in Appendix 5 contains recommended retention periods for the different record series created and maintained by schools in the course of their business. The schedule refers to all information regardless of the media in which it is stored. Some of the retention periods are governed by statute while others are guidelines. Every effort has been made to ensure that these retention periods are compliant with the requirements of the Data Protection Act 1998 and the Freedom of Information Act 2000. Managing record series using these retention guidelines will be deemed to be "normal processing" under the legislation mentioned above.

Data Breaches
All data controllers have a responsibility under the Data Protection Act (DPA) 1998 to ensure appropriate and proportionate security of the personal data they hold.

Fulford School processes personal data (including sensitive data), and must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to, personal data. Whilst we take every care to protect data and information, to ensure that it is not changed, lost, stolen or falls into the wrong hands, this guidance will form a point of reference to inform our actions if a breach occurs. A data breach is an incident in which any personal data or sensitive data is compromised, disclosed, copied, transmitted, accessed, lost, stolen or used by unauthorised individuals, whether accidentally or on purpose.

This guidance applies to all users of school information, data, information systems and the school site. It applies to not only staff but also service providers and consultants and encompasses data, information, software, systems, paper documents and personnel.

There has been a data breach if there has been:

- Accidental loss
- Theft of equipment on which data is stored
- Unauthorised access to data
- Human error such as emailing data by mistake
- Leaving copies on MFD
- Failure of equipment
- Loss of data or equipment through natural disasters
- Hacking
- Where information is obtained by deception – "Blagging"

Staff must report any data breaches immediately to their line manager or a member of the SLT using the Breach Management Form – see Appendix 4. Once reported an investigation must start within 24 hours to establish the nature of the breach, the type of data and data sensitivity involved, whether the data is personal data relating to individuals, and if so, who the subjects are and how many are involved.

Fulford School Information Management Policy

RAG rating:

The following criteria are to be used when investigating and risk assessing data breaches:

	Critical	A breach of security involving sensitive personal data and / or a large volume of personal data. The incident has or is likely to cause serious harm or distress (emotional, financial or physical damage) to the individual(s) concerned. The breach will need to be reported to the Information Commissioner's Office and / or is sufficiently serious to warrant urgent remedial action.
	Serious	A breach of security which has resulted in the loss, release or corruption of personal data. The actual or potential harm is limited in duration and / or impact. The incident is not considered sufficiently serious to require reporting to the Information Commissioner's Office but other remedial action is considered necessary.
	Minor /Near Miss	A data breach which has not caused any actual or potential harm.

Helpful tips for the risk assessment

- Protections in place such as encryption.
- The potential harm to the individuals to whom the data relates.
- Numbers affected by the breach.
- Wider consequences to consider, such as a risk to public health or loss of public confidence.

Appropriate steps should be taken to recover data losses wherever possible such as recovering lost equipment, remote "wiping" of equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords if affected.

Breaches will require not just an initial response to investigate and contain the situation but also, a recovery plan including where necessary, damage limitation. This may involve input from ICT, HR and Legal and in some cases contact with external stakeholders and suppliers.

Notification to the individual(s), any external organisation, such as the police or other appropriate regulatory body e.g. the Information Commissioners Office (ICO) or bank(s) should have a clear purpose, whether this is 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. The Senior Information Risk Owner (SIRO, the Headteacher,) will seek advice and will determine whether external notification, individual contact, media briefing or HR processes need to be undertaken. Factors to consider relating to notification are whether individuals could act on the information you provide to mitigate risks, if there are a large number of people affected, or there are very serious consequences, how notification can be made appropriate for particular groups of individuals e.g. if you are notifying children or vulnerable adults.

Not every incident will warrant notification and you need to consider who to notify, what you are going to tell them and how you are going to communicate the message. Any communication with individuals should include a description of how and when the breach occurred, what data was involved and what you have done to respond to the risks posed by the breach. Although until May 2017 there is no legal obligation to report breaches to the ICO, the Commissioner believes that "serious breaches" should be notified. Serious breaches may be considered in the light of harm/distress been caused to individuals or loss of sensitive data. From May 2017 serious data breaches the law requires that all serious breaches are reported to the ICO.

The cause of the breach and the response to it must be reviewed. Policies, procedures and responsibilities must be reviewed in the light of any breach occurring with remedial action taken as appropriate. This review and response will be recorded on the "Breach Management Form" – see Appendix 4.

Fulford School Information Management Policy

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.

Review
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher, or nominated representative.

Contacts
If you have any enquires in relation to this policy, please contact Mrs D Skinner, Office Manager at office@fulford.school.york.sch.uk who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745 3

Fulford School Information Management Policy

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
Requests for information must be made in writing; which includes email, and be addressed to Mrs D Skinner, Office Manager. If the initial request does not provide sufficient details to allow us to locate the information, then further enquiries will be made.

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.

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 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 their 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.

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 sufficient details to locate the information.

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

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.

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.

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

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.

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.

Fulford School Information Management Policy

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.

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.

Fulford School Information Management Policy

Appendix 2

Fair Processing (Privacy) Notices: students in Fulford School

Data Protection Act 1998: How we use student information

We collect and hold personal information relating to our students and may also receive information about them from sources such as their previous school, the local authority and/or the Department for Education (DfE). We use this personal data to:

- support our students' learning
- monitor and report on their progress
- provide appropriate pastoral care; and
- assess the quality of our services

This information, while not an exhaustive list, will include student contact details, a photograph or photographs of the student, assessment information/test results, attendance information, any exclusion information, student destinations after leaving the school, and personal characteristics such as religion and ethnic group, where this information has been supplied. The main student photograph held on the individual student profile will be used by staff for identification purposes only and, save where required by law, will not be divulged to a third party without parental permission. Any other photographs of students will be used in line with parental permissions relating to their use.

Information is also kept relating to any special educational needs a student may have as well as on relevant medical conditions or safeguarding issues. *For students enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) for each student and may also give us details about their learning or qualifications.*

O*nce our students reach the age of 13, the law requires us to pass on certain information to the Local Authority, the DfE and to providers of youth support services in your area who have responsibilities in relation to the education or training of 13-19 year olds. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers and to third parties in line with agreed data processing protocols e.g. university admissions authorities, exam results services and exam boards in order to secure appropriate services for students. Please note this is not a definitive list.*

A parent/guardian can request that only their child's name, address and date of birth be passed to the Local Authority by informing the School Office Manager, Mrs D Skinner. This right is transferred to the student once he/she reaches the age 16.

We will not give information about our students to anyone without your consent unless the law and our policies allow us to do so, for example in relation to the transfer of school records where students move to a new school or college, where safeguarding concerns warrant this disclosure to protect student welfare, where data is required to detect or prevent potential criminal activity or where this is needed to meet the statutory information requirements upon the school. If you want to receive a copy of the information about your son/daughter that we hold, please contact the School Office Manager, Mrs D Skinner.

We are required, by law, to pass certain information about our students to our local authority (LA) and the Department for Education (DfE). Where third parties are granted access to student level data, they must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

The DfE may share student level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and where it is in compliance with the Data Protection Act 1998.

Decisions on whether the DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to student level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

Where the school publishes photographs of students on our website or on publicity materials this will be done in accordance with the permissions supplied to the school by their parents.

For more information on how this sharing process works, please visit: https://www.gov.uk/guidance/national-student-database-apply-for-a-data-extract

For information on which third party organisations (and for which project) student level data has been provided to, please visit: https://www.gov.uk/government/publications/national-student-database-requests-received

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:
http://www.york.gov.uk/info/200600/data_protection/177/data_protection/4 and
http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you are unable to access these websites please contact the LA or DfE as follows:

Information Governance Officer
West Offices,
Station Rise,
York
YO1 6GA
email: data.protection@york.gov.uk
Telephone: (01904) 552933

Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT
Website: www.education.gov.uk
email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

Fulford School Information Management Policy

Appendix 3

Fair Processing (Privacy) Notices: For Fulford School Staff

The Data Protection Act 1998: How we use your information

We process personal data relating to those we employ to work at our school. This is for employment purposes, to aid the running of the school and to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body

This personal data includes identifiers such as names and national insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- our local authority
- the Department for Education (DfE)

If you require more information about how we and/or DfE store and use your personal data please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you want to see a copy of information about you that we hold, please contact Deborah Skinner, Office Manager

Fulford School Information Management Policy

Appendix 4

Breach Management Form – Reporting & Investigation

Please complete this form and return it as soon as possible to Sam Bradford, Business Manager.

Date reported :	
Name of Person reporting:	
Line Manager Name:	
Provide as much details of the incident as you can.	E.g. dates/times, any actions taken so far etc
Explain any reasons if there has been any delay in reporting this incident	
Details of the investigation including any initial steps taken, actions and recommendations with timescales	*For example:* • *whether the data is personal data relating to individuals, and if so who are the subjects and how many are involved.* • *consider the extent of the sensitivity of the data,* • *what might be the consequences of data loss, e.g. extent of harm or distress to individual(s), risk to the organisation etc* • *What measures did we have in place to prevent an incident of this nature occurring?* • *Has there been any previous incidents?* • *any policies and procedures considered relevant to this incident and audit evidence of staffing having read/received these*
Evaluation, response, notification and review : *This is done by the investigation manager . If assessed as a critical data breach involving large amounts of data, or when there has been a breach involving a significant number of peoples' personal data and possible notification to regulator(s) etc, need to include Chief Executive/SIRO/ Director(s) as appropriate*	
RAG Rating :	
Meeting/Discussion date and attendees :	

Fulford School Information Management Policy

Evidence of completed recommendations :	
Signature/s and Date	

Fulford School Information Management Policy

Breach Management - Risk Assessment Q & A

Questions	Answers
Service Area where breach happened or involved	
Lead officer on case	
How did the data loss occur e.g. disclosed in error, loss of encrypted laptop etc	
Nature of breach – what type of personal data is involved e.g. names, medical information etc	
What date did it happen on/or when did someone realise there had been an incident	
How many people are affected	
Any distress/harm caused	
Where is the data now and how many people have seen it	
What is being done to recover the data	
Any protections in place e.g. encryptions	
What could the information tell a third party about the affected data subject(s)	
Are any other agencies involved e.g. contractors, domestic violence team, etc	
Any other agency / regulator notified e.g. press, bank,	
Is ICO notification necessary	
Is it necessary to process as a serious incident requiring investigation and be notified appropriately?	
What policies are in place to support staff	
What training/awareness raising measures have been taken in the light of this episode	
Has there been a previous incident in this service area before and what and when it happened	
If it involves a member of staff have there been any previous incidents involving same staff	
Have any gaps been identified in system to mitigate further incidents	
What steps taken to improve weak areas	
Future monitoring and recommendations	

Fulford School Information Management Policy

Audit Trail/Preserving evidence log

Date/Time	Who consulted	Nature of Activity	Action	Completed
5.9.0.14 0800	*Team Manager*	*Discussion on staff roles and responsibilities*	*As access to this particular site was not required for role, ICT contacted*	*0830*
5.9.14 0900	*Staff involved in breach*	*Interview*	*As motive appears deliberate, matter escalated to HR*	*1000*
5.9.2014 1400	*ICT expert*	*Systems checked for unauthorised use*	*Block on system and agreed to make it a "dedicated user site"*	*1600*

Fulford School Information Management Policy

Data Breach Response template

1. Background

2. Escalation, Containment, audit trail and notification

3. Assessment of the breach

4. Risk assessment, mitigation and evaluation

References:

Information Commissioner's Office - Guide to Data Protection
https://ico.org.uk/for-organisations/guide-to-data-protection/
Information Commissioner's Office – Guide to Data Protection Reform – breach notification
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/

Fulford School Information Management Policy

Appendix 5

Record Retention Schedule

	Basic file description	Data prot Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record
1. Child Protection					
1.1	Child Protection files	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	DOB + 25 years[1]	SECURE DISPOSAL
1.2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance)Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL
[1]This amendment has been made in consultation with the Safeguarding Children Group [2]From January 1st 2005 subject access is permitted into unstructured filing systems and log books and other records created within the school containing details about the activities of individual pupils and members of staff will become subject to the Data Protection Act 1998					
2. Governors					
2.1	Minutes				
	• Principal set (signed)	No		Permanent	Retain in school for 6 years from date of meeting
	• Inspection copies	No		Date of meeting + 3 years	SECURE DISPOSAL (If these minutes contain any sensitive personal information they should be shredded)
2.2	Agendas	No		Date of meeting	SECURE DISPOSAL
2.3	Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting

2.4	Annual Parents' meeting papers	No		Date of report + 6 years	Retain in school for 6 years from date of meeting
2.5	Instruments of Government	No		Permanent	Retain in school whilst school is open
2.6	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required
2.7	Action Plans	No		Date of action plan + 3 years	SECURE DISPOSAL
2.8	Policy documents	No		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)
2.9	Complaint files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years Review for further retention in the case of contentious disputes SECURE DISPOSAL routine complaints
2.10	Annual Reports required by the Department for Education	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years	
2.11	Proposals for schools to become, or be established as Specialist Status schools	No			Current year + 3 years
3. Management					
3.1	Log books	Yes		Date of last entry in the book + 6 years	Retain in school for 6 years from the date of the last entry
3.2	Minutes of the Senior Management Team and other internal administrative bodies	Yes		Date of meeting + 5 years	Retain in the school for 5 years from meeting

3.3	Reports made by the head teacher or the management team	Yes		Date of report + 3 years	Retain in the school for 3 years from meeting
3.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes		Closure of file + 6 years	SECURE DISPOSAL
3.5	Correspondence created by head teacher, deputy head teachers, heads of year and other members of staff with administrative responsibilities	No		Date of correspondence + 3 years	SECURE DISPOSAL
3.6	Professional development plans	Yes		Closure + 6 years	SECURE DISPOSAL
3.7	School development plans	Yes		Closure + 6 years	Review
3.8	Admissions - if the admission is successful	Yes		Admission + 1 year	SECURE DISPOSAL
3.9	Admissions - if the appeal is unsuccessful	Yes		Resolution of case + 1 year	SECURE DISPOSAL
3.10	Admissions - Secondary Schools - casual	Yes		Current year + 1 year	SECURE DISPOSAL
3.11	Proofs of address supplied by parents as part of the admissions process	Yes		Current year + 1 year	SECURE DISPOSAL
3.12	Supplementary information form including additional information such as religion, medical conditions etc.				
4. Pupils					
4.1	Admission Registers	Yes		Date of last entry in the book (or file) + 6 years Reconsider Retention Period. Feedback from Teaching Relative was thought to be 7 Year Retention. These records are no longer generated in paper but electronically	Retain in the school for 6 years from the date of the last entry then consider transfer to the Archives

				held using SIMS BROCON software	
4.2	Attendance Registers	Yes		Date of register + 3 years	SECURE DISPOSAL (If these records are retained electronically any back up copies should be destroyed at the same time)
4.3	Pupil Files Retained in Schools				
4.3b	• Secondary		Limitation Act 1980	DOB of the pupil + 25 years[3]	SECURE DISPOSAL
4.4	Pupil Files	Yes			
4.4b	• Secondary		Limitation Act 1980	DOB of the pupil + 25 years[4]	SECURE DISPOSAL
4.5	Special Education Needs files, reviews and Individual Education Plans	Yes		DOB of the pupil + 25 years the review NOTE: This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. there is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period	SECURE DISPOSAL
[3]If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary [4]As Above					
4.6	Correspondence Relating to Authorised Absence and Issues	No		Date of absence + 2 years	SECURE DISPOSAL
4.7	Examination results	Yes			
4.7a	• Public	No		Year of examinations + 6 years	SECURE DISPOSAL

4.7b	• Internal examination results	Yes		Current year + 5 years[5]	SECURE DISPOSAL
4.8	Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL
4.9	Statement maintained under The Education Act 1996 – Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
4.10	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
[5]If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary					
4.11	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
4.12	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
4.13	Parental permission slips for school trips – where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL
4.14	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE DISPOSAL
4.16	Records created by schools to obtain approval to run an Education Visit outside the Classroom – Secondary Schools	No	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998)	Date of visit + 10 years	N

5. Curriculum					
5.1	School Development Plan	No		Current year + 6 years	SECURE DISPOSAL
5.2	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
5.3	Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.4	Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.5	Class Record Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.6	Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.7	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL

5.8	Pupils' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.9	Examination Results	Yes		Current year + 6 years	SECURE DISPOSAL
5.10	SATS records – Examination Papers and Results	Yes		Current year + 6 years	SECURE DISPOSAL
5.11	PAN Reports	Yes		Current year + 6 years	SECURE DISPOSAL
5.12	Value Added and Contextual Data			Current year + 6 years	SECURE DISPOSAL
5.13	Self-Evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL
6. Personnel Records held in schools					
6.1	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
6.2	Staff Personal files	Yes		Termination + 7 years	SECURE DISPOSAL
6.3	Interview notes and recruitment records	Yes		Date of interview + 6 months	SECURE DISPOSAL
6.4	Pre-employment vetting information (including CRB checks)	No	CRB guidelines	Date of check + 6 months	SECURE DISPOSAL (by designated member of staff)
6.5	Disciplinary proceedings:	Yes	Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice		
6.5a	• Oral warning			Date of warning + 6 months	SECURE DISPOSAL[7]
6.5b	• Written warning – level one			Date of warning + 6 months	SECURE DISPOSAL
6.5c	• Written warning – level two			Date of warning + 12 months	SECURE DISPOSAL
6.5d	• Final warning			Date of warning + 18 months	SECURE DISPOSAL
6.5e	• Case not found			If child protection related please see 1.2 otherwise	SECURE DISPOSAL

				SECURE DISPOSAL immediately at the conclusion of the case	
6.6	Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further	SECURE DISPOSAL
6.7	Annual appraisal/assessment records	No		Current year + 5 years	SECURE DISPOSAL
6.8	Salary cards	Yes		Last date of employment + 85 years	SECURE DISPOSAL
6.9	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year + 3 years	SECURE DISPOSAL
6.10	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current + 6 years	SECURE DISPOSAL
6.11	Proofs of identity collected as part of the process of checking "portable" enhanced CRB disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file	
[7] If this is placed on a personal file it must be weeded from the file					
7. Health and Safety					
7.1	Accessibility plans		Disability Discrimination Act	Current year + 6 years	SECURE DISPOSAL
7.2	Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
7.2a	• Adults	Yes		Date of incident + 7 years	SECURE DISPOSAL
7.2b	• Children	Yes		DOB of child + 25 years[8]	SECURE DISPOSAL

7.3	COSHH			Current year + 10 years [where appropriate an additional retention period may be allocated]	SECURE DISPOSAL
7.4	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL
[8]A child may make a claim for negligence for 7 years from their 18th birthday. To Ensure that all records are kept until the pupil reaches the age of 25 this retention period has been applied					
7.5	Policy statements			Date of expiry + 1 year	SECURE DISPOSAL
7.6	Risk Assessments	Yes		Current year + 3 years	SECURE DISPOSAL
7.7	Process of monitoring areas where employees and persons are likely to have become in contact with asbestos			Last action + 40 years	SECURE DISPOSAL
7.8	Process of monitoring areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	SECURE DISPOSAL
7.9	Fire precaution log books			Current year + 6 years	SECURE DISPOSAL
8. Administrative					
8.1	Employer certificate			Closure of the school + 40 years	SECURE DISPOSAL
8.2	Inventories of equipment and furniture			Current year + 6 years	SECURE DISPOSAL
8.3	General file series			Current year + 5 years	Review to see whether a further retention period is required
8.4	School brochure or prospectus			Current year + 3 years	
8.5	Circulars (staff/parent/pupils)			Current year + 1 year	SECURE DIOSPOSAL
8.6	Newsletters, ephemera			Current year + 1 year	Review to see whether a further retention period is required

8.7	Visitors book			Current year + 2 years	Review to see whether a further retention period is required
8.8	PTA/Old Pupils Associations			Current year + 6 years	Review to see whether a further retention period is required
9. Finance					
9.1	Annual Accounts		Financial Regulations	Current year + 6 years	
9.2	Loans and grants		Financial Regulations	Date of last payment on loans + 12 years	Review to see whether a further retention period is required
9.3	Contracts				
9.3a	• Under seal			Contract completion date + 12 years	SECURE DISPOSAL
9.3b	• Under signature			Contract completion date + 6 years	SECURE DISPOSAL
9.3c	• monitoring records			Current year + 2 years	SECURE DISPOSAL
9.4	Copy orders			Current year + 2 years	SECURE DISPOSAL
9.5	Budget reports, budget monitoring etc.			Current year + 3 years	SECURE DISPOSAL
9.6	Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
9.7	Annual Budget and background papers			Current year + 6 years	SECURE DISPOSAL
9.8	Order books and requisitions			Current year + 6 years	SECURE DISPOSAL
9.9	Delivery documentation			Current year + 6 years	SECURE DISPOSAL
9.10	Debtor DISPOSALs		Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL
9.11	School Fund cheque books			Current year + 3 years	SECURE DISPOSAL
9.12	School Fund – Paying in books			Current year + 6 years then review	SECURE DISPOSAL
9.13	School Fund - Ledger			Current year + 6 years then review	SECURE DISPOSAL
9.14	School Fund - Invoices			Current year + 6 years then review	SECURE DISPOSAL
9.15	School Fund – Receipts			Current year + 6 years	SECURE DISPOSAL

9.16	School Fund bank Statements			Current year + 6 years then review	SECURE DISPOSAL
9.17	School Fund School Journey Books			Current year + 6 years then review	SECURE DISPOSAL
9.18	Student grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
9.19	Free school meals registers	Yes		Current year + 6 years	SECURE DISPOSAL
9.20	Petty cash books			Current year + 6 years	SECURE DISPOSAL
10. Property					
10.1	Title Deeds			Permanent	Permanent, these should follow the property unless the property has been registered at the Land Registry
10.2	Plans			Permanent	Retain in school whilst operational
10.3	Maintenance and contractors		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
10.4	Leases			Expiry of lease + 6 years	SECURE DISPOSAL
10.5	Lettings			Current year + 3 years	SECURE DISPOSAL
10.6	Burglary, theft and vandalism report forms			Current year + 6 years	SECURE DISPOSAL
10.7	Maintenance log books			Current year + 6 years	SECURE DISPOSAL
10.8	ContractorsOSAL6 year		Current year + 6 years	SECURE DISPOSAL	
11. Local Authority					
11.1	Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
11.2	Attendance returns	Yes		Current year + 1 year	SECURE DISPOSAL
11.3	Circulars from LEA			Whilst required operationally	Review to see whether a further retention period is required
12. Department for Children, Schools and Families					
12.1	HMI reports			These do not need to be kept any longer	

12.2	OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required
12.3	Returns			Current year + 6 years	SECURE DISPOSAL
12.4	Circulars from Department for Children, Schools and Families			Whilst operationally required	Review to see whether a further retention period is required
13. Connexions					
13.1	Service level agreements			Until superseded	SECURE DISPOSAL
13.2	Work Experience Agreement			DOB of child + 18 years	SECURE DISPOSAL
14. School Meals					
14.1	Dinner Register			Current year + 3 years	SECURE DISPOSAL
14.2	School Meals Summary Sheets			Current year + 3 years	SECURE DISPOSAL
15. Family Liaison Officers and Home School Liaison Assistants					
15.1	Day Books	Yes		Current year + years then review	SECURE DISPOSAL
15.2	Reports for outside agencies i.e. where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school then destroy	SECURE DISPOSAL
15.3	Referral forms	Yes		While the referral is current	SECURE DISPOSAL
15.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL
15.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	DELETE
15.6	Group Registers	Yes		Current year + 2 years	SECURE DISPOSAL

Fulford School Information Management Policy

Appendix 6

Any records due for destruction must be processed in accordance with the retention periods identified earlier in this documentation.

Record Retention and Disposal Guidance

Disposal of Records				
Department:				
Name:				
Record title:				
Record format:				
Approximate number of records:				
Reason for disposal:				
Method of disposal: (tick as appropriate)	**Destruction:**		**Transferred to Archives:**	
Method of destruction: (if applicable)				
Date of disposal:				
***Authority:**				

* The destruction of records should be approved by an authorised person in line with this policy.

Fulford School Information Management Policy

Appendix Seven

Data Protection Act 1998, - Disclosure requests

To: Fulford School

From:

Please select below the purpose(s) of this enquiry :-

Section 29 (1)

(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.	

Section 35 (1) ent or collection of any tax oatute, case law or court order. Please indicate which you are relying on.....	
Section 35 (2) ent or collection of any tax oatute, case law or court order. Please indicate which you are relying on....g, exercising, or defending legal rights.	

If other, please state:.....

1. **Nature of the enquiry:** *[brief overview including stage of any criminal investigation/charge]*	
2. **Information is required in respect of the following persons:** *Enter here details of the person and address etc if known*	
3. **The information sought is needed to:** *Detail here precisely what information you want to know*	
4. **Consent ereo satisfy s7(6) DPA:**	
I confirm that the personal data requested is required for these purposes as above and failure to provide the information is, in my view, likely to prejudice those purposes	
Signed	Position :
Name	Date

Access Enquiries - Should the existence of this request and any subsequent processing of data become liable to disclosure, please contact the originator immediately for advice before taking any further

School Decision:		
Reasons:		
Signed	Position	Date