PORTSMOUTH AND WINCHESTER DIOCESAN ACADEMIES TRUST

DATA PROTECTION POLICY

Date Agreed: **September 2019**

Review Date: **September 2021**

Signed: _____

Chair of the Governors

Portsmouth and Winchester Diocesan Academies Trust
St Blasius C of E primary Academy
Data Protection Policy

Revision Record

Revision No.	Date Issued	Prepared By	Approved	Comments
1	15th March 2017	NC/AJ	RSC	Changes in advance of GDPR 2018
2	13th April 2018	AJ	RSC	Removal of old Privacy Notice and reference to new notice on page 8.
3	14th May 2018	NC/AJ	RSC	Fully revised to take account of new GDPR regulations
4	September 2019	CW	LGB	Reviewed policy

THE CHURCH OF ENGLAND

THE CHURCH OF ENGLAND

Contents

1. Aims

This policy is set out to ensure that all personal data held on staff, pupils, parents, local governors, Members, Directors, visitors, suppliers and other individuals, is collected, held, processed and shared in accordance with all current and potential future data protection laws.

This policy applies to all personal data, regardless of the format.

2. Legislation and guidance

This policy meets the requirements of the General Data Protection Regulation ("GDPR") and the expected provisions of the Data Protection Act 2018 ("DPA 2018"). 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 also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with the Trust's funding agreement and Articles/Memorandum of Association.

2. 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 e.g. UPN • 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.

3. The data controller

Our Trust processes personal data relating to parents, pupils, staff, local governors, Members, Directors, visitors, suppliers and others, and therefore is a data controller.

A Data Controller is responsible for complying with GDPR principles in an effective manner.

Portsmouth & Winchester Diocesan Academies Trust ("Trust") is registered as a data controller with the Information Commissioner's Office (Registration Number: ZA080425).

4. Roles and responsibilities

This policy applies to all staff employed by our Trust in addition to volunteers working in our organisation, and to external organisations or individuals (Data Processors) that carry out processing of personal data on behalf of Data Controller. This is part of an outsourcing arrangement and governed by a written contract.

4.1 Data Protection Officer

The Trust's 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 at least an annual report of their activities directly to the Trust Board and, where relevant, report to the board their advice and recommendations on data protection issues across the Trust.

The DPO is also the first point of contact for individuals whose data the all academies processes, and for the ICO.

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

Our DPO is Fiona Perkins who is contactable via 02392 899682 or fiona.perkins@portsmouth.anglican.org

4.2 Staff and volunteers

All staff and volunteers are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust 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, , 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
    - If they need help with any contracts or sharing personal data with third parties

5. Data protection principles

The GDPR is based on data protection principles that our Trust and all academies must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

6. Collecting personal data

6.1 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 Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract e.g. employment contracts
- The data needs to be processed so that the Trust can **comply with a legal obligation. For example:**
    - Education (Independent School Standards) Regulations 2014 32(1)(f) - "an annual written report of each registered pupil's progress and attainment…."
    - Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR) 12(1) – "The responsible person must keep a record of any (a) reportable incident...."
    - The Education (Independent School Standards) Regulations 2014 9(c) – "a record is kept of the sanctions imposed upon pupils for serious misbehaviour"
    - The Education (Independent School Standards) Regulations 2014 18(2)(d) – "…an enhanced criminal record certificate is obtained…."
- 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 Trust, as a public funded entity, 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 Trust 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 meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will obtain parental consent via the Acceptable Use agreements (except for matters concerning child protection/safeguarding).

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

As a Multi-Academy Trust, Portsmouth and Winchester Diocesan Academies Trust processes the personal data of its employees, pupils, parents, suppliers, Members, Directors, local governors and visitors so that it may manage educational establishments in accordance with the law.

Employees/Suppliers/Visitors/Members/Directors/Local Governors

The processing of this personal data is necessary for employment/supplier contracts to which each employee/supplier and the Trust are parties. Further employee information is taken in order to support the Trust's health and safety responsibilities, for statistical analysis, to pay commitments on their behalf and to ensure that they are able to undertake the tasks allocated to them. Where necessary, the Trust is also required by law to obtain and document suitability checks (e.g. Disclosure and Barring, Section 128 and qualifications) and record further information in the event of an accident or incident.

Pupils/Parents

The Trust and each academy processes the personal information of its pupils and their parents, to record their progress for statistical purposes and so that at least an annual written report may be provided as required by law. For a child's protection, medical conditions and any other risk of harm will be documented. To meet with regulations, the Trust and academy may note behavioural standards and to record further information in the event of an accident or incident.

Annually, the academy will contact each child/parent to gain permission to obtain and/or publish images when it is appropriate e.g. sports event. If the Trust does not receive a reply, it will consider no agreement has been given. Parents may also withdraw this consent at any point.

6.2 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, in documents such as the Privacy Notice.

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 Trust's retention policy.

7. 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, except in the case where it could compromise the protection and safeguarding of a child
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and local authority or 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/child protection 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 pupils 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.

8. Subject access requests and other rights of individuals

8.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust 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
- Existence of any rights e.g. the right to request rectification
- The right to lodge a complaint with the Information Commissioner

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

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

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

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

8.3 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.

8.4 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, erase or 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 academy staff receive such a request, they must immediately forward it to the DPO.

9. Parental requests to see the educational record

There is no automatic right of access in an academy setting, for parental access to educational records. However, as we wish to work in partnership with our parents, our Trust has determined that we will provide a person/persons with parental responsibility to free access to their child's record (which contains most information about a pupil) within 15 school days of receipt of a written request. However, as stated in Sections 7 and 8, information will not be shared where it is considered that the protection or a child or legal proceedings may be compromised.

Those with parental responsibility also have a right to receive "an annual written report of each registered pupil's progress and attainment…." as per the Education (Independent School Standards) Regulations 2014 32(1)(f)

10. CCTV

We use CCTV in various locations around academy sites to ensure that they remain 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 Fiona Perkins, Data Protection Officer.

11. Photographs and videos

As part of our Trust and individual academy activities, we may take photographs and record images of individuals within our setting.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials as part of the admissions process. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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 the academy on notice boards and in academy or Trust magazines, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on the Trust, individual academy websites or social media platforms e.g. Twitter, Facebook

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.

Please see our Trust policies http://www.pwdat.org/policies-alphabetical-order/ and pupil admissions forms for more information on our use of photographs and videos.

12. 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 Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- 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 Trust, academy 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

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- 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
- 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
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils, local governors, Members and Directors who store personal information on their personal devices are expected to follow the same security procedures as for Trust owned equipment (see our Acceptable Use Policies)
- 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)

14. 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. Please see the Trust's Data Retention Policy for further details: http://www.pwdat.org/policies-alphabetical-order/

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

15. Personal data breaches

The Trust together with each academy, 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.

When appropriate, we will report the data breach to the ICO without undue delay and where feasible, not later than 72 hours after becoming aware of it. Such breaches in an academy context may include, but are not limited to:

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

We will also report the breach to the data subjects where there is a high risk to an individual/s rights and freedoms. Each incident will assessed individually.

16. Training

All staff and local governors have been provided with data protection training. It is the responsibility of each academy to ensure that this is included as part of the induction programme for all new staff who join the Trust and for refresher training as required.

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

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary, as required. This policy will be formally reviewed by the Trust at least every two years.

18. Email out of office arrangements

When on leave, all academy and central staff must set their email out of office to advise that all Freedom of Information requests, Subject Access Requests and Breach notifications are to be directed to the Data Protection Officer, Mrs Fiona Perkins and should provide her contact email address. Fiona should redirect her emails to other members of the central team during her periods of annual leave likewise.

19. Links with other policies

This data protection policy is linked to our:

- Acceptable Use Policies
- Child Protection Policy
- Safeguarding policy
- Data Retention Policy
- Freedom of Information Supplementary Information for Parents
- ICO Freedom of Information Guide
- Privacy notices
- Risk management policy
- Single Central Record Guidance

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 Trust 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 all interested parties including the Portsmouth & Winchester Diocesan Academies Trust Board
- 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 will be stored on the Trust's risk register. 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 nature of the 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 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 Trusts risk register
- The DPO and all interested parties 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 results will be presented to the Trust board for review and to make any requisite determinations in accordance with respective policies.

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 relevant IT manager/company 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: Lawful Processing Conditions

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose. – May be withdrawn by the data subject at any time. Used for images (other than CCTV) and other optional personal data, but not mandatory personal data. Examples: Pupils' images (not CCTV or bodycams videos) and optional employee data

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. - This has been used for employee, supplier and any other individuals who are party to a contractual arrangement with the Trust.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations). The list of Acts that justify the processing of data are:-

- Education (Independent School Standards) Regulations 2014 32(1)(f) - "an annual written report of each registered pupil's progress and attainment…." - Pupils
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR) 12(1) – "The responsible person must keep a record of any (a) reportable incident...." - Everyone
- The Education (Independent School Standards) Regulations 2014 9(c) – "a record is kept of the sanctions imposed upon pupils for serious misbehaviour" - Pupils
- The Education (Independent School Standards) Regulations 2014 18(2)(d) – "…an enhanced criminal record certificate is obtained…." - Employees/Members/Directors/Local Governors

(d) Vital interests: the processing is necessary to protect someone's life. Used in relation to child safeguarding Children – safeguarding

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. – Academies as defined under the Academies Act 2010 are designated public authorities in relation to Freedom of Information Act 2000 enquires. There is no separate definition of a public authority in the GDPR. Therefore this is the primary lawful condition

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.) - Please see explanation under (e) – An academy trust is considered to a public authority and thus this lawful condition is not available to Trust as a justification for collecting personal data.

Special Category Data

If processing special category data:-

race;

ethnic origin;

politics;

religion;

trade union membership;

genetics;

biometrics (where used for ID purposes);

health;

sex life; or

sexual orientation.

then:-

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in

so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

Applies to Employees and Members/Directors/Local Governors

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

Applies to pupils

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

Applies to Employees/Children

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Applies to Employees/Children

Criminal Offence Data

If processing criminal data then the following applies:-

“Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.”

Applies to Employees and Members/Directors/Local Governors