St Mary's Academy Trust

Data Protection Policy

Date agreed by HR Committee: 9th September 2022

Date to be reviewed: 9th September 2023

1. Aims

1.1 As the data controller, the Trust comply with our obligations under UK GDPR and DPA. The Trust is committed to being concise, clear, and transparent about how they obtain and use personal information and will ensure data subjects are aware of their rights under the legislation.

1.2 It is our aim to ensure every staff member and volunteer has a general understanding of GDPR law and understand how it could affect their decisions to make an informed judgement about how information is gathered, used, and ultimately deleted. Furthermore, every staff member and volunteer must read, understand, and comply with this policy.

2. Legislation and Guidance

2.1 This policy fulfils the requirements of the UK GDPR law and the DPA 2018; it is based on guidance published by the Information Commissioner's Office [ICO] and the ICO's code of practice for subject access requests.

2.2 For schools who use CCTV, this policy reflects the ICO's code of practice for the use of surveillance cameras and personal information.

2.3 The policy is in line with the ICO Children's Code; in respect of this, you must follow your school's action plan to ensure you meet the 15 standards which are a legal requirement (speak with your Headteacher for further information.

2.4 This policy complies with our funding agreement and articles of association.

3. Definitions

Terms	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. Where the above identifying data is present, this could include, for example: • Children's achievement and progress • Parents Banking information

	• Safeguarding needs • Financial status • Parental status, e.g.: LAC **A full list of types of all data, including personal data can be found in the Retention Schedule.**
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.

4. The Data Controller

4.1 The Trust processes personal data relating to parents, pupils, staff, governors, visitors, and others, and therefore is a data controller.

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

5. Roles and Responsibilities

5.1 This policy applies to all staff, governors and volunteers employed by the Trust, and to external organisations or individuals working on our behalf. Non-compliance by any member of staff will be treated as misconduct and dealt with via the disciplinary procedure. Please note this could be categorised as gross misconduct and may result in dismissal. Non-Compliance by external organisations or individuals working on our behalf may result in the termination of the SLA/Contract.

5.2 **Governing Board**

5.2.1 The governing board has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations. The Trust means all employees of the Trust.

5.2.2 The Governing bodies and proprietors should ensure staff have due regard to the data protection principles, which allows them to share personal information, as provided in the DPA 2018 and the UK GDPR.

5.2.3 The Governing bodies and proprietors should ensure that staff who need to share 'special category personal data' are aware that the DPA 2018 contains 'safeguarding of children and individuals at risk' as a processing condition that allows practitioners to share information.

5.3 **Data Protection Officer**

5.3.1 The Data Protection Officer [DPO] is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and coordinating the development of related policies and guidelines where applicable.

5.3.2 They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

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

5.3.4 Our DPO is Jo Hudson and is contactable via the Trust Office on 01226 282721.

5.4 **Headteacher**

5.4.1 Headteachers act as the representatives of the data controller on a day-to-day basis.

5.5 **All Staff**

5.5.1 Staff are responsible for collecting, storing, and processing any personal data in accordance with this policy, and informing the school of any changes to their own personal data, such as a change of address. Staff should contact 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 they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, use 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

6. Data Protection Principles

6.1 The UK GDPR is based on data protection principles that we must comply with.

6.2 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, or processed in a way that ensures it is appropriately secure.

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

7. Collecting Personal Data

7.1 **Lawfulness, Fairness and Transparency**

7.1.1 You must only process personal data where you have one of 6 'lawful bases' (legal reasons) to do so under data protection law.

7.1.2 The lawful bases are:

- 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

7.2 For special categories of personal data, you must also meet one of the special category conditions for processing which are set out in the UK GDPR and DPA 2018.

7.3 Where you offer online services to pupils, such as classroom apps, and you intend to rely on consent as a basis for processing, you must get parental consent (except for online counselling and preventive services).

7.4 Where a new process is introduced involving the processing/storing of personal data you should inform your manager so that an assessment can be carried out as to which ground we can process the data, and whether a data impact assessment is required. This will be via a discussion with the DPO.

7.5 **Limitation, Minimisation and Accuracy**

7.5.1 You must only collect personal data for specified, explicit, and legitimate reasons and explain these reasons to the individuals when you first collect their data.

7.5.2 If you 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 to do their jobs.

7.5.3 When you no longer need the personal data you hold, you must ensure it is deleted or anonymised. This must be done in accordance with the Trust's retention schedule.

8. Sharing Personal Data

8.1 You should 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
- You need to liaise with other agencies; however, if this is necessary, you will need to seek consent before doing so
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils, for example, IT companies. When doing this, you must:

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

- Contact the DPO to 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
- Where data sharing is required for the above purposes, approval must be given by the DPO where a new third party is used and/or for ad-hoc requests for data from third parties outside any usual SLA's.

8.2 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, if personal data is sufficiently anonymised, or consent has been provided

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

8.4 If you are required to transfer personal data to a country or territory outside the European Economic Area, you must do so in accordance with data protection law.

8.5 **Restrictions**

8.5.1 Schools should not (under the UK GDPR as supplemented by the DPA 2018) provide pupils' education data where the serious harm test under that legislation is met. For example, in a situation where a child is a refugee, this could mean that schools can withhold education data under the UK GDPR, and they should do so where the serious harm is testified. Please contact the DPO to discuss this on a case by case basis.

9. Subject Access Requests and Other Rights of Individuals

9.1 **Subject Access Requests**

9.1.1 Individuals have a right to make a 'subject access request' to gain access to personal information that we hold about them, including, 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, and whether any automated decision-making is being applied to

their data, and what the significance and consequences of this might be for the individual.

9.1.2 Subject access requests should be submitted in writing, either by letter or email to the DPO. They should include the name of the individual, correspondence address, a contact number and email address, and details of the information requested.

9.1.3 If you receive a subject access request, you must immediately forward it to the DPO.

9.2 **Children and Subject Access Requests**

9.2.1 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.

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

9.3 **Responding to Subject Access Requests**

9.3.1 When responding to requests, you:

- 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

You must 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

9.3.2 If the request is unfounded or excessive, you may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. Please discuss this with the DPO.

9.3.3 A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

9.3.4 If the DPO confirms that you can refuse a request, you must 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**

9.4.1 In addition to the right to make a subject access request (see above), and to receive information when you 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 based on 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)

10. Parental Requests to See Educational Record

10.1 As a multi academy trust there is no automatic parental right of access to the education records we hold however we will consider requests received and respond in a timely manner. We will only provide information to a parent about their child and not any comparison information against other pupils. If the information required is excessive, we will reserve the right to implement a charge. Requests must be made in writing to their child's headteacher.

11. CCTV

11.1 Schools using CCTV on site to ensure it remains safe will adhere to the ICO's code of practice for the use of CCTV and the Trusts CCTV policy.

11.2 We do not need to ask individuals' permission to use CCTV, but you will need to make it clear where individuals are being recorded. Security cameras must be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

11.3 Any enquiries about the operation of the CCTV system should be directed to Callum Cook on 01226 749164.

12. Photographs and Videos

12.1 As part of our school activities, you may take photographs and record images of individuals within our school, however, you will need to obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing, and promotional materials (see suite of consent forms on the Trust Shared drive). You will also need to clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

12.2 Uses of photographs and/or videos 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

12.3 Consent can be refused or withdrawn at any time. If consent is withdrawn, you will need to delete the photographs or videos and not distribute it further.

12.4 When using photographs and videos in this way you must not accompany them with any other personal information about the child, to ensure they cannot be identified.

12.5 For further information, please refer to our Child Protection and Safeguarding policy and our Acceptable Use policy.

13. Personal Accounts

13.1 For the purposes of disciplinary, we reserve the right to monitor personal accounts through access and viewing them in instances of alleged misconduct; notice will be given of our intention to access this data.

14. Data Protection by Design and Default

14.1 The Trust has put measures in place to show that data protection is integrated into all our data processing activities, including:

- Identifying a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Completing data impact assessments where the school'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 providing training resources to staff, governors and volunteers including 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), and 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. Responsibilities

15.1 **All staff, governors and volunteers must ensure that** they 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.

15.2 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 are not left unattended in an unsecure office, classroom, or staffroom.
- Signing in books for both visitors and staff are kept in a secure location and not left unattended in a reception area.
- Notices are clearly displayed by electronic signing in equipment
- Notices are clearly displayed for the use of CCTV.
- When a laptop/desktop computer is left unattended the screen is locked by pressing the windows key and L. This is in all cases regardless of the length of time the equipment is to be left unattended.
- 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).
- Personal data must not be saved to the desktop of a device.
- Where personal information needs to be taken off site, staff sign it in and out from the school office. Personal data must never be left in an unattended vehicle in any circumstances, if transporting personal data, the route must be direct.
- Conversations in relation to personal data are held in a secure and confidential environment.
- All school e-mails are avoided where possible to share personal data.

16. Data Security

- 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, 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 and Acceptable Use Policy).
- Sharing personal information with anyone other than a Trust employee or governor must be approved by the Headteacher unless it is for the purpose of a life-saving situation i.e., sharing information with a paramedic or other medical professional.
- Social media platforms are strictly prohibited for sharing any form of personal data. This includes Whats App groups.
- You must follow the latest retention schedule guidelines at all times and the records you keep must reflect the information contained in this document.

16.1 For staff who are remote working (including homeworking), point 15 must be followed and in addition: -

- Ensure any hard copies of documents are destroyed using the School/Business Centres' secure destroying of confidential waste procedures and not in a household bin.
- Ensure documents containing personal data are stored securely and privately and return such documents to the workplace as soon as you can do so.
- Ensure adequate privacy away from friends and family when discussing personal data.
- Ensure your screen is not visible by friends or family or any other person if working near a window.

17. Disposal of Records

17.1 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 you cannot or do not need to rectify or update it.

17.2 For example, you must use an external confidential shredding service for paper-based records and overwrite or delete electronic files. You must obtain sufficient guarantees from any third party used that they comply with data protection law.

18. Personal Data Breaches

18.1 The school will make all reasonable endeavours to ensure that there are no personal data breaches.

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

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

- A non-anonymised dataset being published on the school 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 school laptop containing non-encrypted personal data about pupils.

19. Training

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

19.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary. This training is mandatory and failure to complete required training may result in disciplinary action being taken.

20. Monitoring Arrangements

20.1 The DPO is responsible for monitoring and reviewing this policy.

20.2 This policy will be reviewed and updated if necessary if any changes are made to the bill that affect the Trusts practice.

21. Data Impact Assessment

21.1 At all stages of this procedure data obtained will be used only for the purpose for which it is intended and will be stored securely with restricted access to those involved in the process. Following the process data will be stored on the electronic personal file for the duration of the employees' employment with the Trust and for 6 years thereafter. The data will be destroyed at this time using a confidential shredding service.

22. Equality Impact Assessment

22.1 This policy has been impacted assessed by the HR Committee, if on reading this policy you feel there are any equality and diversity issues, please contact HR who will if necessary, ensure the policy is reviewed.

Induction

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance 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

Where necessary: -

- 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 Financial loss
    - Changing codes, for example door key codes
    - 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 in the secure electronic HR folder
- 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: o Facts and cause o Effects o 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 in the secure electronic HR folder
- 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

Induction

Appendix 2: Actions to Minimise the Impact of Data Breaches

Examples of actions you will need to take to mitigate the impact of different types of data breach are detailed below, 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.

A) Sensitive information being disclosed via email (including safeguarding records)

- Inform the DPO
- 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 headteacher to instruct ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will ask the headteacher 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 ask the headteacher to 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 along with IT 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

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

- Inform the DPO
- Plan information reviewed by governors prior to web posting
- Remove data
- Discuss with parent that it was shared and removed with reassurance about intervention purpose
- Share the positive forecast impact of the intervention
- If appropriate the DPO will report to the ICO

C) Non-anonymised pupil exam results or staff pay information being shared with governors • Inform the DPO

- If sent by e-mail retract the e-mail where possible
- Inform the governors and ask that they delete the information immediately
- Interview with the member of staff who shared the information – determine course of action i.e. changes to systems/disciplinary
- Letter to inform of breach to those affected and explain the remedial action put in place
- If appropriate the DPO will report to the ICO

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

- Upon theft discovery User account password reset and inform DPO
- Interview with the staff member who lost/had stolen the device and the nature/quantity of the data stored on the laptop and ensure 101 crime number recorded as appropriate.
- Is the threat ongoing for example if the data itself has been stolen/hacked. (Consider insurance and asset management).
- Letter to inform of breach sent to those affected and the remedial action put in place.
- A record of the results and outcome even if rapidly resolved to be shared with the DPO.
- Incident review with DPO and policy/system update if required
- If appropriate the DPO will report to the ICO

I have the read the Data Protection Policy and agree to adhere to this. I understand that failure to do so may result in disciplinary action.

Name: ……
Place of Work: ……
Signed: ……
Date: ……

(A signed copy will be retained on your secure personal file I accordance with the Trust's Retention Schedule)