General Data Protection Regulation (GDPR)

Data Protection Policy

CATEGORY:	Policy
CLASSIFICATION:	Legal (Reserved Policy)
PURPOSE	Policy covering scope and responsibilities for Data Protection & Biometric Data in Bridgnorth Endowed School.
Controlled Document Number:	**3**
Version Number:	**1**
Controlled Document Lead:	Director of Business & Finance (controller of policy register)
Approved by Governors:	27th June 2018
Review Date:	27th June 2019
Distribution: • **Essential Reading for:** • **Information for:**	 All Managers All Employees

1. Introduction

The General Data Protection Regulations (GDPR) defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Personal information is information about a living individual, who can be identified from the information.

1.1 Bridgnorth Endowed School is committed to protecting the privacy of individuals and handles all personal information in a manner that complies with the GDPR. It is the **personal responsibility** of all employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf to comply with this policy.

1.2 Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990 and the GDPR. All breaches will be investigated and appropriate action taken.

1.3 This policy explains what the school's expectations are when processing personal information and should be read in conjunction with other relevant school policies (such as ICT Policy).

2. GDPR Principles

2.1 The GDPR is supported by a set of 6 principles which must be adhered to whenever personal information is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal information.

2.2 The GDPR principles state that personal information must:

Be processed fairly, lawfully and transparently	**Obtained for a specified, explicit and legitimate purpose**	**Be adequate, relevant and limited to what is necessary**
Be accurate and where necessary up to date	Not be kept longer than is necessary	Be handled ensuring appropriate security

3. Access and Use of Personal Information

3.1 Access and use of personal information held by the school, is only permitted by employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf, for the purpose of carrying out their official duties. Use or access for any other purpose is not allowed. Deliberate unauthorised use and access to copying, destruction or alteration of or interference with any personal information is strictly forbidden.

4. Collecting Personal Information

4.1 When personal information is collected, for example on a questionnaire, survey or an application form, the 'data subject' (that is the person who the information is about) must be told. This is known as a Privacy Notice.

4.2 Personal information collected, must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where anonymous information would suffice.

4.3 If the information is collected for one purpose, it cannot then be used for a different and unconnected purpose without the data subject's consent unless there is another lawful basis for using the information (see section 5 below). It must be made clear to the 'data subject' all the purposes that their information may be used for **at the time the information is collected**.

5. Lawful Basis for Processing

5.1 When Bridgnorth Endowed School processes personal information, it must have a lawful basis for doing so. GDPR provides a list of 'conditions' when we can process personal or 'special category' personal information. This is contained within Article 6 and Article 9 of the regulations ***(see Appendix 1)***.

5.2 The GDPR defines special category personal information as information relating to:

- Race and ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- processing of genetic/biometric data to uniquely identifying a person
- physical or mental health or medical condition;
- sexual life

5.3 Whenever the school processes personal information, it must be able to satisfy at least one of the conditions in Article 6 of the GDPR and when it processes 'special category' personal information; it must be able to satisfy at least one of the conditions in Article 9 of the GDPR as well.

5.4 The school can process personal information if it has the data subject's consent (this needs to be 'explicit' when it processes sensitive personal information). In order for consent to be valid it must be 'fully informed' which means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress and should be recorded.

6. Disclosing Personal Information

6.1 Personal information must not be given to anyone internally or externally, unless the person giving the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information.

6.2 If personal information is given to another organisation or person outside of the school, the disclosing person must identify the lawful basis for the disclosure (see section 4 above) and record their reasoning for using this basis. This record as a minimum should include;

- a description of the information given;
- the name of the person and organisation the information was given to;
- the date;
- the reason for the information being given; and
- the lawful basis.

6.3 If an information sharing agreement or protocol exists, this should be adhered to when providing personal information to others. The agreement/protocol will provide the legal basis for disclosure.

6.4 In response to any lawful request, only the minimum amount of personal information should be given. The person giving the information should make sure that the information is adequate for the purpose, relevant and not excessive.

6.5 When personal information is given either externally or internally, it must be communicated in a secure manner. For external communications use GCSX or the Secure Communications System (SCS), special delivery or courier, etc. For internal communications either hand deliver or make sure you email the information to the correct recipient.

7. Accuracy and Relevance

7.1 It is the responsibility of those who receive personal information to make sure so far as is possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure that it is still accurate and up to date. If the information is found to be inaccurate, steps must be taken to put it right. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded.

7.2 ‘Data subjects’ have a right to access personal information held about them and have errors corrected. More information about a ‘data subject’s’ rights can be found in Section 9 of this policy.

8. Retention and Disposal of Information

8.1 Bridgnorth Endowed School holds a large amount of personal information. The GDPR requires that we do not keep personal information for any longer than is necessary. Personal information should be checked at regular intervals and deleted or destroyed

securely when it is no longer needed, provided there is no legal or other reason for holding it.

8.2 The *Retention Schedule* (see Part 2) must be checked before records are disposed of, to make sure that the prescribed retention period for that type of record is complied with. Alternatively advice should be sought from Information Governance.

9. Individuals Rights

9.1 Individuals have a number of rights under GDPR. These include:

- **The right to be informed** – See section 4 - Collecting Personal Information
- **The right to access** – A person can ask for a copy of personal information held about them (this is known as a Subject Access request - SAR);
- **The right to rectification** – Personal data can be rectified if it is inaccurate or incomplete
- **The right to erasure** – Person can ask for the deletion or removal of personal data where there is no reason for its continued processing
- **The right to restrict processing** – Person has the right to block or suppress processing of their personal data
- **The right of data portability** – Allows a person to obtain and reuse their personal data for their own purposes
- **The right to object** – A person can object to an organisation processing their personal data for direct marketing, on the basis of legitimate interests or for scientific/historical reseach and statistics
- **Rights related to automated decision making/profiling** – A person can ask for human intervention in an automated process

9.2 If any school receives such a request on any of the above matters they should seek advice from the Information Governance Team.

9.3 The school has one calendar month in which to respond to a SAR, provided the applicant has put their request in writing by completing a subject access request form and suitable proof of identification has been supplied. An extension of a further 1-2 months will be applied where a request is deemed complex The Information Governance Team co-ordinates the processing of all SAR requests. ***See Appendix 2*** for a copy of the SAR form.

10. Reporting Security Incidents

10.1 Bridgnorth Endowed School has a responsibility to monitor all incidents that occur within the organisation that may breach the security and/or the confidentiality of its information. All incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that the school can learn from its mistakes and prevent losses recurring.

10.2 Specific procedures have been developed for the reporting of all information security incidents. It is designed to make sure that all relevant information is communicated correctly so that timely corrective action can be taken. The documents below need to be read, understood and followed (see Part 3):

- Information Security Breach Procedure – under ‘I’ on intranet
- Data Breach Investigation – under ‘D’ on intranet

10.3 All employees (permanent, temporary and contractors) must be aware of the procedures and obligations in place for reporting the different types of incidents which may have an impact on the security of the school’s information.

Article 6 Conditions – Personal Data

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. **This shall not apply to processing carried out by public authorities in the performance of their tasks.**

Article 9 Conditions – Special Category Data

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 2

General Data Protection Regulations
Right of Access to Personal Data

SUBJECT ACCESS REQUEST FORM

Information

We should respond to your request within one calendar month. However this period does not start until:

a) We are satisfied about your identity
b) You have provided enough detail to locate the information you are seeking

Please complete the following sections of this form providing as much information as possible to help us deal with your request.

1. Provide details of the person about whom the school is holding data (the Data Subject)

Full Name (Print) _____

Date of Birth _____

Present Address:	Previous Address (if less than 3 years at your present address):
Post Code:	Post Code:

Telephone Number _____

Email address _____

2. Are you requesting information about yourself (person referred to in question 1)? If **YES**, then go to question 3. If **NO** please complete the following:

Full Name (Print) _____

Present Address:

Post Code:

Telephone Number: _____

Email address: _____

Relationship with data subject and brief explanation as to why you are requesting this information rather than the data subject:

_____

_____

If you are acting on behalf of the data subject you will need to enclose their written authority including a signature or other legal documentation (e.g. power of attorney) to confirm this request. You also need to enclose evidence of your identity and that of the data subject (see section 4 for details of acceptable identity)

3. Please provide a clear description of the information that you are requesting, see table below. **If you provide <u>specific</u> details of what information you want, e.g. name of a document relevant to a time period rather than just the whole of your file you may receive a quicker response.**

Description of Information	School Service Holding this Information	Time Period for Information Requested

If you are asking for social care information please provide the name of your Social Worker or Personal Assistant	Name:

4. Please provide **two** pieces of evidence of your identity (one containing a photo). Acceptable types of documents used to verify your identity are detailed below.

Driving Licence	Passport	National ID Card	Medical Card	Utility Bill

You may wish to send your documents special/recorded delivery. Your proof of identity will be returned to you securely after verification.

5. All information in respect to your request will be sent to you via secure email unless alternative arrangements are made. We may require further evidence of your identity if you collect your information from school premises.

Declaration

To be completed by all applicants. Please note that any attempt to mislead the school may lead to prosecution.

I (insert name) _____

_____

certify that the information given on this application form and any attachments therein to Bridgnorth Endowed School is accurate and true.

I understand that it is necessary for the school to confirm my identity and it may be necessary to obtain more information in order to locate the correct information.

Signature _____

Date _____

Return of the Form

If you are either posting your documents and payment or hand delivering them then our address is detailed below:

Information Governance
Mrs Susan Underhill
Bridgnorth Endowed School
Northgate
Bridgnorth
Shropshire
WV16 4ER

Our email address is ***sunderhill@bridgnorthendowed.co.uk***

How we will send you the information you have requested

We want you to receive the information you have requested in the most convenient way for you.

However we do have an obligation under the General Data Protection Regulations to provide you with the information you have requested in the most secure way possible.

We believe the most secure way to provide you with the information is either:

- For you to collect the documentation in person from our offices
- For us to email you the information securely/encrypted using our Secure Communication System which would allow you to electronically access the information requested (free of charge)

We can post your information to you but there are risks attached to providing you with your information using this method, e.g. Royal Mail may lose your information, deliver it to the wrong address, etc.

Please confirm you are happy to receive your information by our Secure Communication System by ticking the box below and confirming the email address that your information should be sent to:

Tick Box		EMAIL ADDRESS	

Alternatively if you prefer any of the other methods below please indicate which by ticking ONE of the boxes below:

Collection in person		CD or Paper Copy *(please circle your choice)*

By Post (special delivery)		CD or Paper Copy *(please circle your choice)*

GDPR Policy Part 2

RECORDS & RETENTION

The following document is taken from the Information & Records Management Society – School Toolkit ***http://irms.org.uk/page/SchoolsToolkit***

The relevant sections are shared with staff as part of staff induction and all staff should refer to this prior to secure disposal of any documentation / records.

Facilities are made available for staff to securely dispose of sensitive records.

This policy is linked to the General Data Protection Regulations (GDPR) Data Protection Policy.

Management of the school

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL
1.1.2	Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
	Inspection Copies 2			Date of meeting + 3 days	If these minutes contain any sensitive, personal information they must be shredded.

1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
1.1.4	Meeting papers relation to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002 Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL
1.1.5	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County archives service when the school closes
1.1.6	Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County archives service when the school closes
1.1.7	Action plans created and administered by the Governing body	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8	Policy documents created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL

1.1.9	Records relating to complaints dealt with by the Governing Body	Yes		Date if resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.1.10	Annual Reports created under the requirements of the Education (Governors Annual Reports) (England) (Amendment) Regulations 2002		(Governors Annual Reports) (England) (Amendment) Regulations 2002	Date of report + 10 years	SECURE DISPOSAL
1.1.11	Proposals concerning the change of status of a maintained school including Special Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

1.2 Headteacher and Senior Management	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
1.2.1	Log books of activity in the school maintained by the Headteacher	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be a permanent historical value and should be offered to the County Archives Service if appropriate
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative responsibilities bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of report + 3 years then review	SECURE DISPOSAL
1.2.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities.	There may be data protection issues if the minutes refers to individual pupils or members of staff			SECURE DISPOSAL
1.2.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities.	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL

1.2.6	Professional development plans	Yes	Life of plan + 6 years	SECURE DISPOSAL
1.2.7	School development plan	No	Life of plan + 3 years	SECURE DISPOSAL

1.3 Admissions Process	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
1.3.1	All records relating to the creation and implementation of the Schools Admission Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy +3 years then review	SECURE DISPOSAL
1.3.2	Admissions- if the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions- if the admission is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL

1.3.4	Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.	REVIEW Schools may wish to consider keeping the admission register permanently as often school receive enquiries from past pupils to confirm the dates they attended the school
1.3.5	Admissions- Secondary schools- Casual	Yes		Current year + 1 year	SECURE DISPOSAL
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	Schools Admission Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Current year + 1 year	Current year + 1 year
1.3.7	Supplementary Information form including additional information such as religion, medical conditions	Yes			
	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process co	SECURE DISPOSAL

1.4 Operational Administration	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
1.4.1	General files series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
1.4.2	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
1.4.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
1.4.5	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

2. Human Resources

This section deals with all matters of Human Resources management within the school

2.1 Recruitment	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
2.1.1	All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading to to the appointment of a new member of staff- unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.1.4	Pre- employment vetting information- DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73,74	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months.	

2.1.5	Proofs of identity collected as part of the process sod checking “portable” enhanced DBS 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 members of staff’s personal file.	
2.1.6	Pre-employment vetting information- Evidence providing the right to work in the United Kingdom	Yes	An employer’s guide to right to work checks (Home Office May 2015)	Where possible these documents should be added to the Staff Personal File (see below), but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years.	

2.3 Management of Disciplinary and Grievance Processes	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded.	Yes	“Keeping children safe in education Statutory guidance for school and colleges March 2015”;	Until the person’s normal retirement ages or 10 years from the date of the allegation whichever	SECURE DISPOSAL These records must be shredded.

			Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	
2.3.2	Disciplinary Proceedings	Yes			
	Oral warning			Date of warning + 6 months	SECURE DISPOSAL (If warnings are placed on personal files they must be weeded from the file)
	Written warning- level 1			Date of warning + 6 months	
	Written warning- level 2			Date of warning + 12 months	
	Final warning			Date of warning + 18 months	
	Case not found			If they incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

2.4 Health and Safety	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
2.4.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	Records relating to accident/injury work	Yes		Date of incident + 12 years. In the case of serious accident a further retention period will need to be applied.	SECURE DISPOSAL
2.4.4	Accident reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	Adults			Date of incident +6years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to health Regulations 2002. SI 2002 NO 2677 Regulation 11;	Current year + 40 years	SECURE DISPOSAL

			Records kept under the 1994 and 1999 Regulations to be kept as id the 2002 Regulations had not been made. Regulation 18 (2)		
2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last Action + 50 years	SECURE DISPOSAL
2.4.8	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL

2.5.1 Payroll and pensions	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960) revised 1999 (SI999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

3. Financial Management of the School

This section deals with all aspects of the financial management of the school including the administration of school meals

3.1 Risk Management and Insurance	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL

3.2 Asset Management	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

3.3 Accounts and Statements including Budget Management	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL

3.3.2	Loans and grants managed by the school	No		Date of last payment on the loan +12 years then REVIEW	SECURE DISPOSAL
3.3.3	Student Grant Applications	Yes		Current year + 3 years	SECURE DISPOSAL
3.3.4	All records relating to the creation and management of budgets including Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current year +6years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No		Current financial year +6years	SECURE DISPOSAL

3.4 Contract Management	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
3.4.1	All records relating to the management of contract under seal	No	Limitation Act 1980	Last payment on the contract +12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract +6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year +2years	SECURE DISPOSAL

3.5 School Fund	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
3.5.1	School Fund- Cheque books	No		Current year +6years	SECURE DISPOSAL
3.5.2	School Fund- Paying in books	No		Current year +6years	SECURE DISPOSAL
3.5.3	School Fund-Ledger	No		Current year +6years	SECURE DISPOSAL
3.5.4	School Fund- Invoices	No		Current year +6years	SECURE DISPOSAL
3.5.5	School Fund- Receipts	No		Current year +6years	SECURE DISPOSAL

3.5.6	School Fund- Bank Payments	No		Current year +6years	SECURE DISPOSAL
3.5.7	School Fund- Journey Books	No		Current year +6years	SECURE DISPOSAL

3.6 School Meals Management	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
3.6.1	Free School Meals Registers	Yes		Current year +6years	SECURE DISPOSAL
3.6.2	School Meal Registers	Yes		Current year +3years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets	No		Current year +3years	SECURE DISPOSAL

4. Property Management

This section covers the management of buildings and property

4.1 Property Management	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
4.1.1	Title deeds of properties belonging to the school	No		PEMANENT These should follow the property unless the property has been	

				registered with the Land Registry	
4.1.2	Plans of property belong to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Leases of property leased by or the school	No		Expiry of lease +6years	SECURE DISPOSAL
4.1.4	Records relating to the letting of the school premises	No		Current financial year +6years	SECURE DISPOSAL

4.2 Maintenance	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year +6years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		Current year +6years	SECURE DISPOSAL

5. Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above.

5.1 Pupil's Educational Record	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Primary		Limitation Act 1980 (Section 2)	Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • To another primary school • To a secondary school • To a pupil referral unit • If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupils transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained

	Secondary			Date of birth of the pupil +25years	for the statutory retention period. Primary schools do not ordinarily have sufficient storage space to store records for pupils who have nit transferred in the normal way. It makes more sense to transfer the record to the local Authority as it is more likely that the pupil will request the record from the Local Authority. SECURE DISPOSAL
5.1.2	Examination Results- Pupil Copies	Yes			
	Public		The information should be added to the pupil file	All uncollected certificates should be returned to the examination board.	
	Internal		The information should be added to the pupil file		

5.2 Attendance	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
5.2.1	Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made	SECURE DISPOSAL
5.2.2	Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of birth of the pupil +25 years	REVIEW NOTE: This retention period is the minimum retention 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 of business risk analysis involved in any decision to keep the

					records longer than the minimum retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil +25 years (This would normally be retained on the pupil file)	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability act 2001 Section 2	Date of birth of the pupil +25 years (This would normally be retained on the pupil file)	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability act 2001 Section 14	Date of birth of the pupil +25 years (This would normally be retained on the pupil file)	SECURE DISPOSAL unless the document is subject to a legal hold

6. Curriculum Management

6.1 Statistics and Management Information	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
6.1.1	Curriculum returns	No		Current year +3years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year +6years	
	SATS Records	Yes			
6.1.3	Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year +6years to allow suitable comparison	SECURE DISPOSAL
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL

6.1.3	Published Admission Number (PAN) Reports	Yes		Current year +6years	SECURE DISPOSAL
6.1.4	Value added and contextual data	Yes		Current year +6years	SECURE DISPOSAL
6.1.5	Self-Evaluation Forms	Yes		Current year +6years	SECURE DISPOSAL

6.2 Implementation of Curriculum	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
6.2.1	Schemes of work	No		Current year +1year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.2	Timetable	No		Current year +1year	
6.2.3	Class record books	No		Current year +1year	
6.2.4	Mark books	No		Current year +1year	
6.2.5	Record of homework	No		Current year +1year	
6.2.6	Pupil's work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year +1year	SECURE DISPOSAL

7. Extra-Curricular Activities

7.1 Educational Visits outside the classroom	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the classroom- Primary Schools	No	Outdoor Education Advisors' Panel National Guidance website http://oeapng.info specifically Section 3- "Legal Framework and Employer Systems" and Section 4- Good practice	Date of visit +14years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom- Secondary Schools	No	Outdoor Education Advisors' Panel National Guidance website http://oeapng.info specifically Section 3- "Legal Framework and Employer Systems" and Section 4- Good practice	Date of visit +10years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trip where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the

					storage capacity to retain every single consent form issues by the school for this period.
7.1.4	Parental permission slips for school trips- where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

7.3 Walking bus	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
7.3.1	Day books	Yes		Current year +2years then review	
7.3.2	Reports for outside agencies- where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school then destroy	
7.3.3	Referral forms	Yes		While the referral is current	

7.3.4	Contract data sheets	Yes		Current year then review, if contract is no longer active then destroy	
7.3.5	Contract database enteritis	Yes		Current year then review, if contract is no longer active then destroy	
7.3.6	Group registers	Yes		Current year +2years	

8. Central Government and Local Authority

This section covers records created in the course of interaction between the school and the local authority

8.1 Local Authority	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
8.1.1	Secondary Transfer Sheets (Primary)	Yes		Current year +2years	SECURE DISPOSAL
8.1.2	Attendance returns	Yes		Current year + 1year	SECURE DISPOSAL
8.1.3	School Census Returns	No		Current year +5years	SECURE DISPOSAL
8.1.4	Circulars and other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL

8.2 Central Government	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
8.2.1	Ofsted reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2	Returns made to central government	No		Current year +6years	SECURE DISPOSAL
8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL

GDPR Policy Part 3

Information Security Breach Procedure

What to do in the event of a possible databreach / incident

1. Introduction

1.1 This procedure supports the school's ICT security policy and **must be read in conjunction** with it. This procedure details the necessary steps to take if you have concerns that there has been a breach of personal identifiable information (PII – see 1.2 for examples) by school employees, community members or third parties[1] contracted to provide school services.

1.2 Some typical examples of PII include, but are not limited to:-

- **Personal Data –** e.g. name; address; telephone number; date of birth; NI number; bank account details
- **Sensitive/Special Personal Data –** e.g. information specifically relating to physical or mental health or condition; race or ethnicity; political opinions; religious beliefs, or beliefs of a similar nature; membership of a trade union or non-membership;; sexual life; commission or alleged commission of an offence;

1.3 The principles of securing information (in accordance with Principle 7 of the Data Protection Act and principle 6 of the General Data Protection Regulations from May 2018), can be found in individual schools ICT and security policies. For further guidance on information security contact the Director of Business & Finance on 01746 762103.

2. What is a possible breach of PII?

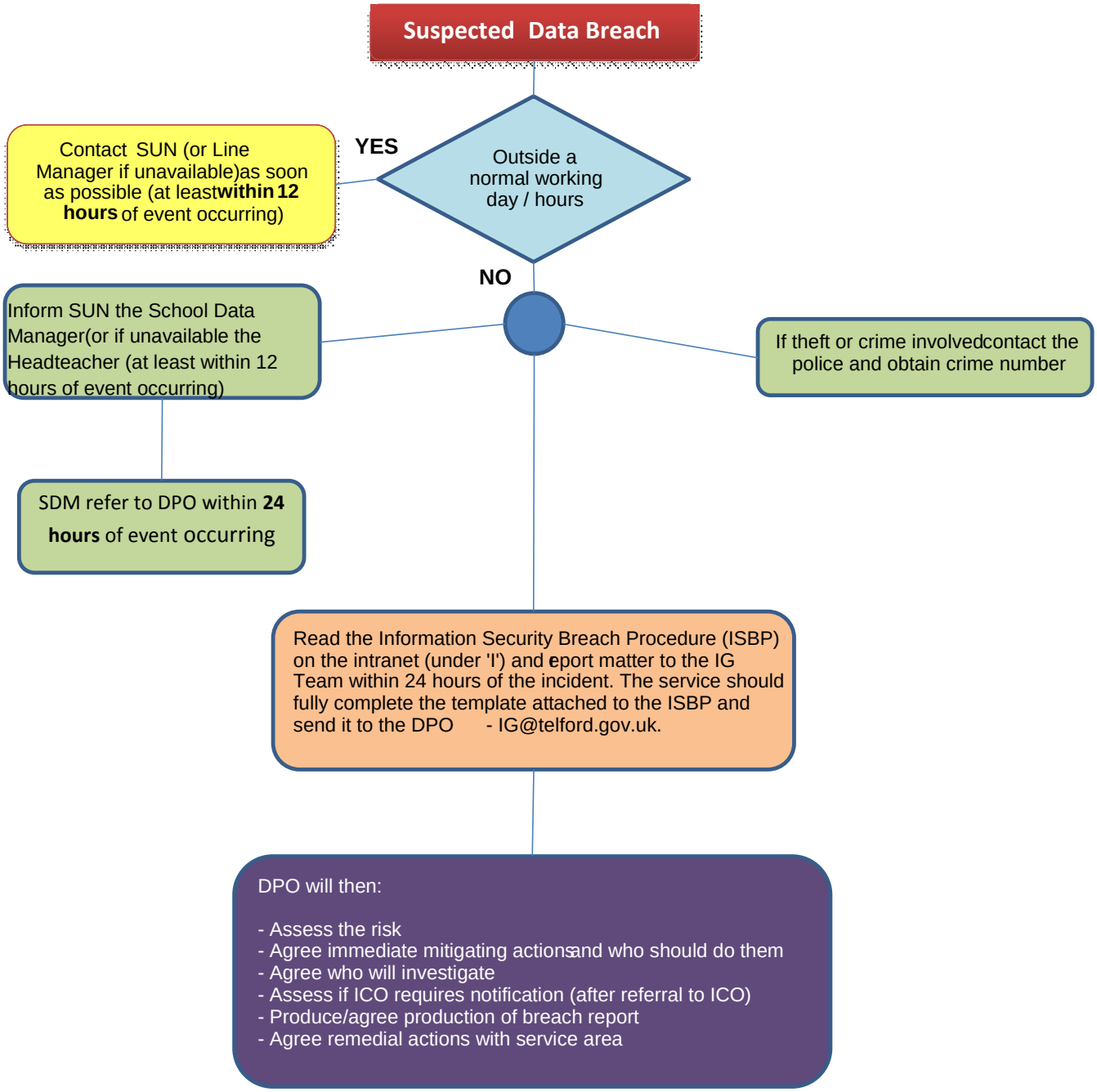
2.1 A breach of PII is where identifiable personal information has been or has the potential to be:

- Viewed or copied by an individual unauthorised to do so,
- Communicated to an unauthorised individual/organisation, e.g. sent to wrong address and opened/read
- Lost or stolen

There are many examples of what constitutes a possible data breach, typical examples are detailed below:

- Loss of mobile phone/laptop or other ICT equipment
- PII being emailed/posted/faxed to an unintended recipient or address and read by the individual, e.g. a letter containing social care information or financial information about an individual being sent to 36 Smith Street instead of 63 Smith Street (the intended recipient) and opened
- Loss of information/records relating to individuals and read by an unauthorised person, e.g. a lost file containing personal grant information
- Viewing PII on an ICT system that you do not need to access as part of your role
- Not keeping information secure; i.e. leaving correspondence on your desk at the end of the working day

[1] Third parties could include temporary employees, agency workers, volunteers, partners or contracted service providers



2.2 There may be security incidents where PII has been given to an unauthorised person (due to a human or procedural error) but the recipient has not opened/read the PII. The PII has then been returned or it has been confirmed that it has been destroyed. Cases such as these should be notified to the data manager and they will be expected to undertake their own investigation into the security incident and implement actions that will minimise the possibility of a similar incident in the future.

3. What should I do if I become aware of a possible data breach?

3.1 Outside a normal working day

3.1.1 If you become aware of a possible data breach you should report it immediately where you can. If this occurs outside normal working hours, e.g. bank holidays, weekends, etc., please contact your SDM (or line manager if SDM is unavailable) within 12 hours of the incident occurring. At Bridgnorth Endowed School,

the DPM is Sue Underhill. She will liaise with the Strategy Committee of the Board of Governors over any significant issues.

3.2 Normal working day

3.2.1 If a breach occurs or you suspect one has occurred you will need to inform your line manager (who will inform the SDM or if not available the Headteacher immediately (or as a minimum within 12 hours of incident occurring). The matter must then be forwarded to the DPO within 24 hours of the incident occurring for recording and investigation.

3.2.2 If the incident involves theft or a crime then you should contact the police and report this. Please make sure you obtain and record a crime reference number from the police where applicable.

3.2.3 If the incident involves the loss or theft of ICT equipment then this should also be logged with the ICT Service Desk on 01952 383333 or via your desktop link.

3.2.4 When the matter is reported to the DPO and ICT (where relevant) the following information as a minimum should be to hand:

- Crime reference number given to you by the police (if applicable)
- Police station and constabulary the incident was reported to (if applicable)
- Place, time and date(s) the incident occurred
- Staff member and/or team(s) or 3rd party suppliers involved
- A summary of the information that has been lost, stolen or incorrectly communicated
- A list of the individuals affected or that could be at risk
- A list of organisations that may need to be contacted (e.g. shared service information), if applicable
- Confirmation as to who else in the authority has been informed, e.g. SDM, Headteacher, etc

3.2.5 When the incident is reported to the DPO they will:

- Assess the level of the risk associated with the incident
- Agree the immediate mitigating actions that should take place and who should undertake them including who else needs to be informed (internally and externally)
- Agree who will undertake an investigation into the incident – low risk will be the service area; medium – service area/IG by agreement; high risk – IG.
- Compare the incident against notification rationale outlined by the Information Commissioners Office (ICO) and notify (after approval by the SIRO) if applicable
- Produce or agree the production of an incident report, see ***Appendix 1*** for required layout
- Agree remedial action to be taken by the relevant service area
- Communicate any lessons learnt corporately where appropriate

3.2.6 Managers can obtain guidance on possible action to be taken in relation to employees implicated in data breaches by accessing the relevant Human Resources guidance document.

4. Advice and assistance

4.1 Supplementary guidance in respect to managing data breaches in specific service delivery units (due to the nature/volume of information being handled) has been agreed locally with the relevant Service Delivery Manager(s) and Assistant Director(s). This local guidance does not replace the requirements of this policy.

4.2 If you require any further information, or if you experience any difficulties accessing any documentation, please contact:-

Audit & Governance
Tel: 01952 382537
Email: ig@telford.gov.uk

4.3 Alternative formats (i.e. hard copy, large print or Braille) of this procedure are available upon request.

Suggested Report Template

Appendix 1

(Input in grey below are example entries only)

Tick relevant box

Breach?	✓	Incident?	

See section 2 of ISBP for guidance on what constitutes a breach or incident

Date Occurred	*10/12/13*	Officer Implicated	*R Montgomery*

Date and name of SDM informed (and the AD where relevant)	Was breach/incident identified as a result of a customer complaint (Y or N?)	
10/12/12/17 - Suzanne Dodd		*Y*

Categories of Data Breached	Number of Individuals Affected	Number of Records Breached
Name, Address, Bank details	*1*	*6*

Description of breach/incident (including the type of information and date/location of incident)
Bank statements collected for identification purposes returned to 15 Darby Road on 10/12/13 instead of correct address 51 Darby Road

Reported to police Y/N?	*N*	Date Reported / Police Station	*N/A*	Crime number	*N/A*

Has information been returned to school or destroyed?	Do you intend to notify the data subject(s) affected? If YES please consult DPO prior to doing this If NO please give an explanation for this
Information returned to Council on 12/12/13	*Yes – as they will be able to ask their bank to watch their account*

How did breach/incident occur?
Officer had incorrectly updated the contact record for this customer

Measures already taken to address breach
1. Procedures for updating contact records reissued to all staff *2. Warning of this incident emailed to all staff* *3. QA checks to be put in place monitoring contact records accuracy*

BELOW SECTIONS TO BE COMPLETED ONCE INVESTIGATION ENDED

Description of action (if any) taken against officer implicated in the breach/incident
Informal discussion with SDM and warning about future conduct

Lessons learnt to be implemented (if relevant)
1. Procedures for updating contact records reissued to all staff *2. Warning of this incident emailed to all staff* *3. QA checks to be put in place monitoring contact records accuracy*