Moorlands Learning Trust

DATA PROTECTION POLICY

	Position/Committee	Date
Prepared by	CEO/CFO	February 2021
Approved by	BOARD OF TRUSTEES	February 2021
To be Reviewed	CEO/CFO	Every 2 years unless data protection legislation changes before the 2-year review period February 2023

TOGETHER WE ACHIEVE OUR PERSONAL BEST

Contents

1. Aims....3
2. Legislation and guidance....3
3. Definitions....3
4. The data controller....4
5. Roles and responsibilities....4
6. Data protection principles....5
7. Collecting personal data....6
8. Sharing personal data....6
9. Subject access requests and other rights of individuals....7
10. Parental requests to see the educational record....9
11. Biometric recognition systems....9
12. CCTV....9
13. Photographs and videos....10
14. Data protection by design and default....10
15. Data security and storage of records....11
16. Disposal of records....11
17. Personal data breaches....11
18. Training....12
19. Monitoring arrangements....12
20. Links with other policies....12
Appendix 1: Personal data breach procedure....13-14
Appendix 2: Data protection impact assessment (DPIA) enquiry form 15-16
Appendix 3: How to decide whether you need to do a DPIA 17-19
Appendix 4: Data protection impact assessment template 20-26

1. Aims

Our Trust aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and/or any corresponding or equivalent national laws or regulations which relate to the use of personal data..

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics

	• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Data protection impact assessment (DPIA)	Where a new data processing activity is proposed, an existing data processing activity is changed or a data processing activity is likely to result in a high risk to people's rights and freedoms, a DPIA should be undertaken. (see Appendices 2-4)

4. The data controller

Each Trust school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore, each Trust school is a data controller.

Each Trust school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all our staff** (which includes contractors, temporary and permanent employees). All staff must familiarise themselves with this policy. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal.

5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Moorlands Learning Trust Board (MLTB) and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes.

Full details of the DPO's responsibilities are set out in their job description.

Our current DPO is Alison Kaye:

Email: alison.kaye@moorlandslearningtrust.co.uk.

Address: Ilkley Grammar School, Cowpasture, Road, Ilkley, West Yorkshire, LS29 8TR

5.3 Headteacher

The headteacher in each Trust school acts as the representative of the data controller on a day-to-day basis.

5.4 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 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
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals and whether the completion of a Data Protection Impact Assessment is required (see Appendices 2-4)
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The Trust will comply with the following data protection principles when processing personal information:

- We will process personal information lawfully, fairly and in a transparent manner;
- We will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

- We will only process personal information that is adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- We will keep accurate and, where necessary, up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay
- We will keep personal information for no longer than is necessary for the purposes for which it is processed

We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and again accidental loss, destruction or damage.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also identify a lawful special condition for processing that information, which are set out in the GDPR. If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Records Management standards.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- 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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

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.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address

- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 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 aged 13 and above are generally 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 students at our school may not 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.

9.3 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

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

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.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify inaccurate or incomplete data
- Erase data if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for processing
- Restrict processing of their personal data or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing

- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Academies must provide an annual written report of each registered pupil's progress and attainment in the main subject areas taught to the parents of that registered pupil (except that no report need be provided where the parent has agreed otherwise). Any request for this information will be complied with within 15 days under the regulations.

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) this will be treated as a Subject Access Request (see section 9).

11. Biometric recognition systems

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

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can pay for school dinners in cash at each transaction if they wish.

Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around Trust school sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of 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 Operations Manager. Staff viewing CCTV footage will be asked to record this in the CCTV log. Members of staff are not permitted to view the footage alone.

13. Photographs and videos

As part of our Trust schools activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

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.

See child protection and safeguarding policies for more information on our use of photographs and videos.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data changes. (the DPO will advise on this process). See Appendices 2-4.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

The Trust will use appropriate technical and organisational measures in accordance with the school's policies to keep personal information secure, and in particular to protect against unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage

These may include:

- Making sure that, paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Making sure that, papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Ensuring that, where personal information needs to be taken off site from time to time, staff will take responsibility for its security in line with each school's E-Safety Policy.
- Ensuring that, passwords used to access school computers, laptops and other electronic devices are at least 8 characters long, containing letters and numbers. Staff and students are reminded to change their passwords at regular intervals.
- Making sure that, where possible, encryption software is used to protect all portable devices and removable media, such as laptops, ipads and USB devices.
- Making sure that, staff, students or governors who store personal information on their personal devices, are expected to follow the same security procedures as for school-owned equipment (see our e-safety policy/ICT policy/acceptable use agreement)
- Making sure that, 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 (see section 8)

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

Schools within Moorlands Learning Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

We will report the data breach to the ICO within 72 hours of becoming aware of a breach, if it is likely to result in a risk to the rights and freedoms of individuals.

A data breach may take many different forms, for example:

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

18. Training

All Trustees, Governors and staff are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated as necessary. If any changes are made to data protection legislation in the UK that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full Board of Trustees

20. Links with other policies

This data protection policy is linked to the following policies :

- Freedom of Information policy
- E-Safety policy
- Child Protection & Safeguarding policy
- Staff Code of Conduct policy
- CCTV policy
- Privacy Notices for: School Workforce/Parents/Carers and Students

Appendix 1: 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 immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- 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 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

Actions to minimise the impact of data breaches

We will take the actions set out below 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.

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 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

Appendix 2: Data protection impact assessment (DPIA) enquiry form

Data protection impact assessment (DPIA) enquiry

School staff can use this form to notify their data protection officer (DPO) that they are considering entering into a purchase or contract with a third party that would involve sharing or processing personal data.

DPOs will review such notifications to determine whether or not a data protection impact assessment (DPIA) is needed, and will inform staff of their findings and any recommendations for the DPIA using the form on page 2.

Data protection impact assessment (DPIA) enquiry form

Your name _____

Date form completed _____

Date form sent to data protection officer (DPO) _____

	DPOs: make any comments here
Please give a brief description of the project you are considering *(For example, purchase of online apps, or provision of IT services from an external provider)*	
Will this project involve the processing or sharing of personal data? *(Personal data is defined as any information that could identify individuals, such as names, contact details, user names or ID numbers)* YES / NO	
If 'YES', please give a description of what personal data you will be processing or sharing, and the scale of this processing	
Will this project involve the processing or sharing of sensitive personal data? *(Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometrics, physical or mental health, sexual orientation, or photographs)* YES / NO	
If 'YES', please give a description of what sensitive data you will be processing or sharing, and the scale of this processing	

Please return this form to your DPO.

DPO enquiry findings

For the DPO: complete this form outlining your recommendations and return to the appropriate person(s). Keep a copy for your records. Once the DPIA has been completed and sent to you, update this form and your records. In the event that a DPIA has not been undertaken, record the reasons in your records file.

Having reviewed the information submitted above, I recommend that a DPIA:	
IS required	
IS NOT required	
The reason for this decision is:	
I recommend that the DPIA is carried out by:	

Date findings concluded by DPO: _____

Signed by DPO: _____

Complete once a DPIA has been carried out:

Date DPIA conducted: _____

Copy of DPIA received and filed: YES / NO

File number/link to file: _____

How to decide whether you need to do a DPIA

Schools must conduct a data protection impact assessment (DPIA) where a proposed data processing activity is likely to result in a high risk to people's rights and freedoms. It's up to the school to work out whether the processing meets this description, in consultation with the data protection officer.

This checklist summarises the types of data processing activities to watch out for, based on DPIA guidance from the Information Commissioner's Office (ICO).

Types of processing that schools are more likely to carry out are highlighted in yellow. However, the other types listed here may still apply, depending on the scope of your activities.

Types of processing that ALWAYS require a DPIA under the GDPR

Type of processing	Example
Systemic and extensive profiling which result in a significant effect on the individual	• Credit checks • Mortgage and loan applications • Fraud prevention • Insurance underwriting • Application of artificial intelligence
Large-scale use of sensitive 'special category' data, or data on criminal convictions	• Trade union membership data • Health records • Social care records • Research projects • Political parties membership data • Fraud prevention • Application of artificial intelligence • Dating websites and applications
Monitoring of a publicly accessible area	• Audio/video surveillance of public areas e.g. CCTV • Automatic number plate recognition • Intelligent transport systems • Traffic management systems involving monitoring of vehicle and driver behaviour • Wi-Fi or Bluetooth tracking • Application of artificial intelligence to existing processes
Use of 'new technologies', or new uses of existing technologies	• Artificial intelligence, machine learning and deep learning • Connected and autonomous vehicles • Intelligent transport systems • Smart technologies (including wearable devices)

	• Market research involving neuro-measurement (i.e. emotional response analysis)
Processing that could result in someone being denied a service, where it is based on automatic decision-making or involves the processing of special category data	• Pre-check processes related to contracts • Credit checks • Mortgage or insurance applications
Large-scale profiling of individuals	• Data processed by 'Smart' meters or 'Internet of Things' applications • Hardware and software offering fitness and lifestyle monitoring • Social media networks • Application of artificial intelligence to existing processes
Processing of biometric data	• Facial or thumbprint recognition systems • Building access systems • Identity verification • Access control and identity verification for hardware and applications (e.g. voice recognition, fingerprint and facial recognition)
Processing of genetic data (other than by a health professional to provide someone with medical care)	• Medical diagnosis • DNA testing • Medical research
Matching, combining or comparing personal data obtained from multiple sources	• Direct marketing • Monitoring use or uptake of statutory services or benefits • Fraud prevention • Federated identity assurance services
Invisible processing, where the data about a person has not been obtained from the person themselves	• Selling or purchasing lists of people and their data • Direct marketing • Online tracking by third parties • Online advertising • Data aggregation and data aggregation platforms • Re-use of publicly available data
Tracking an individual's location or behaviour	• Data processing at the workplace • Data processing in the context of home and remote working • Social networks, software applications • Hardware and software offering fitness/lifestyle and health monitoring

	• 'Internet of Things' devices, applications and platforms • Online advertising • Web and cross-device tracking • Data aggregation and data aggregation platforms • Eye tracking • Processing location data of employees • Loyalty schemes • Tracing services • Wealth profiling – identification of high net-worth individuals for direct marketing
Targeting of children or other vulnerable individuals, particularly for marketing purposes, to create a profile of them, or if you intend to offer online services directly to them	• Social networks and applications • Connected toys
Processing that puts people at risk of physical harm if there was a data breach	• Whistleblowing/complaint procedures • Social care records

Types of processing that may not be high risk, but where you should still conduct a DPIA

Your processing activities may not fit the criteria for 'high risk' processing and therefore not legally require a DPIA. However, it's good practice to conduct one whenever you change the way you process data.

Your school should treat data protection as it would any other risk, so conduct DPIAs in the same spirit as you would conduct risk assessments or equality impact assessments.

Forbes Solicitors and Caroline Collins offered these school-specific examples that may not fall into the categories suggested above.

If you're unsure whether your school needs to do a DPIA, err on the side of caution and conduct one.

Changes in school processes	• School mergers or closures • Introduction of remote working • New visitor sign-in systems
New technology purchased or implemented	• ICT hardware or software e.g. your management information system (MIS) • Changes to the ICT infrastructure e.g. moving to the cloud • New devices purchased e.g. tablets for lessons, laptops for staff
Changes to suppliers or service providers	• Switching catering or payroll providers

Appendix 4: Data protection impact assessment template

Data protection impact assessment template

Use this template to conduct a data protection impact assessment (DPIA). The italics are there to prompt you at each step.

Step 1: identify the need for a DPIA	
Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. *Summarise why you identified the need for a DPIA.*	

Step 2: describe the data processing in more detail	
Nature of the data processing	
• *How will you collect, use, store and delete the data?* • *What is the source of the data?* • *Will you be sharing the data with anyone? (You might find it*	

useful to create to a flow diagram) • *What types of processing are involved that can be identified as potentially high risk?*	
Scope	
• *What is the nature of the data, and does it include special category or criminal offence data?* • *How much data will you be collecting and using?* • *How often?* • *How long will you keep it?* • *How many individuals are affected?*	
Context	

• *What is the nature of your relationship with the individuals?* • *Do they include children or other vulnerable groups?* • *How much control will they have over the processing?* • *Would they expect you to use their data in this way?* • *Have there been prior concerns or previous security flaws to do with this type of processing?* • *Is it novel in any way?* • *What is the current state of technology in this area and are there any current issues of public concern that you should factor in?*	
Purposes	
• *What do you want to achieve?* • *What is the intended effect on individuals?* • *What are the benefits of the processing for you, and more broadly?*	

Step 3: consultation process	
Explain how you will consult with relevant stakeholders	
• *When and how will you seek individuals' views on your data processing activity?* • *If you feel it's not appropriate to consult with relevant stakeholders, how can you justify this decision? (Make sure you always record any decision not to consult)* • *If you are consulting, who else within your organisation do you need to involve?* • *Do you need any of your data processors or any other third parties to help with the consultation?* • *Do you plan to consult information security experts, or any other experts?*	

Step 4: assess necessity and proportionality	
Describe how you will make sure you comply with data protection law, and keep the processing proportionate to what you actually need	
• *What is your lawful basis for processing the data in this way?* • *Does the processing actually achieve your purpose?* • *Is there a less intrusive way to achieve the same outcome?* • *How will you ensure the data is good quality and limited to what is necessary?* • *What information will you give individuals about how their data is used?* • *How will you help to support their rights under the GDPR?* • *What measures do you take to ensure processors and other third parties comply with data protection law?* • *How do you safeguard any international transfers of the data?*	

Step 5: identify and assess risks			
Describe the source of risk and the nature of potential impact on individuals *Risks may include:* • *A privacy breach caused by technical issues or human error, where individuals are at risk of discrimination, identity theft, fraud, loss of confidentiality, physical or emotional harm* • *Poor processes or inadequate due diligence leading to non-compliance with the GDPR, resulting in financial or reputational damage to the school*	Likelihood of harm *(remote, possible or probable)*	Severity of harm *(minimal, significant or severe)*	Overall risk *(low, medium or high)*

Step 6: identify measures to reduce risk				
For risks identified as medium or high, identify additional measures you will take to reduce or eliminate the risk				
Risk	**Options to reduce or eliminate risk**	**Effect on risk *(eliminated, reduced or accepted)***	**Residual risk *(low, medium or high)***	**Measure approved *(yes or no)***

Step 7: sign off and record outcomes		
	Name and date	**Actions**
Measures approved by:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual risk, consult the ICO before going ahead with the project*
DPO advice provided:		*DPO should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice:		
DPO advice accepted or overruled by:		
If the advice was overruled, explain why:		
Consultation responses reviewed by:		
If your decision is not the same as individuals' views, explain why, and why you have decided to continue with the processing:		
This DPIA will be kept under review by (name):		
Date:		