Data Protection Policy

Policy Level	Statutory	Ref No	ICT02
Approved by	Risk & Audit Committee	Approved date	27.06.25
Responsibility	DPO/CFOO	Next review	Summer Term 2026
Version Number	**Date Issued**	**Author**	**Update Information**
3.0	30.06.25	DPO/CFO	Supersedes policy dated June 2024

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 school 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. In addition this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

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

4.2 The 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 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 the 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 school complies with all relevant data protection obligations.

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

6.3 **Headteacher** - the Headteachers acts as the representative of the Data Controller on a day-to-day basis. The Headteacher is responsible for ensuring that their school is compliant to data protection laws. The Headteacher 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 school of any changes to their personal data, such as a change of address
- Contacting the CFOO/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

BIT 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 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 school.

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

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 BIT 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:

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

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

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

8.14 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.

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

8.16 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 school we may collect and **process** the **personal data** set out in our 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 **Record of Data Processing Activi**ties or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

9.3 The **Record of Data Processing Activities** will be reviewed on an at least annual basis by the CFO although some sections may be delegated to and reviewed by other member of staff. It will also be reviewed when a significant change to data processing occurs and in line with recommendations made in any **DPIAs** (see section 17).

9.4 The **Record of Data Processing Activities** will is a comprehensive overview of how we organise and process personal data. It includes information on school's/trust's function, the purpose of processing, names and contact details of joint controllers (if applicable), categories of data subjects, categories of personal data, with whom the data may be shared, contracts with third party data processors, internation transfers (if applicable), retention schedules, technical and organisations security measures, lawful basis for processing, rights of the individual, whether automated decision making has been used, the source of the personal data, access arrangements and whether any DPIAs have been completed.

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 4

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 BIT 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 BIT for these purposes. Privacy Notices detailing how the information will be stored and used can be accessed through the BIT 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.

13.2 BIT will maintain a data retention and disposal schedule which is an annual review of school records and data destruction which aligns with our retention schedule (see Appendix 4).

13.3 BIT is responsible for ensuring that this annual review takes place and that the Annual Review of School Records and Data Destruction checklist is completed. Some sections may be delegated to specific members of staff/roles.

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 **Subject Access requests -** data subjects may request access to all **personal data** that the Trust holds about them. Such requests will be considered in line with the Trust's **Subject Access Request** Procedure. This procedure is available on the Trust website.

14.3 Individuals have a right to make a '**subject access request'** to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

14.4 **Subject access requests** can be either verbal or in writing (letter or email). To ensure greatest clarity it is preferred that such requests are made in writing. must be submitted in writing. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested
- How the requestee would like the information to be shared with them (eg. paper or electronic format)

14.5 If staff receive a subject access request, they must immediately forward it to the DAO or CFO. (See Appendix 2 for Procedures relating to **Individual Rights**)

14.6 **Children and subject access requests** - Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

If a young person is 13 years or over and is felt to have the maturity and competency to understand the request and the nature of the information that will be shared their consent should be sought to check that they are happy for their personal data to be shared with their parent/carer.

14.7 **Responding to subject access requests -** When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge

- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

14.8 We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child.

14.9 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

14.10 A parent/carer can request to see their child's **educational record**, or request it on behalf of their child, in writing. The information will be presented within 15 school days of receiving the request. There will be no charge for the information requested. As an School 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

14.11 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.

1.12 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**.

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

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

14.6 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

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

14.8 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.

14.9 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

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

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

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

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

14.10.4 where the **processing** is unlawful but the **data subject** has asked BIT not to delete the **personal data**

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

14.11 If BIT 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.

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

The Right to Be Forgotten

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

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

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

14.13.3 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.

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

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

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

14.13.6 to exercise the right of freedom of expression or information

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

14.14 for public health purposes in the public interest

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

14.16 in relation to a legal claim.

14.17 If BIT 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 main School 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

15.3.6 **Working away from the school premises – electronic working.** Guidance procedures are available for staff

15.3.7 **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

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 BIT 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 schools and implement a thorough data breach action plan to manage if/when a data breach occurs. Procedures are set out in Appendix 3.

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 school laptop containing non-encrypted personal data about pupils

17. Data Protection Impact Assessments

17.1 BIT 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 BIT will complete an assessment of any such proposed **processing** at the procurement stage and prior to any processing taking place 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.

17.5 The **Record of Data Processing Activities** (see section 9.3) will be updated in line with any recommendations made as part of a **data protection impact assessment** to reflect the new data processing.

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, Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so. This may include:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

18.2 Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

18.3 BIT 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.

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

18.5 Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

18.6 Further detail is provided in our Record of Data Processing Activities.

18.7 Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

19. Data processors

19.1 We contract with various organisations who provide services to BIT; these are detailed within the 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 BIT. BIT 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. BIT will get written consent from at least one parent or carer before we take any biometric data from their child and first process is. BIT 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 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. BIT does not prohibit this as a matter of policy.

21.2 BIT 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 school to prevent.

21.3 BIT 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 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 and Year 8 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 9, 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. For our secondary pupils, we will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils 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.

22. CCTV

22.1 BIT operates a CCTV system in its schools. 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 Trust will only use surveillance cameras for the safety and security of the school and 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 BIT's CCTV policy is available on the website (insert hyperlink)

23. Training

23.1 All staff, governors and trustees are provided with data protection training as part of their induction process.

23.2 Data protection training also forms part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary Specific training will be provided for staff who handle personal information and especially special category personal data and/or that is pertinent to their role,

23.3 Best practice requires that all staff complete suitable training on an annual basis. At the Trust all staff will complete at least one annual piece of GDPR-related training with half termly refreshers/briefings being discussed at staff meetings.

23.4 A record of staff completion of training will be maintained by Office team to ensure that all staff have completed the necessary training

24. Data Retention

Bolton Impact Trust maintains a records management policy. The retention schedule is based on guidance from the DfE. It encompasses records managed by all types of school – some of the file descriptions listed may not be relevant to every school.

The Trust has a separate Data Retention policy.

25. 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 retention and disposal schedule	This is an annual review of schools records and data destruction checklist which aligns with the Retention Schedule (Appendix 4)
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.
Individual Rights of a Data Subject	Under GDPR there are 8 individual rights (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/): • Right to be informed • Right of access • Right to rectification • Right to erasure • Right to restrict processing • Right to data portability • Right to object

Information Commissioner's Office (ICO)	The Information Commissioner's Office is the legal authority who managed GDPR and Data Protection.
Privacy Notices	A Privacy Notice can also be known as a "fair processing notice" and is a document that informs data subjects about how their personal data is collected, used and protected. It offers transparency in data processing and helps individuals understands their rights and the risks associated with data collection.
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.
Record of Data Processing Activities or record of Processing Activities (ROPA)	A Record of Data Processing Activities or A Record of Processing Activities (ROPA) is a documented overview of all personal data processing activities an organisation undertakes. It's a key requirement under the General Data Protection Regulation (GDPR) and other data protection laws, designed to demonstrate compliance and accountability.
Retention schedule	The retention and disposal schedule outlines how long records should be kept and how they should be disposed of. This is a separate document.
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 the Trust such as staff and those who volunteer in any capacity including governors, trustees & members.

Appendix 2a

Procedures relating to Individual's Rights

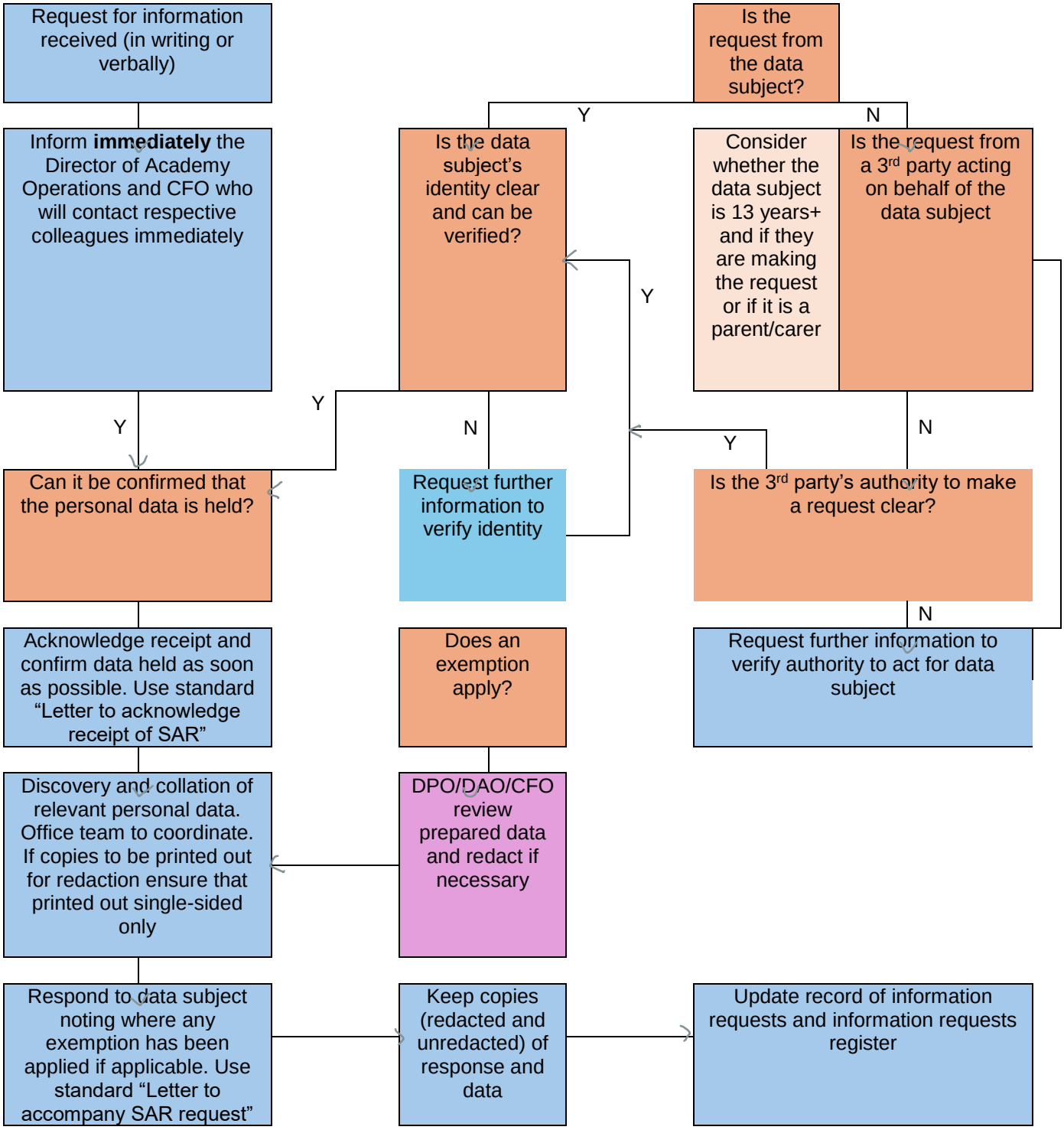
There are 8 Rights for Individuals under GDPR (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/)

Whenever an individual

	Summary	Reference in policy
Right to be informed	Individuals have the right to be informed about the collection and used of their personal data	This is included in **Privacy Notices**
Right of access	Individuals have the right to access and receive a copy of their personal data and other supplementary information. This is often called a **Subject Access Request (SAR)** **See below for school/trust specific procedures**	Paragraphs 14.2 – 14.10
Right to rectification	UK GDR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete	Paragraphs 14.16 – 14.18
Right to erasure/right to be forgotten	Individuals can have their personal data erased	Paragraphs 14.23 – 14.25
Right to restrict processing	Individuals have the right to request the restation or suppression of their personal data	Paragraphs 14.16 – 14.18
Right to data portability	The right to data portability allows individuals to obtain reused their personal data for their own purposes across different services	Paragraphs 14.26 – 14.27
Right to object	UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances	Paragraphs 14.11 – 14.15
Rights related to automated decision-making including profiling		This is included in **Privacy Notices**

Appendix 2b

Procedures relating to Individual's Rights – responding to a Subject Access Request



Appendix 2c

Record of Information Requests

Type of Information request	Subject Access Request (SAR)		Freedom of Information Request (FOI)		Request by parent to see their child's educational record (N/A for academies)	
Time scale to respond	30 days from receipt		20 school days from receipt		15 school days from receipt	

Please tick appropriate box

Date request received		**Response deadline**	
Date response sent		**Format in which information sent**	
Name of requestor		**Contact details of requestor**	
Name of data subject			

Details of information requested (If SAR details of personal data requested) *Copy and paste request*	
Identity verified for data subject and requestee if different *(eg solicitor) (List verification eg. passport, birth certificate)*	
Consent/authorisation given *(Form of Authority or consent from YP if 13 years+ or request from 3rd party)*	
If rejected reason for rejection	
If extended deadline, reason for extension	
Any applicable charges	
Redactions *(List reasons why redactions have been made)*	
Response given *Copy and paste/add as attachment*	

Appendix 3

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 CFOO and 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 CFOO, who will communicate as appropriate within the Trust. 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 school's computer system. The DPO and Head Teacher 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