Bolton Impact Trust

Data Protection, Information Management and Retention Policy

Reviewed By	**R Leonard/ G Smith**
Last Reviewed	**June 2023**
Approved by/when	**Central Leadership Team**
To be reviewed	**July 2024**
ICO registration number	**ZA226045**

Contents

1 Policy statement

1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a multi academy trust we will collect, store and **process personal data** about our pupils, **workforce**, parents and others. This makes us a **data controller** in relation to that **personal data**.

1.2 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.3 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.4 All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

2 About this policy

2.1 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('**GDPR**'), the Data Protection Act 2018, and other regulations (together '**Data Protection Legislation**').

2.2 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

2.5 It meets the requirements of GDPR and the provisions of the Data Protection Act 2018. It is based on guidance published by the **Information Commissioner's Office** (ICO). It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. As an Academy Trust regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record does not apply.

3 Definition of data protection terms

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in Appendix 1 to this policy.

4 Data Controller

4.1 Bolton Impact Trust processes personal data relating to pupils, parents, staff, governors, visitors and others and is therefore a Data Controller

4.2 Bolton Impact Trust is registered as a **Data Controller** with the **ICO** and will renew this registration annually or as is otherwise legally required

5 Data Protection Officer

5.1 As a Multi Academy Trust we are required to appoint a **Data Protection Officer (DPO).** Our **DPO** is Gill Smith and they can be contacted at gill@mindography.co.uk

5.2 The **DPO** is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the **DPO**.

5.3 The **DPO** is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

6 Roles and responsibilities

This policy applies to all staff employed by Bolton Impact Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

6.1 **Trust Board –** The Trust Board has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

6.2 **Data Protection Officer** - see section 5.

6.3 **Academy Leads** – The Academy Leads act as the representative of the Data Controller on a day-to-day basis. The Academy Leads of each school are responsible for ensuring that their academy is compliant to data protection laws. Academy Leads will delegate duties throughout the school to ensure that correct processes and procedures are undertaken to meet the requirements of compliance.

6.4 **All Staff** - Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Academy or Central Team (as appropriate) of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed

- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach/suspected data breach/near miss
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties
- If they would like training or awareness sessions arranged for themselves or colleagues

Bolton Impact Trust ensure that all staff (including contract, temporary, third party and supply staff) are given the correct information from the offset on our expectations of staff in terms of data protection. All staff across the Trust work in a "data safe" culture. We implement this mind-set to help make staff aware that any action that they do that comes into contact with personal data is done in such a way to protect a data subject's personal data.

7 Data protection principles

7.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

7.1.1 **processed** fairly and lawfully and transparently in relation to the **data subject**

7.1.2 **processed** for specified, lawful purposes and in a way which is not incompatible with those purposes

7.1.3 adequate, relevant and not excessive for the purpose

7.1.4 accurate and up to date

7.1.5 not kept for any longer than is necessary for the purpose

7.1.6 **processed** securely using appropriate technical and organisational measures.

7.2 **Personal data** must also:

7.2.1 be **processed** in line with **data subjects'** rights

7.2.2 not be transferred to people or organisations situated in other countries without adequate protection.

7.3 We will comply with these principles in relation to any **processing** of **personal data** by the Trust.

8 Fair and lawful processing

8.1 Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

8.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

8.2.1 that the **personal data** is being **processed**

8.2.2 why the **personal data** is being **processed**

8.2.3 what the lawful basis is for that **processing** (see below)

8.2.4 whether the **personal data** will be shared, and if so with whom

8.2.5 the period for which the **personal data** will be held

8.2.6 the existence of the **data subject's** rights in relation to the **processing** of that **personal data**

8.2.7 the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

8.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

8.4 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:

8.4.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract

8.4.2 where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011)

8.4.3 where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest

8.4.4 where the **processing** is for a legitimate reason other than when we are carrying out a task in the public interest

8.4.5 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data.** If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent whether the pupil is over 13 years of age (except for online counselling and preventive services)

8.5 When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:

8.5.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence

8.5.2 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment

8.5.3 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities

8.5.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.

8.6 We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

8.7 If any **data user** is in doubt as to whether they can use any **personal data** for any purpose then they must contact the DPO before doing so.

Vital Interests

8.8 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

8.9 Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

8.10 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

8.11 When pupils and or our **workforce** join Bolton Impact Trust a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, among other things. Where appropriate third parties may also be required to complete a consent form.

8.12 In relation to all pupils under the age of 13 years old we will seek consent from an individual with parental responsibility for that pupil.

8.13 We will generally seek consent directly from a pupil who has reached the age of 13, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

8.14 If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:

8.14.1 inform the **data subject** of exactly what we intend to do with their **personal data**

8.14.2 require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in

8.14.3 inform the **data subject** of how they can withdraw their consent.

8.15 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.

8.16 The DPO must always be consulted in relation to any consent form before consent is obtained.

8.17 A record must always be kept of any consent, including how it was obtained and when.

9 Processing for limited purposes

9.1 In the course of our activities as a Multi Academy Trust we may collect and **process** the **personal data** set out in our Schedule of Processing Activities/Record of Data Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).

9.2 We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities/Record of Data Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

10 Notifying data subjects

10.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

10.1.1 our identity and contact details as **Data Controller** and those of the DPO

10.1.2 the purpose or purposes and legal basis for which we intend to **process** that **personal data**

10.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**

10.1.4 whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place

10.1.5 the period for which their **personal data** will be stored, by reference to our Retention Schedule - Appendix B

10.1.6 the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making

10.1.7 the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

10.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

10.3 The Trust may be provided with information relating to third parties in the form of emergency contact details. Parents are required to obtain the consent of any third party whose details they provide to the Academy Trust for these purposes. Privacy notices detailing how the information will be stored and used can be accessed through the Bolton Impact Trust website.

11 Adequate, relevant and non-excessive processing

11.1 We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

12 Accurate data

12.1 We will ensure that **personal data** we hold is accurate and kept up to date.

12.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

12.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

13 **Timely processing**

13.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

14 **Processing in line with data subject's rights**

14.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

14.1.1 request access to any **personal data** we hold about them

14.1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing

14.1.3 have inaccurate or incomplete **personal data** about them rectified

14.1.4 restrict **processing** of their **personal data**

14.1.5 have **personal data** we hold about them erased

14.1.6 have their **personal data** transferred

14.1.7 object to the making of decisions about them by automated means.

The Right of Access to Personal Data

14.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the trust's **Subject Access Request** Procedure. This procedure is available on our trust website at "Making a Subject Access Request".

14.3 As an Academy Trust regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record does not apply. Requests from parents to access their child's educational records will be dealt with as a Subject Access Request (SAR).

The Right to Object

14.4 In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

14.5 An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

14.6 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

14.7 In respect of direct marketing any objection to **processing** must be complied with.

14.8 The Trust is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

The Right to Rectification

14.9 If a **data subject** informs the Trust that **personal data** held about them by the Multi Academy Trust is inaccurate or incomplete then we will consider that request and provide a response within one month.

14.10 If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the **data subject** within one month of their request that this is the case.

14.11 We may determine that any changes proposed by the **data subject** should not be made. If this is the case then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

14.12 **Data subjects** have a right to 'block' or suppress the **processing** of **personal data**. This means that the Academy Trust can continue to hold the **personal data** but not do anything else with it.

14.13 The Trust must restrict the **processing** of **personal data**:

14.13.1 where it is in the process of considering a request for **personal data** to be rectified (see above)

14.13.2 where the Trust is in the process of considering an objection to processing by a **data subject**

14.13.3 where the **processing** is unlawful but the **data subject** has asked the Trust not to delete the **personal data**

14.13.4 where the Trust no longer needs the **personal data** but the **data subject** has asked the Trust not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Multi Academy Trust.

14.14 If the Trust has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

14.15 The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

14.16 **Data subjects** have a right to have **personal data** about them held by the Trust erased only in the following circumstances.

14.16.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected.

14.16.2 When a **data subject** withdraws consent – which will apply only where the Trust is relying on the individuals consent to the **processing** in the first place.

14.16.3 When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object.

14.16.4 Where the **processing** of the **personal data** is otherwise unlawful.

14.16.5 When it is necessary to erase the **personal data** to comply with a legal obligation.

The Trust is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

14.16.6 to exercise the right of freedom of expression or information

14.16.7 to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law

14.16.8 for public health purposes in the public interest

14.16.9 for archiving purposes in the public interest, research or statistical purposes

14.16.10 in relation to a legal claim.

14.17 If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

14.18 The DPO must be consulted in relation to requests under this right.

Right to Data Portability

14.19 In limited circumstances a **data subject** has a right to receive their **personal data** in a machine readable format, and to have this transferred to another organisation.

14.20 If such a request is made then the DPO must be consulted.

15 Data security

15.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.

15.2 We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.

15.3 Security procedures include:

15.3.1 **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the academy reception.

15.3.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

15.3.3 **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.

15.3.4 **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

15.3.5 **Working away from the school premises – paper document**. Guidance procedures are available for staff in all schools within Bolton Impact Trust

15.3.6 **Working away from the school premises – electronic working.** Guidance procedures are available for staff in all schools within Bolton Impact Trust.

15.3.7 **Document printing.** Documents containing **personal data** must be sent to printers using secure printing and collected with a personal code.

15.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

16 Personal Data Breaches

16.1 Bolton Impact Trust will make all reasonable endeavours to ensure that there are no data breaches and aim to ensure that all personal data that we hold is protected to the highest possible standard.

16.2 We are aware that data breaches may occur in any of our academies or in the trust and implement a thorough data breach action plan to manage if/when a data breach occurs. Procedures are set out in Appendix 2.

16.3 When appropriate we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on a school website which shows the exam results of pupils eligible for pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a academy/trust laptop containing non-encrypted personal data about pupils

17 Data Protection Impact Assessments

17.1 Bolton Impact Trust takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

17.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

17.3 Bolton Impact Trust will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

17.4 The DPO should always be consulted as to whether a **data protection impact assessment** is required, and if so how to undertake that assessment.

18 Disclosure and sharing of personal information

18.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, [and / or Education and Skills Funding Agency ESFA], Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

18.2 Bolton Impact Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

18.3 In some circumstances we will not share safeguarding information. Please refer to our Child Protection and Safeguarding Policy.

18.4 Further detail is provided in our Schedule of Processing Activities/Record of Data Processing Activities.

19 Data processors

19.1 We contract with various organisations who provide services to the Trust; these are detailed within the Schedule of Processing Activities/Record of Data Processing Activities and privacy notices.

19.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

19.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. Bolton Impact Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

19.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

20 Biometric recognition systems

Under the context of the Protection of Freedoms Act 2020 a "child" means a person under the age of 18.

20.1 Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use their finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

20.2 Parents/carers will be notified before any biometric recognition system is put in place. Bolton Impact Trust will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. The trust will use an 'opt in' system for collecting consent. Parents/carers and pupils have the right to chose not to use the School's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. Parents/carers can withdraw consent at any time and any relevant data already captured will be correctly erased and no longer processed.

20.3 Where staff members or other adults use the School's biometric system(s) we will also obtain their consent before it is first used. Alternative means of accessing the relevant service will be offered if consent is not given. Staff and other adults can also withdraw consent at any time and the School will delete any relevant data already captured.

21 Images and videos

21.1 Parents and others attending Bolton Impact Trust events can take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. Bolton Impact Trust does not prohibit this as a matter of policy.

21.2 Bolton Impact Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.

21.3 Bolton Impact Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

21.4 As a Multi Academy Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

21.5 For our primary schools we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials.

21.6 For our secondary pupils in Year 7, Year 8 and Year 9 we will obtain written consent from parents/carers, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

21.7 For our secondary pupils in Year 10 and Year 11 we will obtain written consent from the students for photographs and videos to be taken for communication, marketing and promotional materials.

21.8 If consent is withdrawn we will delete the photograph/video and not distribute it further. We will also keep on record that consent has been withdrawn for that child so that no further photographs will be used.

21.9 When using photographs and videos in this way we will not accompany them with any other personal information about the child to ensure they cannot be identified

21.10

22 CCTV

22.1 Schools within Bolton Impact Trust may operate a CCTV system. Information held by the school is covered under GDPR; capture of CCTV must be in line with relevant codes of practice including the

Surveillance Camera Code of Practice issued by the Surveillance Camera Commissioner, available here: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

and the CCTV Code of Practice issued by the Information Commissioner's Office, available here: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

22.2 The school will only use surveillance cameras for the safety and security of the school, its staff, pupils and visitors.

22.3 Surveillance will be used as a deterrent for violent behaviour and damage to the school. The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility.

22.4 If the surveillance and CCTV systems fulfil their purpose and are no longer required the school will deactivate them.

22.5 Academy CCTV policies are available on the relevant academy section of the website

23 Changes to this policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

Appendix 1

DEFINITIONS

Term	Definition
Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Controllers	The people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Processing Impact Assessment (DPIA)	A DPIA is a process that is carried out in order to asses if data processing is taking place in line with relevant legislation.
Data Processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Data Protection Officer (DPO)	A Data Protection Office (DPO) should be appointed when any large scale processing or data occurs and/or processing of data may be deemed a risk.
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Data Users	Those of our workforce (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Personal Data	Any information relating to an identified or identifiable living natural person (a data subject); an identifiable living natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Information Commissioner's Office (ICO)	The Information Commissioner's Office is the legal authority who managed GDPR and Data Protection.
Processing	Any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making

	available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Special Category Personal Data	Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Subject Access Request (SAR)	This is when a data subject formally lodges a request to view/access the personal that that is held on them.
Workforce	Includes any individual employed by Academy Trust such as staff and those who volunteer in any capacity including governors, trustees & members.

Appendix 2

PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must contain the breach and immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Academy Lead, Director of Academy Operations and the Chair of Governors/Trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

- Records of all breaches will be on the trust's computer system. The DPO, Academy Lead and Director of Academy Operations will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach. Such data breaches could include:

- Details of pupil premium interventions for named children being published on the school website

- Non-anonymised pupil exam results or staff pay information being shared with governors

- A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- The school's cashless payment provider being hacked and parents' financial details stolen

For example, if **Sensitive information was disclosed via email (including safeguarding records)** the type of actions that could be put in place would be:

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Name of Academy

Information Security Incident Report Form

All boxes must be completed

To be completed by the person reporting the breach

Name	
Job Title	
Name of Academy	
Telephone number	
E-mail address	
Date	
What has happened? Please provide as much information as you can about what has happened, what went wrong and how; include a description of the data, eg: format, volume, from which system, and the location of the breach.	
How did you find out about the breach? If you were not the person who originally found there had been a breach, please explain how you found out about it and how they found out about it.	
Was the breach caused by a cyber incident?	

Yes		**No**		**Not yet known**	

When was the breach discovered?	**Date:**		**Time:**	
When did the breach occur?	**Date:**		**Time:**	

What has happened to the information? (Please select all that apply)					
Destroyed		**Lost**		**Stolen**	
Altered		**Unauthorised Disclosure**		**Unauthorised Access**	
Other (please give details below)					

Categories of personal data included in the breach (Please select all that apply)			
Basic personal identifiers (eg: name, contact details)		**Identification data (eg: usernames, passwords)**	
Racial or ethnic origin		**Political opinions**	
Religious or philosophical beliefs		**Trade union membership**	
Health		**Sexual life or orientation**	
Gender reassignment data		**Genetic or biometric data**	
Financial information		**Criminal convictions or offences**	
Official documents (eg: driving licences)		**Location data**	
Other (please give details below)		**Not yet known**	

How may data subjects could be affected?	

Categories of data subjects affected (Please select all that apply)			
Employees		**Pupils**	
Parents / Carers		**Governors**	

Volunteers		**Other (please give details below)**	

What is the possible impact of the breach on the data subjects?					
Has there been any actual harm to data subjects? (If yes, please give details below)					
Yes		**No**		**Not yet known**	
What is the likelihood that data subjects will experience significant consequences as a result of the breach? (Please select one option and give further details below)					
Very likely		**Likely**		**Neutral**	
Unlikely		**Very unlikely**		**Not yet known**	

Have you told the data subjects about the breach?			
Yes		**About to or in process of telling them**	
No, but they're already aware		**No, but planning to tell them**	
No, decided not to tell them		**Not yet decided whether to tell them**	
Seeking advice from DPO		**Other (Please give details below)**	

Have you told, or are you planning to tell, any other organisations (e.g. police, regulatory body) about the breach? (If yes, please give details below. If you have a crime reference number, please include it)			
Yes		**No**	
Seeking advice from DPO		**Other (Please give details below)**	

What measures have been taken to deal with the breach? (e.g. contacting the person sent in formation in error, auto-erased lost laptop)

Has the data been recovered? (Please give details - if the breach is due to a misdirected email, include whether you have had confirmation that the recipient has deleted it and whether it was read or unread)					
Yes		**No**		**Partially**	

What measures have been taken / are proposed to mitigate further breaches?

If there is any further information you think should be considered please include it here.

To be completed by the Data Protection Officer

Form received by DPO	**Date:**		**Time:**			
Has the DPO been in contact with the school's GDPR lead?			**Yes**		**No**	
Was the form received within 24 hours of the breach being discovered?			**Yes**		**No**	
If no, was a reason given? (Please give details below)			**Yes**		**No**	
Is the information on the form complete?			**Yes**		**No**	
If not, what further information is required? (Please give details below)						

Breach reported to Academy Lead	**Yes**		**No**		**Date**	
Breach reported to GDPR Lead for Trust (Director of Academy Operations)	**Yes**		**No**		**Date**	
Breach reported to Chair of Governors/ Trustees	**Yes**		**No**		**Date**	

What measures have been agreed should be taken to deal with the breach?

What measures have been agreed should be taken to mitigate harm caused by the breach?

Have data subjects been told about the about the breach (if not already done by person reporting it)?			
Yes		About to or in process of telling them	
No, but they're already aware		No, but planning to tell them	
No, decided not to tell them		Other (Please give details below)	

Does the breach warrant a report to the ICO?	Yes		No	
If yes, when was the breach reported to the ICO?	Date:		Time:	
Was report to ICO made within 72 hours?	Yes		No	

If report was not made within 72 hours, please provide justification for late reporting below.

What has been identified as the root cause(s) of the breach following investigation?

What corrective actions have been identified following investigation?			
Action	**Target Date**	**Owner**	**Date Completed**

DPO Sign-off		**Date**	
Academy Lead Sign-off		**Date**	
Director of Academy Operations Sign-off		**Date**	
Date Incident Investigation Closed			

Appendix 3

Retention schedules and impact levels

Bolton Impact Trust maintains a records management policy which details compliance with the Lord Chancellor's Code of Practice which can be found here:

http://webarchive.nationalarchives.gov.uk/20150603223501/https://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section-46-code-of-practice.pdf

This retention schedule is based on guidance from the records management society:
https://cdn.ymaws.com/irms.org.uk/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

It encompasses records managed by all types of school – some of the file descriptions listed may not be relevant to every school.

Please also note that for a number of years an Independent Inquiry into Child Sexual Abuse (formally the Goddard Inquiry) has been running. For the life of this Inquiry we must not destroy records that are:

- **connected with child protection**
- **connected with child sexual abuse**
- **related to individuals working with children**

In terms of how this fits with GDPR requirements, the suspension of the disposal of these records is covered by the Inquiries Act 2005 which makes it a criminal offence for anyone to knowingly destroy, alter or conceal records and information which is or may be relevant to the Inquiry. In effect this supersedes GDPR.

1 Child Protection

These retention periods should be used in conjunction with the document “Safeguarding Children and Safer Recruitment in Education which can be downloaded from this link:

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

	Basic file description	Data Prot Issues	Statutory Provisions	Retention period [operational]	Action at the end of the administrative life of the record		Protective Marking Classification
1.1	Child Protection files	Yes	Education Act 2002, s175, related guidance “Safeguarding Children in Education”, September 2004	DOB + 25 years[1]	SECURE DISPOSAL	Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university for example)	**IL4-Confidential**

1.2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance)	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL	The following is an extract from "Safeguarding Children and Safer Recruitment in Education" p60	**IL4-Confidential**
			Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005			"Record Keeping	..

						5.10 It is important that a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on a person's confidential personnel file, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference if the person has moved on. It will provide clarification in cases where a future DBS Disclosure reveals information from the police about an allegation that did not result in a criminal conviction. And it will help to prevent unnecessary reinvestigation if, as sometimes happens, an allegation re-surfaces after a period of time. The record should be retained at least until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer."	..

[1] This amendment has been made in consultation with the Safeguarding Children Group.

	Basic file description	Data Prot Issues	Statutory Provisions	Retention period [operational]	Action at the end of the administrative life of the record		Protective Marking Classification
2 Governors							
2.1	Minutes						
	Principal set (signed)	No		Permanent	Retain in school for 6 years from date of meeting	Transfer to Archives	**IL3 - RESTRICTED**
	Inspection copies	No		Date of meeting + 3 years	SECURE DISPOSAL [If these minutes contain any sensitive personal information they should be SECURELY DISPOSED		**IL3 - RESTRICTED**
2.2	Agendas	No		Date of meeting	SECURE DISPOSAL		**IL1–Unclassified**
2.3	Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**

2.4	Annual Parents' meeting papers	No		Date of meeting + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
2.5	Instruments of Government	No		Permanent	Retain in school whilst school is open	Transfer to Archives when the school has closed	**IL1–Unclassified**
2.6	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required	Transfer to Archives	**IL1–Unclassified**
2.7	Action Plans	No		Date of action plan + 3 years	SECURE DISPOSAL	It may be appropriate to offer to the Archives for a sample to be taken if the school has been through a difficult period	**IL1–Unclassified**
2.8	Statutory Policy documents (does not include school specific policies such as writing policies etc.)	No		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
2.9	Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years		**IL3 - RESTRICTED**

					Review for further retention in the case of contentious disputes SECURE DISPOSAL		
2.10	Proposals for schools to become, or be established as Specialist Status schools	No			Current year + 3 years	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL2–PROTECT**
3 Management							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
3.1	Log Books	Yes[1]		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives	**IL3 - RESTRICTED**
3.2	Minutes of the	Yes[1]		Date of meeting + 5	Retain in the	Transfer to Archives	**IL3 - RESTRICTED**

	Senior Management Team and other internal administrative bodies			years	school for 5 years from meeting	[The appropriate archivist will then take a sample for permanent preservation]	
3.3	Reports made by the head teacher or the management team	Yes[1]		Date of report + 3 years	Retain in the school for 3 years from meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL3 - RESTRICTED**
3.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes[1]		Closure of file + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
3.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	No		Date of correspondence + 3 years	SECURE DISPOSAL		**IL2–PROTECT**

3.6	Professional development plans (Management plans for professional development plans of staff)	Yes		Closure + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
3.7	School development plans	No		Closure + 6 years	Review	Offer to the Archives	**IL2–PROTECT**
3.8	Admissions – if the admission is successful	Yes		Admission + 1 year	SECURE DISPOSAL		**IL3 - RESTRICTED**
3.9	Admissions – if the appeal is unsuccessful	Yes		Resolution of case + 1 year	SECURE DISPOSAL		**IL3 - RESTRICTED**
3.10	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL		**IL3 - RESTRICTED**
3.11	Proofs of address supplied by parents as part of the admissions process	Yes		Current year + 1 year	SECURE DISPOSAL		**IL3 - RESTRICTED**
[1] From January 1st 2005 subject access is permitted into unstructured filing systems and log books and other records created within the school containing details about the activities of individual pupils and members of staff will become subject to the Data Protection Act 1998.							
4 Management							

	Basic file description	Data Prot Issues	Statutory Provisions	Retention period [operational]	Action at the end of the administrative life of the record		Protective Marking Classification
4.1	Admission Registers	Yes		Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives	**IL3 - RESTRICTED**
4.2	Attendance registers	Yes	The Education (Pupil Registration) (England) Regulations 2006 (No. 1751)	Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]		**IL3 - RESTRICTED**
4.3	Pupil record cards						

4.3a	*Primary*	Yes		Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service		**IL3 - RESTRICTED**
4.3b	*Secondary*	Yes	Limitation Act 1980	DOB of the pupil + 25 years[1]	SECURE DISPOSAL		**IL3 - RESTRICTED**
4.4	Pupil files						

4.4a	*Primary*	Yes		Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service		**IL3 - RESTRICTED**
4.4b	*Secondary*	Yes	Limitation Act 1980	DOB of the pupil + 25 years[2]	SECURE DISPOSAL		**IL3 - RESTRICTED**

4.5	Special Educational Needs files, reviews and Individual Education Plans	Yes		DOB of the pupil + 25 years the review NOTE: This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.	SECURE DISPOSAL		**IL4-Confidential**
4.6	Correspondence Relating to Authorised Absence and Issues	No		Date of absence + 2 years	SECURE DISPOSAL		**IL2–PROTECT**
4.7	Absence books	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**

4.8	Examination results	Yes					
4.8a	*Public*	No		Year of examinations + 6 years	SECURE DISPOSAL	Any certificates left unclaimed should be returned to the appropriate Examination Board	**IL2–PROTECT**
4.8b	*Internal examination results*	Yes		Current year + 5 years[3]	SECURE DISPOSAL		**IL2–PROTECT**
4.9	Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL		**IL3 - RESTRICTED**
4.10	Statement maintained under The Education Act 1996 - Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending		**IL4-Confidential**
4.11	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending		**IL4-Confidential**

4.12	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SECURE DISPOSAL unless legal action is pending		**IL4-Confidential**
4.13	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SECURE DISPOSAL unless legal action is pending		**IL3 - RESTRICTED**
4.14	Children's SEN Files	Yes		DOB of pupil + 25 years then review – it may be appropriate to add an additional retention period in certain cases	SECURE DISPOSAL unless legal action is pending		**IL4-Confidential**
4.15	Parental permission slips for school trips – where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL		**IL3 - RESTRICTED**

4.16	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE DISPOSAL		**IL3 - RESTRICTED**
4.17	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Primary Schools	N	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 14 years[4]	N	SECURE DISPOSAL or delete securely	**IL2–PROTECT**
4.18	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Secondary Schools	N	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 10 years[7]	N	SECURE DISPOSAL or delete securely	**IL2–PROTECT**

4.19	Walking Bus registers	Yes		Date of register + 3 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
					[If these records are retained electronically any back up copies should be destroyed at the same time]		
				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			

[1] In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service

[2] As above

[3] If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary.

[4] This retention period has been set in agreement with the Safeguarding Children's Officer

5 Curriculum							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
5.1	Curriculum development	No		Current year + 6 years	SECURE DISPOSAL		**IL1–Unclassified**
5.2	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL		**IL1–Unclassified**
5.3	School syllabus	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL1–Unclassified**
5.4	Schemes of work	No		Current year + 1 year This retention period starts once the document has been superseded	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL1–Unclassified**

5.5	Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL1–Unclassified**
5.6	Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL2–PROTECT**
5.7	Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL2–PROTECT**

5.8	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL2–PROTECT**
5.9	Pupils' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL		**IL2–PROTECT**
5.1	Examination results	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
5.11	SATS records	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
5.12	PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
5.13	Value added records	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
5.14	Self Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**

6 Personnel Records held in Schools							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
6.1	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
6.2	Staff Personal files	Yes		Termination + 7 years	SECURE DISPOSAL		**IL2–PROTECT**
6.3	Interview notes and recruitment records	Yes		Date of interview + 6 months	SECURE DISPOSAL		**IL2–PROTECT**
6.4	Pre-employment vetting information (including DBS Checks)	No	DBS Guidelines	Date of check + 6 months	SECURE DISPOSAL [by the designated member of staff]		**IL2–PROTECT**
6.41	Single Central Record	Yes	ISA guidelines	Keep until school closure	Offer to local authority designated officer		**IL2–PROTECT**

6.5	Disciplinary proceedings:		**Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.**				
6.5a	*oral warning*	Yes		Date of warning + 6 months.	SECURE DISPOSAL		**IL2–PROTECT**
6.5b	*written warning – level one*	Yes		Date of warning + 12 months.	SECURE DISPOSAL		**IL2–PROTECT**
6.5c	*final warning*	Yes		Date of warning + 12 months.	SECURE DISPOSAL		**IL2–PROTECT**
6.5d	*case not found*	Yes		If child protection related please see 1.2	SECURE DISPOSAL		**IL2–PROTECT**
6.6	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		**IL2–PROTECT**

6.7	Annual appraisal/assessment records	No		Current year + 5 years	SECURE DISPOSAL		**IL2–PROTECT**
6.8	Salary cards	Yes		Last date of employment + 85 years	SECURE DISPOSAL		**IL2–PROTECT**
6.9	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year, +3yrs	SECURE DISPOSAL		**IL2–PROTECT**
6.1	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**

6.11	Proof 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.		**IL2–PROTECT**

[1] If this is placed on a personal file it must be weeded from the file.

7 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**		**Protective Marking Classification**
7.1	Accessibility Plans	No	Disability Discrimination Act	Current year + 6 years	SECURE DISPOSAL		**IL1–Unclassified**

7.2	Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980				
7.2a	*Adults (All Accidents)*	Yes		Date of incident + 7 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
7.2b	*Children (All Accidents)*	Yes		DOB of child + 25 years[1]	SECURE DISPOSAL		**IL3 - RESTRICTED**
7.3	COSHH	No		Current year + 10 years [where appropriate an additional retention period may be allocated]	SECURE DISPOSAL		**IL1–Unclassified**
7.4	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
7.5	Policy Statements	No		Date of expiry + 1 year	SECURE DISPOSAL		**IL1–Unclassified**
7.6	Risk Assessments	No		Current year + 3 years	SECURE DISPOSAL		**IL1–Unclassified**

7.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No		Last action + 40 years	SECURE DISPOSAL		**IL1–Unclassified**
7.8	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation	No		SECURE DISPOSAL			**IL1–Unclassified**
7.9	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL		**IL1–Unclassified**

[1] A child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the pupil reaches the age of 25 this retention period has been applied.

8 Administrative							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
8.1	Employer's Liability certificate	No		Closure of the school + 40 years	SECURE DISPOSAL		**IL1–Unclassified**

8.2	Inventories of equipment and furniture	No		Current year + 6 years	SECURE DISPOSAL		**IL1–Unclassified**
8.3	General administrative records (records not specifically listed elsewhere)	No		Current year + 5 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
8.4	School brochure or prospectus	No		Current year + 3 years		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
8.5	Circulars (staff/parents/pupils)	No		Current year + 1 year	SECURE DISPOSAL		**IL1–Unclassified**
8.6	Newsletters, ephemera	No		Current year + 1 year	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
8.7	Visitors book	No		Current year + 2	Review to see	Transfer to Archives	**IL1–Unclassified**

				years	whether a further retention period is required	[The appropriate archivist will then take a sample for permanent preservation]	
8.8	PTA/Old Pupils Associations	No		Current year + 6 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
9 Finance							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
9.1	Annual Accounts	No	Financial Regulations	Current year + 6 years		Offer to the Archives	**IL2–PROTECT**
9.2	Loans and grants	No	Financial	Date of last	Review to see	Transfer to Archives	**IL2–PROTECT**

			Regulations	payment on loan + 12 years	whether a further retention period is required	[The appropriate archivist will then take a sample for permanent preservation]	
9.3	Contracts						
9.3a	under seal	No		Contract completion date + 12 years	SECURE DISPOSAL		**IL2–PROTECT**
9.3b	under signature	No		Contract completion date + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.3c	monitoring records (Bolton Council Corporate Property Unit may hold these records on the schools behalf)	No		Current year + 2 years	SECURE DISPOSAL		**IL2–PROTECT**
9.4	Copy orders	No		Current year + 2 years	SECURE DISPOSAL		**IL2–PROTECT**
9.5	Budget reports, budget monitoring etc	No		Current year + 3 years	SECURE DISPOSAL		**IL2–PROTECT**
9.6	Invoice, receipts and other records covered by the Financial Regulations	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**

9.7	Annual Budget and background papers	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.8	Order books and requisitions	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.9	Delivery Documentation	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.1	Debtors' Records	No	Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.11	School Fund – Cheque books	No		Current year + 3 years	SECURE DISPOSAL		**IL2–PROTECT**
9.12	School Fund – Paying in books	No		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**
9.13	School Fund – Ledger	No		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**
9.14	School Fund – Invoices	No		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**
9.15	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
9.16	School Fund – Bank statements	No		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**
9.17	School Fund – School Journey books	No		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**

9.18	Student Grant Applications	Yes		Current year + 6 years then review	SECURE DISPOSAL		**IL2–PROTECT**
9.19	Free school meals registers	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
9.20	Petty cash books	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
10 Property							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
10.1	Title Deeds	No		Permanent	Permanent these should follow the property unless the property has been registered at the Land Registry	Offer to Archives if the deeds are no longer needed	**IL2–PROTECT**
10.2	Plans	No		Permanent	Retain in school whilst operational	Offer to Archives[1]	**IL3 - RESTRICTED**
10.3	Maintenance and contractors	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**

10.4	Leases	No		Expiry of lease + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
10.5	Lettings	No		Current year + 3 years	SECURE DISPOSAL		**IL2–PROTECT**
10.6	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**
10.7	Maintenance log books	No		Last entry + 10 years	SECURE DISPOSAL		**IL1–Unclassified**
10.8	Contractors' Reports	No		Current year + 6 years	SECURE DISPOSAL		**IL2–PROTECT**

[1] If the property has been sold for private housing then the archives service will embargo these records for an appropriate period of time to prevent them being used to plan or carry out a crime.

11 Local Education Authority							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
11.1	Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
11.2	Attendance returns	Yes		Current year + 1 year	SECURE DISPOSAL		**IL3 - RESTRICTED**

11.3	Circulars from LEA	No		Whilst required operationally	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL1–Unclassified**
12 Department for Children, Schools and Families							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
12.1	OFSTED reports and papers	No		Replace former report with any new inspection report	Schools may wish to retain copies of former reports for longer	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]	**IL2–PROTECT**
12.2	Returns	No		Current year + 6 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
12.3	Circulars from	No		Whilst operationally	Review to see	Transfer to Archives	**IL1–Unclassified**

	Department for Children, Schools and Families			required	whether a further retention period is required	[The appropriate archivist will then take a sample for permanent preservation]	
13 Careers							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
13.1	Service level agreements	No		Until superseded	SECURE DISPOSAL		**IL1–Unclassified**
13.2	Work Experience agreement	Yes		DOB of child + 18 years	SECURE DISPOSAL		**IL3 - RESTRICTED**
14 Schools Meals							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**

14.1	Dinner Register	Yes		C + 3 years	SECURE DISPOSAL		**IL2–PROTECT**
14.2	School Meals Summary Sheets	Yes		C + 3 years	SECURE DISPOSAL		**IL2–PROTECT**
15 Family Liaison Officers and Parent Support Assistants							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
15.1	Day Books	Yes		Current year + 2 years then review	SECURE DISPOSAL		**IL3 - RESTRICTED**
15.2	Reports for outside agencies – where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school then destroy	SECURE DISPOSAL		**IL3 - RESTRICTED**
15.3	Referral forms	Yes		While the referral is current then	SECURE DISPOSAL		**IL4-Confidential**
15.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL		**IL2–PROTECT**

15.5	Contact database entries (FLO contact records with agencies and family member)	Yes		Current year then review, if contact is no longer active then destroy	DELETE		**IL2–PROTECT**
15.6	Group Registers (FLO work)	Yes		Current year + 2 years	SECURE DISPOSAL		**IL2–PROTECT**
15.7	Early Help Assessments	Yes		Current year + 6	SECURE DISPOSAL		**IL4-Confidential**
16 Early Years Provision (Childcare / Nursery provision etc.)							
16.1 Records to be kept by Registered Persons - All Cases							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
16.1.1	The name, home address and date of birth of each child who is looked after on the premises	Yes		Closure of setting + 50 years			**IL3 - RESTRICTED**

				[These could be required to show whether or not an individual child attended the setting in a child protection investigation]			
16.1.2	The name, home address and telephone number of a parent of each child who is looked after on the premises	Yes		If this information is kept in the same book or on the same form as in 16.1.1 then the same retention period should be used as in 16.1.1			**IL3 - RESTRICTED**
				If the information is stored separately, then destroy once the child has left the setting (unless the information is collected for anything other than emergency contact)			

16.1.3	The name, address and telephone number of any person who will be looking after children on the premises	Yes		See 16.4.5 below			**IL3 - RESTRICTED**
16.1.4	A daily record of the names of children looked after on the premises, their hours of attendance and the names of the persons who looked after them	Yes	The Day Care and Child Minding (National Standards) (England) Regulations 2003	The regulations say that these records should be kept for 2 years (SI20031996 7(1b)). If these records are likely to be needed in a child protection setting (see 16.1.1 above) then the records should be retained for closure of setting + 50 years			**IL3 - RESTRICTED**
16.1.5	A record of accidents occurring on the premises and incident books relating to other incidents	Yes	The Day Care and Child Minding (National Standards) (England) Regulations 2003[1]	DOB of the child involved in the accident or the incident + 25 years			**IL2–PROTECT**
				If an adult is injured then the accident book must be kept for 7 years from the date of the incident			

16.1.6	A record of any medicinal product administered to any child on the premises, including the date and circumstances of its administration, by whom it was administered, including medicinal products which the child is permitted to administer to himself, together with a record of parent's consent	Yes	The Day Care and Child Minding (National Standards) (England) Regulations 2003[2]	DOB of the child being given/taking the medicine + 25 years			**IL3 - RESTRICTED**
16.1.7	Records of transfer	Yes		One copy is to be given to the parents, one copy transferred to the Primary School where the child is going			**IL2–PROTECT**

16.1.8	Portfolio of work, observations and so on	Yes		To be sent home with the child			**IL2–PROTECT**
16.1.9	Birth certificates	Yes		Once the setting has had sight of the birth certificate and recorded the necessary information the original can be returned to the parents. There is no requirement to keep a copy of the birth certificate.			**IL3 - RESTRICTED**
[1] The regulations say that these records should be kept for 2 years (SI20031996 7(1b)). The Statute of Limitations states that a minor may make a claim for 7 years from their eighteenth birthday, therefore the retention should be for the longer period.							

[2] The regulations say that these records should be kept for 2 years (SI20031996 7(1b)). The NHS records retention schedule states that any records relating to a child under the age of 18 should be retained until that child reaches the age of 25 years. Therefore, the retention should be DOB of the child being given/taking the medicine + 25 years

16.2 Records to be kept by Registered Persons - Day Care
(Relates to nursery and child minding provision

	Basic file description	Data Prot Issues	Statutory Provisions	Retention period [operational]	Action at the end of the administrative life of the record		Protective Marking Classification
16.2.1	The name and address and telephone number of the registered person and every other person living or employed on the premises	Yes		See 16.4 below			**IL3 - RESTRICTED**

16.2.2	A statement of the procedure to be followed in the event of a fire or accident	No		Procedure superseded + 7 years			**IL1–Unclassified**
16.2.3	A statement of the procedure to be followed in the event of a child being lost or not collected	No		Procedure superseded + 7 years			**IL1–Unclassified**
16.2.4	A statement of the procedure to be followed where a parent has a complaint about the service being provided by the registered person	No		Until superseded			**IL1–Unclassified**

16.2.4	A statement of the arrangements in place for the protection of children, including arrangements to safeguard the children from abuse or neglect and procedures to be followed in the event of allegations of abuse or neglect	Yes		Closure of setting + 50 years			**IL4-Confidential**
				[These could be required to show whether or not an individual child attended the setting in a child protection investigation]			
16.3 Records to be kept by Registered Persons - Overnight provision – under 2's							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**

16.3.1	Emergency contact details for appropriate adult to collect the child if necessary	Yes		Destroy once the child has left the setting (unless the information is collected for anything other than emergency contact)			**IL3 - RESTRICTED**
16.3.2	Contract, signed by the parent, stating all the relevant details regarding the child and their care, including the name of the emergency contact and confirmation of their agreement to collect the child during the night	Yes		Date of birth of the child who is the subject of the contract + 25 years			**IL3 - RESTRICTED**
16.4 Other Records – Administration							
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**		**Protective Marking Classification**
Financial Records							

16.4.1	Financial records – accounts, statements, invoices, petty cash etc	No		Current year + 6 years			**IL2–PROTECT**
Insurance							
16.4.2	Insurance policies – Employers Liability	No	Employers Liability Financial Regulations	The policies are kept for a minimum of 6 years and a maximum of 40 years depending on the type of policy			**IL1–Unclassified**
16.4.3	Claims made against insurance policies – damage to property	Yes		Case concluded + 3 years			**IL2–PROTECT**
16.4.4	Claims made against insurance policies – personal injury	Yes		Case concluded + 6 years			**IL2–PROTECT**
Human Resources							
16.4.5	Personal Files - records relating to an individual's employment history	Yes		Termination + 6 years then review			**IL3 - RESTRICTED**

16.4.6	Pre-employment vetting information (including DBS checks)	No	DBS guidelines	Date of check + 6 months			**IL4-Confidential**
16.4.7	Staff training records – general	Yes		Current year + 2 years			**IL2–PROTECT**
16.4.8	Training (proof of completion such as certificates, awards, exam results)	Yes		Last action + 7 years			**IL2–PROTECT**
	Premises and Health and Safety						
16.4.9	Premises files (relating to maintenance)	No		Cessation of use of building + 7 years then review			**IL1–Unclassified**
16.4.10	Risk Assessments	No		Current year + 3 years			**IL1–Unclassified**

[1] For Data Protection purposes the following information should be kept on the file for the following periods :

• all documentation on the personal file	Duration of employment
• pre-employment and vetting information	Start date + 6 months
• records relating to accident or injury at work	Minimum of 12 years
• annual appraisal/assessment records	Minimum of 5 years
• records relating to disciplinary matters (kept on personal files)	

	o oral warning	6 months
	o first level warning	6 months
	o second level warning	12 months
	o final warning	18 months