



## **UK General Data Protection Regulation Policy**

### **(GDPR, Part A)**

### **Information Security Breach Procedure (Part B)**

<b>FREQUENCY OF REVIEW:</b>	<b>Annually</b>
<b>COMMITTEE:</b>	<b>Audit &amp; Risk Committee</b>
<b>RATIFICATION DATE:</b>	<b>2 December 2025</b>
<b>DATE OF NEXT REVIEW:</b>	<b>Autumn 2026 unless there is a material change</b>

## PART A:

## 1. Introduction



*The UK Data Protection Act 2018 (DPA 18)/UK General Data Protection Regulations (GDPR) and Data Use and Access Act 2025 (DUAA) defines UK law on the processing of data on identifiable living people. It governs the protection of personal data in the UK. Personal information is information about a living individual, who can be identified from the information and/or additional information available.*

- 1.1 TrustEd Schools Alliance, and TrustEd Schools, are committed to protecting the privacy of individuals and handle all personal information in a manner that complies with the DPA18. It is the **personal responsibility** of all employees (temporary or permanent), Trustees, Governors, 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, UK DPA/UK GDPR 2018 and DUAA 2025. All breaches will be investigated and appropriate action taken.
- 1.3 This policy explains what the Trust and schools' expectations are when processing personal information and Part A (GDPR) should be read in conjunction with the Security Breach Procedure (Part B) of this policy and the School Information Security Policy (SISP).
- 1.4 Where the term UK DPA is used in this policy it also encompasses the requirements of the UK GDPR and the DUAA 2025.

## 2. GDPR Principles

- 2.1 The UK DPA 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 UK DPA principles relevant to the school 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

- 2.3 There is a further principle called the Accountability Principle. This requires the school to be able to clearly demonstrate their compliance with the UK DPA. The schools Data Protection Officer undertakes an annual exercise to ensure that the school complies with this principle. See section 12 for further information.

### 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), Trustees, Governors, contractors, agents and anyone else processing information on the schools 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**, via a Privacy Notice.

### 5. Lawful Basis for Processing

- 5.1 When any TrustEd School or the Trust itself, processes personal information, it must have a lawful basis for doing so. The UK DPA provides a list of 'basis' when the school or Trust can process personal and/or 'special category' personal information. This is contained within Article 6 and Article 9 of the regulations (**see Appendix 1**).
- 5.2 The UK DPA 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 UK GDPR and when it processes 'special category' personal information; it must also be able to satisfy at least one of the conditions in Article 9 of the UK GDPR as well.

Note: \*Throughout this policy, 'School' refers to both TrustEd Schools and also TrustEd services.

- 5.4 The school can process personal information if it has the data subject's legal consent (this needs to be 'explicit' when it processes special category 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. Guidance on how consent should be managed can be found from the school office.

## **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 detail 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. Data minimisation should always be employed.
- 6.5 When personal information is given either externally or internally, it must be communicated in a secure manner, e.g. password protected/encrypted emails, special delivery or courier, etc.

## **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 TrustEd Schools' holds personal information. The UK DPA 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 business reason for holding it.
- 8.2 The schools' Information Retention Schedule 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 the schools Data Protection Officer.

## 9. Individuals Rights

- 9.1 Individuals have a number of rights under the UK DPA. 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 research and statistics
  - **Rights related to automated decision making/profiling** – A person can ask for human intervention in an automated process
- 9.2 If the school receives such a request on any of the above matters they should seek advice from their Data Protection Officer as soon as the request is received.
- 9.3 The school has one calendar month in which to respond to a SAR, provided the applicant has clearly stated the nature of their request preferably by completing a subject access request form and suitable proof of identification has been supplied. However the law does allow a SAR to be made verbally. An extension of a further 1-2 months will be applied where a request is deemed complex, the requester should be informed of this within one month of the request being received. The school and Data Protection Officer co-ordinates the processing of all SAR requests. **See Appendix 2** for a copy of the SAR form

## 10. Right to Complain

- 10.1 The DUAA 25 requires the school to have a complaints process in place where a data subject can make a complaint to the school about its processing of their personal data.

- 10.2 A data subject can make a complaint by completing the template on Appendix 3. The school will acknowledge receipt of the complaint within 30 days and process the complaint without undue delay.
- 10.3 The school will keep the data subject informed of progress made in respect to investigating their complaint.
- 10.4 If following this complaints process the data subject remains dissatisfied, they have the right to refer the matter to the Information Commission. Please note the Information Commission require the data subject to go through the school's data protection complaint process prior to contacting them with any referral.

## **11. Reporting Security Incidents**

- 11.1 The school has a responsibility to monitor all incidents that occur which may breach the security and/or the confidentiality of its information. All incidents need to be identified, reported on a timely basis, investigated and monitored. It is only by adopting this approach that the school can learn from its mistakes and prevent losses recurring. The Data Protection Officer must be informed of an incident/breach within 24 hours of the school becoming aware of the matter.
- 11.2 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:
- Information Security Breach Procedure
  - Data Breach Investigation
- 11.3 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 schools information.

## **12. Data Protection Officer**

- 12.1 As the school is a public authority, it has a legal duty to appoint a designated Data Protection Officer.
- 12.2 The Data Protection Officer has a number of legal duties that they must fulfil including:
- Inform and advise the school of its obligations in respect to data protection
  - Monitor compliance with data protection legislation including awareness raising and training of staff
  - Provide advice on data protection impact assessments
  - Be a contact for the Information Commissioners Office
- 11.3 The schools current designated Data Protection Officer is Rob Montgomery/Sarah Daffern – IG@telford.gov.uk.

## **13. Accountability**

13.1 The DPA 18 requires the school to have appropriate measures and records in place to demonstrate compliance with the act.

13.2 The school demonstrates accountability in a number of ways including:

- Having appropriate policies in place
- Following data protection by design and default
- Using data processing agreements in contracts
- Maintaining records of processing activities
- Implementing technical and organisational security
- Managing data breaches
- Completing data protection impact assessments
- Having an appropriately skilled and knowledgeable Data Protection Officer

## 14. Risk Management

14.1 It is the **personal responsibility** of all employees (temporary or permanent), Trustees, Governors, contractors, agents and anyone else handling personal information to do so in a safe and secure manner. This includes Governors on the LGB and Trustees on the Trust Board if at times they have access to personal data when engaged in their role.

## 15. Staff Training

15.1 It is recommended that a data protection course be completed each year by all Trust staff, Governors and Trustees. Training is available on The Key (GDPR for school staff)  
All New staff should complete a suitable training as part of their staff induction.

**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.

# UK Data Protection Act/UK General Data Protection Regulations 2018/Data Use and Access Act 2025

## Right of Access to Personal Data

### SUBJECT ACCESS REQUEST FORM (SAR)

#### Information

We should respond to your request within one calendar month. Note this can be extended for a further 2 months if the request is deemed complex. 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
- c) You have provided clarification to any queries from the school in respect to your request

Please note, by law, the school only has to undertake a reasonable and proportionate search for the information you have requested. If the school believes your request is unreasonable and disproportionate it will inform you of this detailing the reasons for coming to this decision.

**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(s) 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 specific 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 Staff Member Holding this Information	Time Period for Information Requested

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 you make alternative arrangements with the school. 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 **[insert]** School is accurate and true.

I understand that it is necessary for the **[insert]** 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 or hand delivering them then our address is detailed below:

**[insert]** School  
**[insert address]**

Our email address is **[insert]**

\_\_\_\_\_

### **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 school
- For us to email you the information securely/password protected

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 secure email by ticking the box below and confirming the email address that your information should be sent to:**

Tick Box	<input type="checkbox"/>	EMAIL ADDRESS	<input type="text"/>
----------	--------------------------	---------------	----------------------

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

Collection in Person	<input type="checkbox"/>	By Post (Special Delivery)	<input type="checkbox"/>
----------------------	--------------------------	----------------------------	--------------------------

## Data Protection Complaint Form

The school has a data protection complaints process that allows individuals to complain to the school about its processing of their personal data.

The school will acknowledge your complaint within 30 days of receipt and will keep you informed of the progress of investigating the complaint. The school will look to respond to your complaint without undue delay.

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

Full Name		Date	
-----------	--	------	--

School Department/Staff Member related to your complaint (if known)	
---	--

Please describe the nature of your complaint in as much detail as possible

What do you want to happen as a result of this complaint.

## 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.

### 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 <sup>1</sup>
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 <sup>2</sup>			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

<sup>1</sup> In the 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.

<sup>2</sup> 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. <sup>3</sup>	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
2.1.3 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 <sup>4</sup>	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 <sup>5</sup>	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 <sup>6</sup> + 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

<sup>5</sup> 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

<sup>6</sup> 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	<p>The file should follow the pupil when he/she leaves the primary school. This will include:</p> <ul style="list-style-type: none"><li>• to another primary school</li><li>• to a secondary school</li><li>• to a pupil referral unit</li></ul> <p>• 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.</p> <p>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.</p> <p>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</p>
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	<p>"Keeping children safe in education Statutory guidance for schools and colleges March 2015";</p> <p>"Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"</p>	<p>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.</p>	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child protection information held in separate files	Yes	<p>"Keeping children safe in education Statutory guidance for schools and colleges March 2015";</p> <p>"Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"</p>	<p>DOB of the child + 25 years then review</p> <p>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</p>	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	SECURE DISPOSAL
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	

## 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 <a href="http://oeapnginfo.specifically">http://oeapnginfo.specifically</a> 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 <a href="http://oeapnginfo.specifically">http://oeapnginfo.specifically</a> 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

## PART B

# TrustEd Schools Information Security Breach Procedure (v4.6)

## 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 school employees, Governors or third parties<sup>1</sup> 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
  - **Special Category (sensitive) Personal Data** – e.g. information specifically relating to race and ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, biometric data identifying individuals, genetic data, health data, sexual preferences, sex life and/or sexual orientation
- 1.3 The principles of securing information (in accordance with Principle 6 of the UK Data Protection Act/UK GDPR 2018), can be found in the Schools Information Security Policy (SISP). For further guidance on information security contact the Data Protection Officer (DPO).

## 2. What is a possible breach of PII?

- 2.1 A breach of PII is any security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Article 4(12) – GDPR).

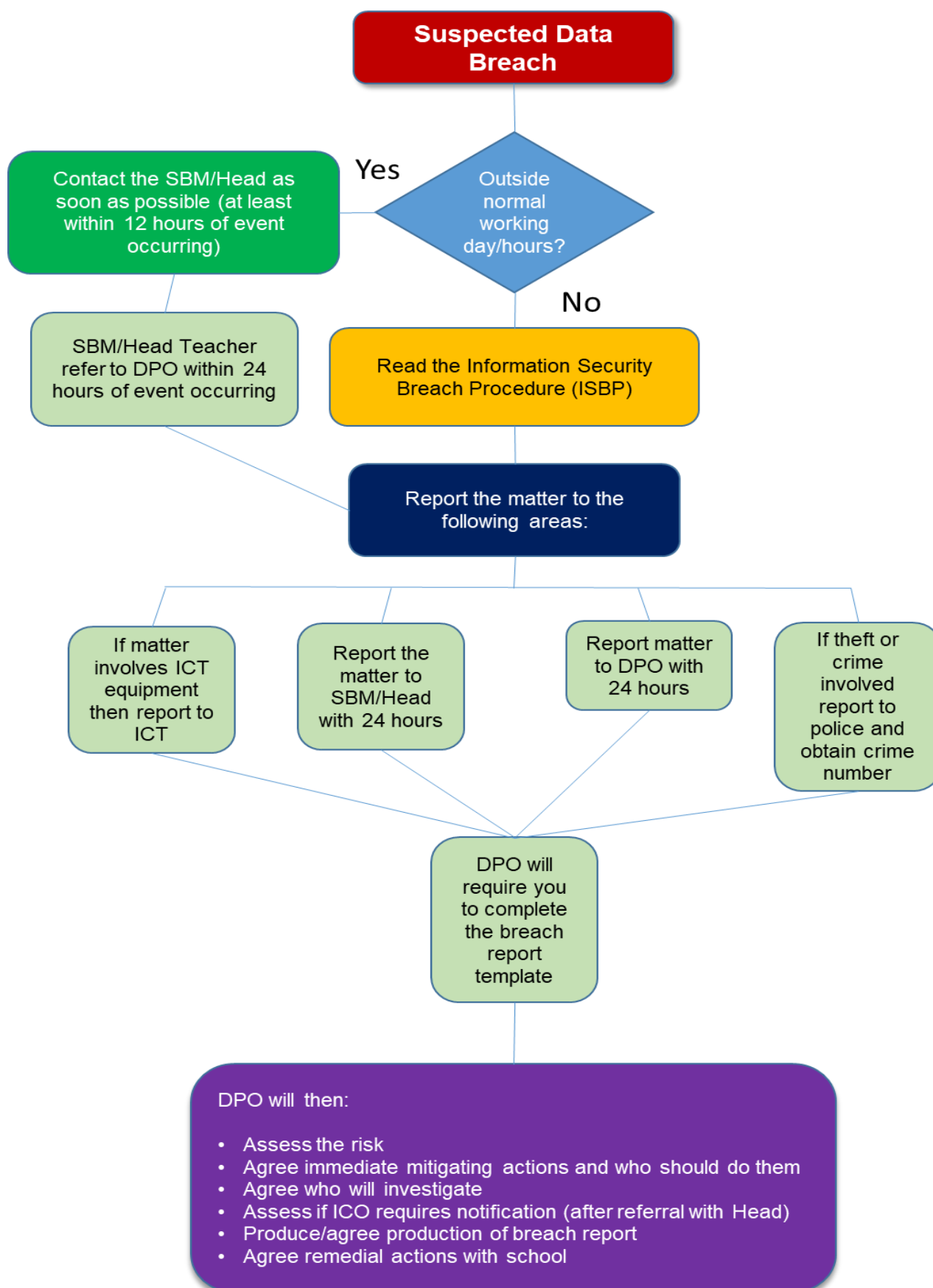
There are many examples of what constitutes a possible data breach, typical examples are detailed below:

- Loss of mobile phone/laptop or other ICT equipment
  - PII being emailed/posted/ to an unintended recipient or address and read by the individual, e.g. a letter containing child protection 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 personnel information
  - Viewing PII that you do not need to access as part of your role
  - Not keeping personal 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 the DPO and the school 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.

---

<sup>1</sup> 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 the SBM/Head Teacher within 24 hours of the incident occurring and then follow 3.2 below.

## **3.2 Normal working day**

- 3.2.1 If you know/suspect a breach has occurred you will need to inform the SBM or Head Teacher immediately (or as a minimum within 24 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 IDT Service Desk on 01952 384444 or your ICT Technician. The school ICT manager should also be informed. For the Trust Central Team this is the Trust Estates Manager.
- 3.2.4 When the matter is reported to the DPO and IDT (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
  - School employee or 3<sup>rd</sup> 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 if applicable
  - Confirmation as to who else in the school has been informed, e.g. SBM, Head Teacher, 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 breach
  - Compare the incident against notification rationale outlined by the Information Commissioners Office (ICO) and notify (after approval by the Head) if applicable
  - Agree the production of a breach report, see **Appendix 1** for required layout
  - Agree remedial action to be taken
  - Communicate any lessons learnt school-wide where appropriate
- 3.2.6 Managers can obtain guidance on possible action to be taken in relation to employees implicated in data breaches by discussing with Human Resources.

## **4. Advice and assistance**

- 4.1 If you require any further information please contact the SBM or DPO (email IG@telford.gov.uk).

## Suggested Report Template

(Input in grey below are example entries only)

Tick relevant box

<b>Breach?</b>	<input checked="" type="checkbox"/>	<b>Incident?</b>	<input type="checkbox"/>
----------------	-------------------------------------	------------------	--------------------------

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

<b>Date Occurred</b>	12/12/23	<b>Officer Causing the Breach</b>	R Montgomery
----------------------	----------	-----------------------------------	--------------

<b>Date and name of SBM informed (and Head where relevant)</b>	<b>Was breach/incident identified as a result of a complaint (Y or N?)</b>	Y
13/12/23 – Anthea Lowe		

<b>Categories of Data Breached</b>	<b>Number of Individuals Affected</b>	<b>Number of Records Breached</b>
Name, Address, Bank details	1	6

<b>Description of breach/incident (including the type of information and date/location of incident)</b>
Bank statements collected for identification purposes returned to 15 Darby Road on 11/12/23 instead of correct address 51 Darby Road

<b>Reported to police Y/N?</b>	N	<b>Date Reported / Police Station</b>	N/A	<b>Crime number</b>	N/A
--------------------------------	---	---------------------------------------	-----	---------------------	-----

<b>Has information been returned to School or destroyed?</b>	<b>Do you intend to notify the data subject(s) affected?</b>
	If YES please consult DPO prior to doing this If NO please give an explanation for this
Information returned to School on 11/12/23	Yes – as they will be able to ask their bank to watch their account

<b>How did breach/incident occur?</b>
Employee had incorrectly updated the contact record for this parent

<b>Measures already taken to address breach</b>
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**

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

<b>Lessons learnt to be implemented (if relevant)</b>
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