Trusted Schools' Partnership

General Data Protection Regulation

(GDPR)

Data Protection Policy

FREQUENCY OF REVIEW:	**Every two years**
RATIFICATION:	**Autumn Term 2020**
DATE OF NEXT REVIEW:	**Autumn Term 2022** **unless there is a material change**
RATIFIED BY:	

1. Introduction & Scope of Policy

1.1 This policy is based on the requirements of the latest Information Commissioners Office (ICO) Data Sharing Code of Practice. The policy will help ensure any sharing is fair, transparent and in line with the Data Protection Act 2018 (DPA 18) and the rights and expectations of the people whose information is being shared.

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

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. This policy explains what the Trust's expectations are when processing personal information and should be read in conjunction with other relevant Trust policies and School Policies (such as the ICT and E-Safety Policy).

2. What do we mean by data/information sharing

2.1 Information sharing is the disclosure of data from one or more organisations to a third party organisation(s), or the sharing of information between different parts of the School.

2.2. This policy covers the sharing of personal information on a systematic and exceptional basis.

2.2.1 **Systematic Information Sharing** – this involves the routine sharing of the same or similar information for the same person between a set number of organisations. Sharing ordinarily takes place under the conditions of an agreed information sharing agreement.

2.2.2 **Exceptional Information Sharing** – these are one off adhoc decisions to share information

2.3 It is important to remember that data protection principles also apply to information shared **within** the School as well as sharing with external organisations.

3. Information Sharing and the Law

3.1 The School derives its powers to share information from either Acts of Parliament or other legislation that governs the Council's activities.

3.2 The first point to consider before sharing information is what legal basis is there to share information. The legal basis will ordinarily fit into one of three categories.

3.2.1 **Express obligations** – This is where there is an established legal requirement for the School to share information. An example of this would be legislation that requires the School to share information with Her Majesty's Revenues & Customs (HMRC) for taxation purposes.

3.2.2 **Express powers** – The School will be given legal powers to enable the sharing of information. An example of this is the Strengthening Families programme that allows the School to share information with the Department of Work & Pensions (DWP).

3.2.3 **Implied powers** – Certain legislation regulates how School services are run but does not give express powers to share information. However to meet the requirements of the legislation there is implied power to share information. An example here would be the Children's Act which requires Schools to protect children. To protect a child the School may have to share information with a number of organisations.

4. Deciding on Sharing Personal[1] Information

4.1 There are a number of factors to be considered before information sharing takes place. The following questions need to be considered before sharing.

4.1.1 **What is sharing meant to achieve?** A clear objective for sharing should be identified. This will assist in deciding on what elements of information need to be shared.

4.1.2 **What information needs to be shared?** Only the elements of information required to meet the objective identified should be shared. Where opinion is being shared it should be clearly denoted that this is an opinion being shared.

4.1.3 **Who requires access to the shared information?** 'Need to know' principles should be applied. Individuals should only be able to access shared information if they need to.

4.1.4 **When should it be shared?** It should be recorded whether the sharing was on an exception or systematic basis.

4.1.5 **How should it be shared?**
Externally - Information should only be shared securely, e.g. electronically using secure email or hand delivered to named individuals or sent by post (special delivery/secure courier) dependent on the level of sensitivity of the information being shared.

Internally- if sharing is electronic and to/from @telford.gov.uk or @taw.org.uk then this a secure method. However the correct recipients details should be checked before an email is sent. If hard copy information is being shared then hand delivery/collection should be considered for special category (very sensitive) personal information.

4.1.6 **What are the risks in sharing and not sharing the information?** A number of questions should be asked such as what is the potential benefit/harm/damage to an individual whose information may be shared, will an individual be likely to object, etc.

4.1.7 **Can the objective be met without sharing the information or by anonymising it?** If an objective can be met by sharing anonymised information or by not sharing personal information at all then the objective should be met in this alternative way.

4.1.8 **Record what you have shared**. Once you have decided there is adequate justification to share information then the actual sharing should be recorded including what information was shared, to who, when and by who.

4.2 Obtaining consent from individuals to share their personal information should also be factored into the decision making process for sharing information. Consent should be a positive action, specific, given freely, granular and provide an informed indication of the wishes of the individual that they agree to how their personal data will be processed.. See school Guidance Note on Consent.

4.3 It is not always appropriate to obtain consent from an individual (or in fact inform them that sharing is taking place) for sharing their information. Consent is not needed for all aspects of personal information sharing. An example of this is where the School is required to provide the police with information for the prevention and detection of crime or for the protection of children/vulnerable adults. However a legal basis is **always** required before any sharing occurs.

[1] The term personal information is used to generically include personal and sensitive information

5. Fairness and Transparency

5.1 To share information in a fair and transparent manner, individuals should be aware of which organisations are sharing their personal data, with whom and what it is being used for. Fairness also relates to how personal information is shared in that this should happen in a reasonable way that the individual would not reasonably object to. However there are certain exceptions to this, see 4.3 above.

5.2 Fairness and transparency can be achieved by the use of privacy notices which, as a minimum, tells an individual from whom information is being collected why their information will be shared and who it is going to be shared with (either named organisations or types of organisation). See school Guidance Note on Lawful Processing of Personal Data.

6. Security When Sharing Information

6.1 The DPA 18 requires the School to have adequate technical and organisational measures in place to protect personal information. This requirement also covers when the School shares information.

6.2 There are a number of security issues that should be considered in respect to shared / sharing the information.

6.2.1 Information must be shared in a secure manner, see paragraph 4.1.5 for further detail.
6.2.2 Information received from other organisations should be reviewed to ensure there are no conditions of use attached to it and it needs to be kept secure.
6.2.3 Information sent from the School to other organisations should be reviewed to ensure officers understand who will access it and for what purpose.
6.2.4 More sensitive information shared should be afforded additional security.
6.2.5 The level of impact of a data breach on both the individual(s) and the Council

6.3 For more information on required security arrangements please read the schools Information Security Policy.

7. Governance Arrangements

7.1 Responsibility for sharing information lies with the 'Information Asset Owner'. The Information Asset Owner is the Head Teacher.

7.2 The information owner should ensure there are appropriate arrangements in place to share information that comply with the requirements of this policy.

7.3 A further element of governance in respect to information sharing is the use of information sharing agreements (ISA's). An information sharing agreement sets out a number of common rules to be adopted by the various organisations involved in the data sharing operation.

7.4 It is good practice to have an ISA in place if information sharing is taking place on a large scale or on a regular basis. The checklist for the contents of an ISA should be adhered to when drafting an ISA, the checklist can be found in the school office.

8. Reporting Security Incidents

8.1 If the information shared is compromised, e.g. sent to an incorrect recipient, viewed by an unauthorised individual, etc. the schools Information Security Breach Procedure (ISBP) should be instigated immediately.

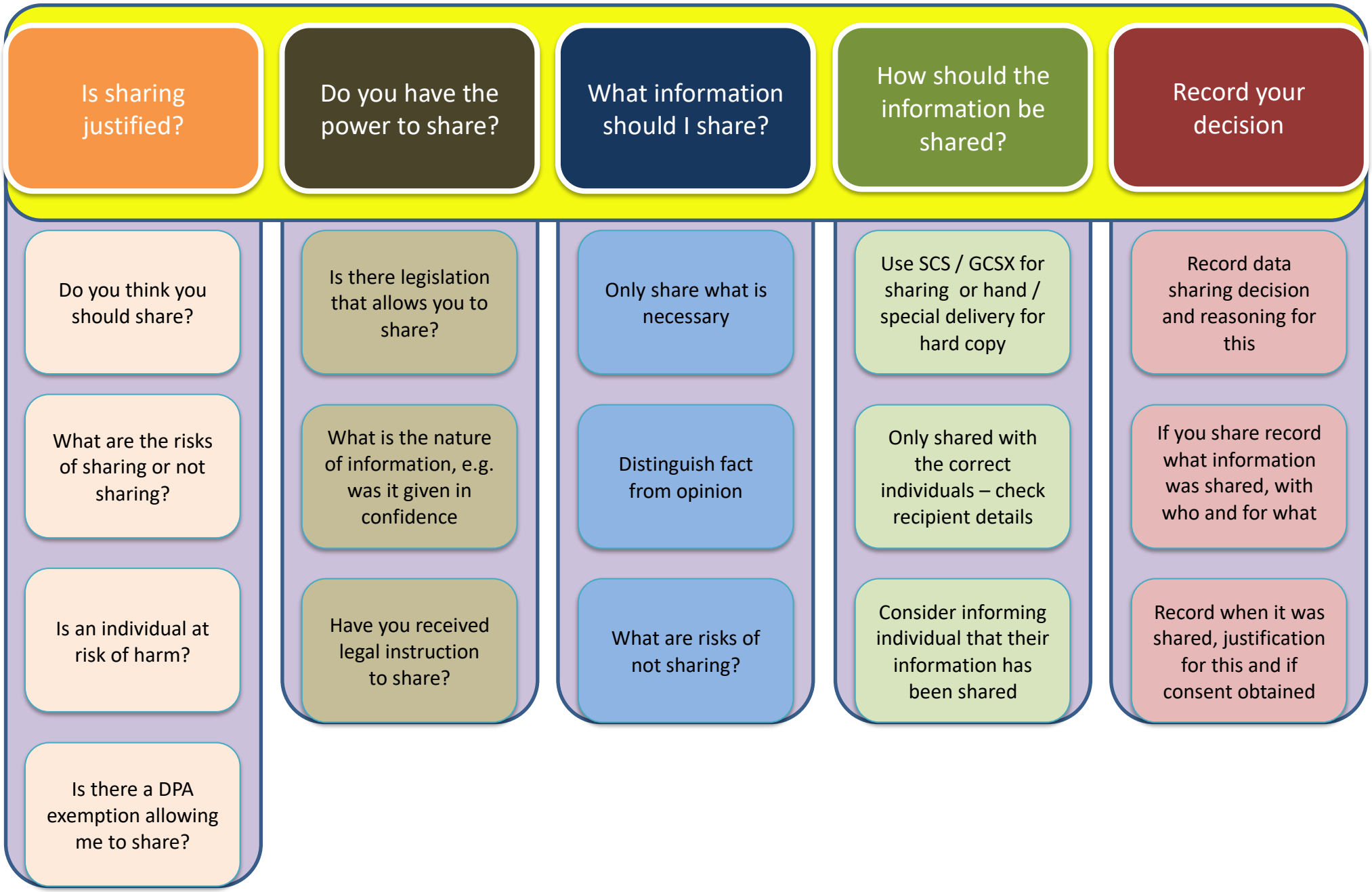
8.2 As per the ISBP procedure, all potential information security incidents should, as a minimum, be reported to the Head Teacher and the DPO.

9. Contacts and Further Information

9.1 Appendix 1 provides 5 steps to effective data sharing. This can be used as a reference when considering sharing information.

Appendix 1

5 Steps to Effective Data Sharing



Document Version Control

Version	Date	Author	Sent To	Comments
3.0	280820	R Montgomery (DPO)	School	Updates from previous version

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 3

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 Trust /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	Trust 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 Trust / school premises.

Declaration

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

I (insert name) _____

_____

certify that the information given on this application form and any attachments therein to BAST / a BAST school is accurate and true.

I understand that it is necessary for the Trust 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:

School requests:

Information Governance
Mr Paul O'Malley
Stokesay Primary School
Craven Arms
Shropshire
SY7 9NW
01588 67227

Trust:

BAST
Information Governance
Mrs S Godden
C/o Oldbury Wells School
Bridgnorth
WV16 5JD
01746 760509
Our email address is foi@telford.gov.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 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]
1.1.2	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 years	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 a 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 relating 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 In this context SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a cross cut shredder.

2 These are the copies which the clerk to the Governor may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

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
1.1.5	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 policy + 3 years	SECURE DISPOSAL
1.1.9	Records relating to complaints dealt with by the Governing Body	Yes		Date of the 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 (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
1.1.11	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

Please note that all information about the retention of records concerning the recruitment of Head Teachers can be found in the Human Resources section below.

1.2 Head Teacher and Senior Management Team					
	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 Head Teacher	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 of 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 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 report refers to individual pupils or members of staff		Date of the report + a minimum of 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 records refer to individual pupils or members of staff		Current academic year + 6 years then review	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 correspondence 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 the plan + 6 years	SECURE DISPOSAL
1.2.7	School Development Plans	No		Life of the 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 School Admissions' 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 appeal 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.[3]	REVIEW Schools may wish to consider keeping the admission register permanently as often schools 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	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Current year + 1 year	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
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc	Yes			
	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process completed	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 file 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 up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.13	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 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 of 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 member of staff's personal file	
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	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	

2.2 Operational Staff Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/ assessment records	Yes		Current year + 5 years	SECURE DISPOSAL

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[5]	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation whichever 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	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	oral warning			Date of warning[6] + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then 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 the 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 at work	Yes		Date of incident + 12 years In the case of serious accidents 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 the incident + 6 years	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; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL
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 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 (SI1999/567)	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

5 This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to

6 Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter please contact your Safeguarding Children Officer for further advice

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 the 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 year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	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 contracts 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 + 2 years	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 + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books	No		Current year + 6 years	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 + 6 years	SECURE DISPOSAL
3.6.2	School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets	No		Current year + 3 years	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		PERMANENT 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 to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	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 + 6 years	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 + 6 years	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			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 pupil 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 for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not 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
	Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes			
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
	Internal			This information should be added to the pupil file	

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
	This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention				
5.1.3	Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.

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 October 2014	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 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 + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records –	Yes			
	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 + 6 years 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 + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self Evaluation Forms	Yes		Current year + 6 years	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 + 1 year	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 + 1 year	
6.2.3	Class Record Books	No		Current year + 1 year	
6.2.4	Mark Books	No		Current year + 1 year	
6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' 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 + 1 year	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 Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	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 Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips 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 issued by the school for this period of time.
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 + 25 years 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	

7.2 Walking Bus					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.2.1	Walking Bus Registers	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]

7.3 Family Liaison Officers and Home School Liaison Assistants					
	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 + 2 years 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 and then destroy	
7.3.3	Referral forms	Yes		While the referral is current	
7.3.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	
7.3.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
7.3.6	Group Registers	Yes		Current year + 2 years	

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 + 2 years	SECURE DISPOSAL
8.1.2	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3	School Census Returns	No		Current year + 5 years	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 + 6 years	SECURE DISPOSAL
8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL

GDPR Policy Part 3

INFORMATION SECURITY FRAMEWORK

BAST Information Security Breach Procedure (ISBP) v3.3

What to do in the event of a possible data breach/incident

1. Introduction

1.1 This procedure supports the Trust's ICT security policies, 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 Trust / school employees, Trust / school community members or third parties[2] contracted to provide Trust / 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 Executive Headteacher on 01746 760509.

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:

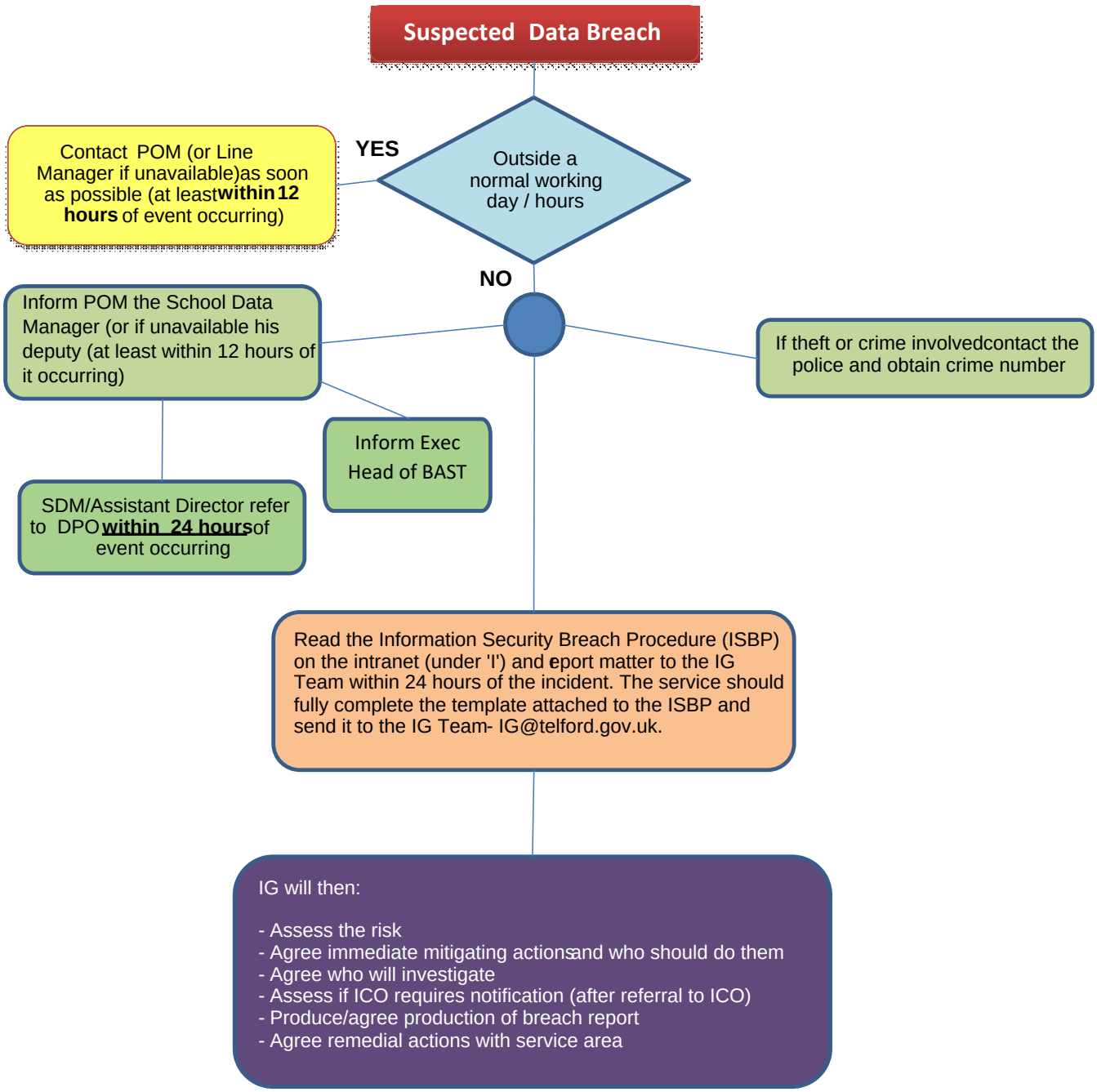
- Viewed or copied by an individual unauthorised to do so,
- Communicated to an unauthorised individual/organisation, e.g. sent to wrong address and opened/read
- Lost or stolen

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

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 IG and the service area 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.

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



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 Stokesay Primary School this is Paul O'Malley. Your SDM will inform the Executive Headteacher in his turn. The Executive Headteacher will liaise with the Audit Committee of the Trust Board 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 relevant Team Leader/Group Manager, SDM or Assistant Director) immediately (or as a minimum within 12 hours of incident occurring). The matter must then be forwarded to IG 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 83333 or via your desktop link.

3.2.4 When the matter is reported to IG 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
- Council officer 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, Assistant Director, Director, Member, etc

3.2.5 When the incident is reported to IG 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 on the intranet.

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.

Appendix 1

Suggested Report Template

(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 Council or destroyed?	Do you intend to notify the data subject(s) affected? If YES please consult IG 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