Data Protection Policy

For the Following Academies:

Holy Trinity C of E Primary School
Connaught Junior School
Crawley Ridge Infant School
Crawley Ridge Junior School
Windlesham Village Infant School

This Data Protection Policy was approved and adopted by the Trust Board: Aut: 2021
It will be reviewed: Aut: 2022

Contents

1 Policy Statement

1.1 Everyone has rights about the way in which their **personal data** is handled. During the course of our activities as a 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** all **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**.

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 the Annex to this policy.

4 Data Protection Officer

4.1 As a Trust we are required to appoint a Data Protection Officer (DPO). Our DPO is Ms Johnstone, and can be contacted on info@tamat.org.uk

4.2 The DPO is responsible for ensuring compliance with 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.

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

5 Data protection principles

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

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

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

5.1.3 adequate, relevant, and not excessive for the purpose.

5.1.4 accurate and up to date.

5.1.5 not kept for any longer than is necessary for the purpose.

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

5.2 **Personal data** must also:

5.2.1 be **processed** in line with **data subjects'** rights.

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

5.3 We will comply with these principles in relation to any **processing** of **personal data** by the Trust and in each academy school within it.

6 Fair and lawful processing

6.1 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**.

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

6.2.1 that **personal data** is being **processed.**

6.2.2 why the **personal data** is being **processed.**

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

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

6.2.5 the period for which the **personal data** will be held.

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

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

6.3 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**.

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

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

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

6.4.3 where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest for example it is not necessary to seek consent to share information for the purpose of safeguarding and promoting the welfare of a child provided that there is a lawful basis to process any personal information required.

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

6.5 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 the following legal grounds:

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

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

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

6.5.4 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.**

6.6 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 join us.

6.7 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

6.8 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

6.9 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.

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

6.11 When pupils and or our **workforce** join TAMAT 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.

6.12 In relation to all pupils under the age of 12 years old, we will seek consent from an individual with parental responsibility for that pupil.

6.13 We will generally seek consent directly from a pupil who has reached the age of 12; however we recognize that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

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

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

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

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

6.15 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.

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

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

7 Processing for limited purposes

7.1 In the course of our activities as a school we may collect and **process** the **personal data** set out in our Schedule of 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**).

7.2 We will only **process personal data** for the specific purposes set out in our Schedule of 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.**

8 Notifying data subjects

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

8.1.1 our identity and contact details as **Data Controller** are those of the DPO.

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

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

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

8.1.5 the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy.

8.1.6 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.

8.1.7 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.

8.2 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.

9 **Adequate, relevant, and non-excessive processing**

9.1 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.

10 **Accurate data**

10.1 We will ensure that **personal data** we hold is accurate and kept up to date in line with school policy and procedures.

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

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

11 **Timely processing**

11.1 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 system, all **personal data** where is no longer required.

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

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

12.1.1 request access to any **personal data** we hold about them.

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

12.1.3 have inaccurate or incomplete **personal data** about them rectified.

12.1.4 restrict **processing** of their **personal data.**

12.1.5 have **personal data** we hold about them erased.

12.1.6 have their **personal data** transferred.

12.1.7 object to the marking of decisions about them by automated means.

The right of access to personal data

12.2 Data subjects may request access to all **personal data** we hold about them. Such requests will be considered in line with the Trusts Subject Access Request (SAR) Procedure. These should be made in writing to the Data Protection Officer on info@tamat.org.uk

The right to object

12.3 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.

12.4 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.**

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

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

12.7 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

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

12.9 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.

12.10 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

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

12.12 The Trust or academy school within it must restrict the **processing** of **personal data**:

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

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

12.12.3 where the **processing** is unlawful, but the **data subject** has asked TAMAT not to delete the **personal data.**

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

12.13 If TAMAT 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.

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

The right to be forgotten

12.15 **Data subjects** have a right to have **personal data** about them held by TAMAT erased only in the following circumstances:

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

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

12.15.3 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.

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

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

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

12.15.6 To exercise the right of freedom of expression or information.

12.15.7 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law.

12.15.8 For public health purposes in the public interest.

12.15.9 For archiving purposes in the public interest, research or statistical purposes.

12.15.10 In relation to a legal claim.

12.16 If TAMAT 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.

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

Right to data portability

12.18 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 other organisations.

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

13 Data security

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

13.2 TAMAT 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.

13.3 Security procedures include:

13.3.1 **Entry controls**. Any stranger seen in entry-controlled areas should be reported to both the Headteacher of the Academy and the CO who is also the DPO.

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

13.3.3 **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.

13.3.4 **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.

13.3.5 **Working away from the school premises – paper documents.** Teachers and staff have a lawful basis to take books and pupil work home to mark. When they do so they should make sure that they keep these documents in bags or in their boots when transporting by car. Once home and not being worked on they should be kept securely inside the house.

When taking more confidential and detailed information about pupils such as school records or safeguarding and SEND files, they should make sure they transport them in the same way. They should complete a sign in and out sheet and pass to the local Data Protection Lead in their school. Confidential information should be returned to the school and replaced in the secure area it was taken from.

When at home, staff should place all documents in a secure area of their house and keep them somewhere specific such as a certain drawer or tray to prevent them from being lost. In particular, staff should avoid leaving documents in their car, as this creates a higher risk of them being stolen. When returning them to school, they should take the documents to their original storage place rather than leaving them on desks unless this is for teaching purposes.

13.3.6 **Working away from the school premises – electronic working**

When working with electronic data that falls under this policy, staff are required to access this through secure networks and protections put in place by each Academy. If staff stop working from their laptop or PC, they should use Windows L or Apple Equivalent to put their laptop or PC into password mode.
The use of non-encrypted USB sticks is strictly prohibited. No personal devices should be used to download or hold school data. If a member of staff is using a mobile device to check school emails, this device should be password protected.

13.3.7 **Document printing**

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

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

14 Data protection impact statements

14.1 TAMAT 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.

14.2 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 we intend to do so.

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

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

15 Disclosure and sharing of personal information

15.1 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.

Consent can be withdrawn at any time by the data subject.

15.2 TAMAT 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 through a written request from the police.

15.3 In some circumstances we will not share safeguarding information. Please refer to our Safeguarding and Child Protection Policy for each Academy.

15.4 Further detail is provided in our Schedule of Processing Activities.

16 Data processors

16.1 We contract with various organisations that provide services to TAMAT including:

16.1.1 Payroll providers, School Meal providers, Management Information System Providers, Finance System Providers, Email and Communication System Providers, Safeguarding System Providers, Performance Management System Providers, Site Entry System Providers and SEND System Providers.

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

16.3 **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 TAMAT. The Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

16.4 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.**

17 **Images and videos**

17.1 Parents and others attending TAMAT 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. TAMAT does not prohibit this as a matter of policy unless it is prohibited by a license agreement.

17.2 TAMAT 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 TAMAT to prevent.

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

17.4 As TAMAT 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. TAMAT will seek the consent of parents and carers before allowing the use of images or videos of pupils for such purposes.

17.5 Whenever a pupil begins their attendance at an academy school within TAMAT they, or their parents where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

18. **Use of CCTV**

18.1 TAMAT Schools may use CCTV around the school site to ensure it remains safe. We will adhere to the ICO's Code of Practice for the use of any CCTV.
We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
Any enquiries about the CCTV system should be directed to the DPO (Ms Johnstone) in the first instance.

19 **Changes to this policy**

This policy will be reviewed and subject to change to meet legal requirements. 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 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. All data subjects have legal rights in relation to their personal information.
Personal Data	Any information relating to an identified or identifiable natural person (a data subject); an identifiable 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.
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 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.
Data Processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
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.
Workforce	Includes any individual employed by the Trust such as staff and those who volunteer in any capacity including governors/trustees/members/parent helpers.

APPENDIX 2
Privacy Notice for Parents and Carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about pupils.
We, TAMAT, are the 'data controller' for the purposes of data protection law.
Our Data Protection Officer for the Trust is Ms Johnstone. The Data Protection Lead for each school can be contacted by emailing the school.

The Personal Data We Hold
Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data
We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Comply with the law regarding data sharing

Our legal basis for using this data
We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn by writing to the Data Protection Officer for TAMAT.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information
While most of the information we collect about pupils is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional.

How we store this data
We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our retention schedule sets out how long we keep information about pupils and is set against the Information and Records Management Society's toolkit for schools.

Data sharing
We do not share information about pupils with **any third party without consent unless the law and our policies allow us to do so**. Where it is legally required or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education – to meet our statutory obligations as state funded schools
- The pupils' family and representatives – to enable us to make usual or emergency contacts
- Educators and examining bodies – to meet our statutory obligations as state funded schools
- Our regulator (Ofsted) – to meet our statutory obligations as state funded schools
- Suppliers and service providers - to enable them to provide the service we have contracted them for such as catering
- Health and social welfare organisations – to meet our statutory obligations as state funded schools
- Professional advisers and consultant – to enable us to quality assure the effectiveness of education provided for our pupils
- Police forces, courts, tribunals – under legal obligations

National pupil database
We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census and end of key stage assessment reporting.
Some of this information is then stored in the National Pupil Database, which is owned and managed by the Department and provides evidence on school performance to inform research.
The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities, and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.
For more information, see the Department's webpage on how it collects and shares data.
You can also contact the Department for Education with any further questions about the NPD.

Transferring data internationally
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.

Parents and pupils' rights regarding personal data
Individuals have a right to make a '**subject access request'** to gain access to personal information that the school holds about them. Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent. Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you mad a subject access request, and if we do hold information about you or your child we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be shared with
- Let you know whether any automated decision-making is being applied to the data and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.
If you would like to make a request, please contact our Data Protection Officer on info@tamat.org.uk

Other rights
Under Data Protection Law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the Data Protection Regulations

To exercise any of these rights, please contact our Data Protection Officer on info@tamat.org.uk

Complaints
We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing please raise it with us in the first instance.
To make a complaint please contact our Data Protection Officer.
Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

- Ms Johnstone on info@tamat.org.uk

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in our schools.

Privacy Notice for Pupils

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.
This privacy notice explains how we collect, store, and use personal data about you.
We, TAMAT, are the 'data controller' for the purposes of Data Protection Law.
Our Data Protection Officer is Ms Johnstone (see 'Contact Us' below).

The personal data we hold
We hold some personal information about you to make sure we can help you learn and look after you at school.
For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.
This information includes:

- Your contact details
- Your test results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs

Why we use this data
We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Check how you are doing in exams and work out whether you or your teachers need any extra help
- Track how well the school is performing
- Look after your well-being

Our legal basis for using this data
We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interests)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission and explain how to go about withdrawing consent.
Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information
While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether to provide the data.
We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store the data
We will keep personal information about you while you are a pupil at one of our schools. We may also keep it after you have left the school, where we are required to by law.
We have a retention schedule, which sets out how long we must keep information about pupils. This follows guidance from the Information and Records Management Society's toolkit for schools.

Data sharing
We do not share personal information about you with anyone outside the school without consent from you or your parents/carers unless the law and our policies allow us to do so.
Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with our local authority and the Department of Education to make sure we are providing you with a good education, your family and representatives to keep you safe and companies like our caterers to make sure we provide you with the best resources and services.

National Pupil Database
We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.
Some of this information is then stored in the National Pupil Database which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.
The database is held electronically so it can easily be turned in statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.
The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.
You can find more information about this on the Department for Education's webpage on how it collects and shares research data.
You can also contact the Department for Education if you have any questions about the database.

Transferring data internationally
Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights
How to access personal information we hold about you
You can find out if we hold any personal information about you, and how we use it, by making a 'subject access request,' as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances. If you want to make a request, please contact our Data Protection Officer.

Your other rights over your data
You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you do not want it to be used if this would cause or is causing harm or distress
- Stop it being used to send you marketing materials

- Say that you don't want it used to make automated decisions (decisions made by a computer or machine rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints
We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.
You can make a complaint at any time by contacting our Data Protection Officer.
You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact your class teacher or school office who will pass on the information to Ms Johnstone.

This notice is based on the *Department for Education's model privacy notice* for pupils, amended to reflect the way we use data in this school.

Privacy Notice for Staff

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.
This privacy notice explains how we collect, store, and use personal data about individuals we employ, or otherwise engage to work at our schools.
We, TAMAT are the 'data controller' for the purposes of data protection law.
Our Data Protection Officer is Ms Johnstone (see 'Contact us' below).

The personal data we hold
We process data relating to those we employ, or otherwise engage to work at our school. Personal data that we may collect, use, store, and share (when appropriate) about you includes, but not restricted to:

- Contact details
- Date of birth, marital status, and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension, and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV cover letter or as part of the application process including information about criminal disclosures and from the Disclosure and Barring Service. Prior to making any criminal disclosure you may wish to seek independent legal advice or contact a relevant organisation e.g. NACRO or UNLOCKED.
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving license
- Photographs
- Data about your use of the school's information and communication system

We may also collect, store, and use information about you that falls int 'special categories' of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation, and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data
The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Our lawful basis for using this data
We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered with you
- Comply with legal and safeguarding obligations
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you go about withdrawing consent if you wish to do so. Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data without your consent.

Collecting this information
While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.
Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are for not complying), or whether you have a choice.

How we store this data
We create and maintain an employment file for each member of staff. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.
Once your employment with us has ended, we will retain this file and delete the information in accordance with our retention schedule which aligns to the Information and Records Management Society's toolkit for schools.

Data Sharing
We do not share information about you with any third party without your consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- The Department for Education – to meet our legal obligations in relation to school workforce census
- Your family or representatives – to enable us to make contact in an emergency
- Educators and examining bodies – as part of safer recruitment
- Ofsed – only when it meets statutory regulation
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Our auditors – to meet our legal requirements to produce an annual set of financial statements
- Survey and research organisations – to allow us to gain vital stakeholders feedback
- Trade union associations – to make sure we are complying with the law and looking after our workforce
- Health authorities – to enable us to meet your health needs if required such as maternity rights and procedures
- Health and social welfare organisations
- Professional advisers and consultants – to enable us to quality assure your work on improving education for our children
- Charities and voluntary organisations – to enable us to work with bodies such as our PTAs
- Police forces, courts, tribunals – to meet our legal obligations
- Professional bodies – to enable us to gain access to high quality professional development

Transferring data internationally
Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with UK Data Protection Law.

Your rights
How to access personal information we hold about you
Individuals have a right to make a '**subject access request'** to gain personal information that the school holds about them.
If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.
If you would like to make a request, please contact our Data Protection Officer.

Your other rights regarding your data
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if that would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the sue of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted, or destroyed or restricted processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer

Complaints
We take any complaint about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing please raise this with us in the first instance.
To make a complaint, please contact our Data Protection Officer through your Headteacher.
Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 1231113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

- Ms Johnstone on info@tamat.org.uk

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in our schools.

Privacy Policy for Job Applicants

The purpose of this privacy notice is to explain to you the data we collect about job applicants as part of our recruitment and selection process.

Data Controller: The Alliance Multi Academy Trust
Data Protection Officer: Ms Ann Johnstone

What Information do we collect about Job Applicants and how?

The categories of information we collect, process, hold and share:

- Personal information (such as name, address, date of birth, contact details, National Insurance Number, Teacher Number – if required).
- Education history, details of qualifications and relevant professional development
- Membership of Professional Bodies
- Employment history (including any gaps in employment and/or education/training)
- Information about reasonable adjustments we may need to make to the shortlisting or interview and assessment process to accommodate a disability
- Information on cautions, convictions, reprimands or final warnings which are not filtered as defined by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended) along with any current police investigations or pending criminal proceedings, including the Self Disclosure Form. You may be asked for information about the above after shortlisting and prior to an interview taking place. You may wish to take independent advice on the disclosure of the information set out above e.g. from www.nacro.org.uk / www.unlock.org.uk
- Information on any disqualification or sanction imposed by a Regulatory Body in relation to working with children
- Information on your DBS Update Service (if applicable)
- Information on any close personal relationships you may have with an existing member of staff, Governing Body, Trust Board or Members
- Proof of your identity if invited to interview
- Special categories of data (including information about your ethnic origin and health conditions) in order for us to monitor the success of our Equality Policies

We collect information from your application form and if shortlisted for interview as part of our selection process which generally includes an interview and some other form of assessment, such as presentations and written tests.

It is our Policy, (in line with DfE statutory guidance), Keeping Children Safe in Education to request references at the shortlisting stage, in advance of the interview. If you have any concerns about this you should contact us before submitting your application. If you are shortlisted, we will also collect data about you from your nominated Referees. Personal data may also be collected from other previous employers listed on your application form to verify information from your application form such as particular experience or qualifications.

If an offer of employment is made to you, the offer will be subject to subject to a number of pre-employment checks to our satisfaction, including a criminal record check with the Disclosure and Barring Service and a pre-employment Health assessment. You will be informed of the checks to be undertaken when an offer is made.

Why We Collect and use this Information

We process data from applicants to undertake the recruitment process and for successful applicants to enter a contract of employment. In particular data is used to:

- Administer the application, shortlisting and selection process
- Assess your suitability to work with children and young people
- Inform the development of recruitment and retention policies
- Defend legal claims

- Monitor protected characteristics in order to promote equality at work

The Lawful Basis on which we process this Information

We process this information about you because the processing is necessary for us to enter into an employment (or other work-related) contract with you. We also need to process this information to ensure that we are complying with our legal obligations and in particular with the DfE statutory guidance document, *Keeping Children Safe in Education*, such as by carrying out pre-employment checks on your right to work in the UK and with the Disclosure and Barring Service. It is not necessary to seek consent to share information for the purpose of safeguarding and promoting the welfare of the child provided that there is a lawful basis to process any personal information required.

We have a legitimate interest in processing data from job applicants in order to administer the recruitment process, to monitor compliance with our policies, to defend any legal claims and to ensure that the most suitable applicant is appointed to the role, based on an assessment of their likely performance amongst other factors. We do not rely on legitimate interests as a reason for processing data unless we have first considered the rights and freedoms of the individuals affected and determined that these do not override the interests we have identified.

We process special category data, such as information about your ethnic origin or health, as part of our equal opportunities monitoring process and in order to meet legal obligations (such as the requirement to make reasonable adjustments for job applicants with a disability). This information is collected with the express consent of job applicants. Consent may be withdrawn by an applicant at any time.

We may offer to contact unsuccessful applicants within a period of six months following the application if another suitable vacancy arises. Information is only used in this way with the express consent of applicants, which may be withdrawn at any time.

If we wish to process your personal data for a new purpose we will inform you of any additional processing.

Collecting This Information

Personal data provided to us as part of the recruitment and selection process is generally given on a voluntary basis and, as such, you have a choice as to whether you provide information to us. However, failure to provide information may mean that your application cannot be processed. You should also be aware that providing false or misleading information (including by omission) may result in your application being rejected and could also be treated as a disciplinary offence in the event that employment is subsequently offered to you.

Posts in our organisation are exempt from the Rehabilitation of Offenders Act 1974 (as amended). If you decide to apply for a position and are subsequently shortlisted you must disclose any cautions and convictions, even if they are spent, **other than** protected cautions and convictions (i.e. those which have been filtered out).

Details on the filtering rules applicable to certain offences can be found on the following websites:

https://www.gov.uk/government/collections/dbs-filtering-guidance

https://www.nacro.org.uk

Equality monitoring information is undertaken only for the purposes of evaluating our equality policies. It is not mandatory and its provision or otherwise will have no effect on the processing of your application form.

Storing this Information

Information from your application form and from the shortlisting and selection process will be stored in a paper-based file, in electronic records within our HR system and also in other IT systems, including email.

A copy of your application form and all other personal data collected during the recruitment and selection process will be held as follows:

For **successful applicants** this will be transferred to a personnel file where it will be held securely. You will be given a workforce privacy notice upon appointment which will explain how we will hold and process your data as an employee.

For **unsuccessful applicants**, securely for a period of six months.

Who we Share this Information with and Why

Your information will be shared with school staff with a recruitment responsibility. This will include members of our HR and administrative staff, those responsible for shortlisting and interviewing and managers within the relevant area of work or department. Equality monitoring information is separated from the application form upon receipt and is not shared with those responsible for shortlisting and interviewing.

We do not share information about job applicants with anyone without consent unless the law and our policies allow us to do so.

We will not share your data with third parties unless and until an offer of employment is made to you. At that stage, your data will be shared to fulfil legal requirements, obtain or provide necessary information or because the third party processes data on our behalf. These third parties include:

- The Disclosure and Barring Service in order to undertake a Criminal Records check
- Suppliers and Consultants who provide us with a service such as Occupational Health, Legal or HR Services
- Relevant professional bodies in order to verify your qualifications (such as the Teaching Regulation Agency for teaching posts)

When we appoint third parties to process data on our behalf, the third party is also required to process the data lawfully and fairly and in a manner that ensures appropriate security of the data, using appropriate technical or organisational measures to protect against unauthorised or unlawful processing and accidental loss.

We do not transfer your data to countries outside the European Economic Area.

Requesting access to your Personal Data

Under Data Protection Legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact our Data Protection Officer (details at the beginning of this document).

You also have the right to:

- Restrict processing of your data in certain circumstances
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- Object to the processing of your data where we are relying on our legitimate interests as the lawful basis for processing
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed and:
- Claim compensation for damages caused by a breach of Data Protection Legislation

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further Information

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer (details at the beginning of this document).

Appendix 3: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) emailing compliance@tamat.org.uk

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

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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 before and after the implementation of steps to mitigate the consequences.

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.

The DPO will document the decisions (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 Data Protection Officer's computer.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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 of the school's awareness of the breach. 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.

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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 stored on the Data Protection Officers computer.

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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.

Sensitive information being disclosed via email (including safeguarding records)

- 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/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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 endeavor to obtain 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

If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.

Other types of breach that you might want to consider 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
- Hardcopy reports sent to the wrong pupils or families