Data Protection Policy

Author:	Lead Governance Professional
Approver:	Finance & Resources Committee
Date:	17th June 2025
Next review:	June 2028 unless there are earlier statutory or guidance changes
Category of policy:	Trust Board

Changes history

Version:	Date:	Amended by:	Substantive changes:	Purpose:
1			New trust policy	

Contents

---

1. Aims

The Agape Multi Academy Trust (The Trust) aims to ensure that all personal data collected about staff, pupils, parents and carers, families, members, trustees, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

Where we refer to The Trust this includes all schools within our trust.

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:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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

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, living 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.

TERM	DEFINITION
Data controller	A person or organisation that determines the purposes and the means of processing 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

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

The Trust is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust Board

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

5.2 Data Protection Officers (DPOs)

Our Data Protection Officers (DPOs) are 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 Trust Board and, where relevant, report to the board their advice and recommendations on trust data protection issues.

Our DPOs are also the first point of contact for individuals whose data the Trust processes, and for the ICO.

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

Our DPOs are:

For Altwood School: Satswana Services, Suite G12 Ferneberga House, Alexandra Road, Farnborough, Hampshire, GU14 6DQ. Email: admin@satswana.com Telephone: 01252 759177. Enquiries and requests should be sent in the first instance to Mrs N. Walker, Headteacher's PA, Altwood School, Altwood Road, Maidenhead, Berkshire, SL6 4PN nwalker@altwoodschool.co.uk

For The Piggott School: Mr David Thatcher, The Piggott School, Twyford Road, Wargrave, Berkshire, RG10 8DS. Email: dpo@piggottschool.org Telephone: 01189 402357

For The Agape Multi Academy Trust: Mrs Rebecca Marr Agape Multi Academy Trust, C/O The Piggott School, Twyford Road, Wargrave, Berkshire, RG10 8DS. Email: MarrR@agapetrust.co.uk Telephone: 01189 402357

5.3 CEO & Headteachers

Our CEO (for the Agape Trust) and our Headteachers (for their respective 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 Trust of any changes to their personal data, such as a change of address
- Contacting the relevant 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 UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals including collecting or processing new data
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on data protection principles that our school 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 school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 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 school to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the Trust (where the processing is not for any tasks the Trust performs as a public authority) 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 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual

- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to child protection or preventative/counselling services offered directly to a child.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor 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

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

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 internationally, we will do so in accordance with UK 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 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form they must immediately forward it to the relevant 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 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.

Children aged 12 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 pupils 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 (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge subject to the point marked * below.
- 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
- May ask the individual to specify the information the request is in relation to in the event a large amount of information is being processed about them

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision. *

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

We will respond to a SAR either by sending the information electronically or in paper copies.

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, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)

- 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 relevant DPO. If staff receive such a request, they must immediately forward it to the DPO.

Where the data in question has been disclosed to third parties the Trust will advise the third parties of any rectification, erasure or restriction of processing where possible.

Requests for rectification, erasure or restriction of processing will be responded to in one month; this will be extended by 2 months where the request is complex.

10. Parental requests to see the educational record

In academies there is no legal right for parents, or those with parental responsibility, to have access to their child's educational record (which includes most information about a pupil). We will however provide this to parents, or those with parental responsibility, within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, we may charge a fee to cover the cost of supplying it.

We will provide access or a copy of the educational record as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils 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 Trust will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils 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 pupils. For example, pupils can pay for school dinners by entering a 4 digit pin (at The Piggott School – Secondary Phase) at each transaction if they wish.

Parents/carers and pupils can 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 Trust will delete any relevant data already captured.

12. Photographs and videos

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

For the Primary Schools/Phases in our Trust we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

For the Secondary Schools/Phases in our Trust we will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the Trust takes photographs and videos, 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
- Internal assessment of student learning and progress across the curriculum areas

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 unless it is in practical subjects where we are capturing performance.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, The Trust will treat this as a data breach and will follow the personal data breach procedure outlined in appendix 1.

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 suitably qualified DPOs, 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 data protection 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 (DPOs 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Trust and DPO's 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

15. 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, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff should take extra care to follow the same procedures for security. The person taking the information from the trust premises accepts full responsibility for the security of the data
- Digital data is coded, encrypted or password protected, both on a local hard drive and on a network drive that is backed up off site

- Memory sticks will not be used to hold personal information. All data should be stored on the school network drive.
- Staff, trustees and governors will not use their personal email for school purposes
- All members of staff, trustees and governors are provided with their own secure log on and password
- All staff will adhere fully to their school's online safety/acceptable use of IT policies
- Staff, trustees and governors must only access and use personal data that they are authorised to access and use and which is needed for a specific task within their role
- All staff involved in processing data will
    - Read and understand this policy
    - Use strong passwords and two-step authentication
    - Encrypt all portable devices if they contain personal data
    - Not download personal data onto personally owned devices unless absolutely necessary. In such cases the personal data should be deleted from the personal device as soon as is practicable after use
- Before sharing data, all staff members, members, trustees and governors will ensure that they are allowed to share it, adequate security is in place to protect it and who will receive the data has been outlined in a privacy notice
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times
- The physical security of the trust's buildings and storage systems and access to them is reviewed on an ongoing basis. If any extra risk in burglary/theft is identified extra measures to secure data will be put in place
- Circular emails to parents must be sent via school Comms/SIMS in touch or use the blind copy function on email systems so email addresses are not disclosed to other recipients
- 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 or incinerate 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.

The Trust maintains an archive of historical interest. This means that some data is used for research purposes (and that is compatible with the purposes for which the data was originally collected) may be kept indefinitely if the relevant conditions apply. These are: that the data is not used to support decisions about individuals, and that substantial damage or substantial distress is not likely to be caused to any data subject. Personal data can be selected for permanent preservation, and stored, if these two conditions apply, on condition that the other data protection principles are complied with.

17. Personal data breaches

The 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.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in our context may include, but are not limited to:

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

18. Training

All staff, trustees and governors 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 Trust's processes make it necessary.

19. Monitoring arrangements

The DPOs are responsible for monitoring and reviewing this policy.

This policy will be reviewed biennially and approved by the Finance and Resources Committee of the Trust Board.

20. Equality Act 2010

We have carefully considered and analysed the impact of this policy on equality and the possible implications for people with protected characteristics as part of our commitment to meet the public sector equality duty requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations. If you feel you have or may be negatively impacted by this policy please contact us.

21. Links with other policies

This data protection policy is linked to our:

- Individual school's Acceptable use policy/E-Security
- Individual school's Bring your own device policy
- Individual school's CCTV policy
- Child protection & safeguarding policy
- Freedom of information policy
- Individual school's Online safety
- Privacy notices

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by filling out a reporting form (see Appendix 2) and emailing it to the relevant DPO. The data breach form is available:

  At Altwood School: on the S:\drive

  At The Piggott School: on the staff shared resources in the school policies and procedures folder School Policies and Procedures

  The Trust encourages near misses to be reported via the data breach form so that the relevant DPO can identify any areas for improvement and adapt processes and procedures as necessary.

- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
  - Staff, members, trustees and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
  - If a breach has occurred or it is considered to be likely that is the case, the relevant DPO will alert the Headteacher and the Chair of the Local Governing Body (if the breach relates to information held by a school) or the CEO and Chair of The Trust Board (if the information is held by the Trust Central Team).
  - The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
  - The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
  - The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
  - The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored securely in an electronic folder held by the relevant DPO. The DPO will also document any preventative steps taken including training.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the Trust's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the Trust is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored electronically on the respective school's or Trust's computer system.
- The DPO and Headteacher (and in exceptional circumstances the CEO) 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 respective DPO and Headteacher and CEO and DPO for the Agape Trust will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT Department to attempt to recall it from external recipients and remove it from the Trust's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
    - The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
    - If safeguarding information is compromised, the DPO will inform the respective designated safeguarding lead and discuss whether the Trust should inform, nay, or all, of its 3 local safeguarding partners
    - If the breach contains any entry codes or passwords then these codes/passwords will be changed immediately

Appendix 2: Form to complete after a data breach

Data Breach Form

This form should be used to log any data breaches.

Section 1

1. Email:

2. Your Name:

3. School name where the breach occurred:

Section 2- Data Breach Details

4. When was the data breach discovered? (DD/MM/YYYY and time)

5. When did the data breach occur? (DD/MM/YYYY and time)

6. Please describe what happened.

7. Have any preventative steps been taken prior to reporting the data breach? Please provide as much detail as possible if steps have already been taken to minimise the date breach.

8. Categories of personal data included in the breach. Please tick all that apply.
   - Data revealing racial or ethnic origin
   - Political opinions
   - Religious or philosophical beliefs
   - Trade union membership
   - Sex life data
   - Sexual orientation data
   - Gender reassignment data
   - Health data
   - Basic personal identifiers, e.g. name, contact details
   - Identification data, e.g. usernames and passwords
   - Economic and financial data, e.g. credit card numbers, bank details
   - Official documents, e.g. driving licence
   - Location data, e.g. coordinates
   - Genetic or biometric data
   - Criminal convictions or offences
   - Other

9. How many data subjects could be affected? Please remembers if the breach is related to a pupil, they are classed as a data subject.

10. How many personal records are affected by the data breach?

11. Categories of data subjects that could be affected?
    - Employees
    - Students
    - Parents
    - Third Party Providers
    - Local Authority

12. Potential consequences of the breach

13. Is the personal data breach likely to result in a high risk to data subjects?
    - Yes
    - No
    - Not yet known

14. Was the breach caused by a cyber incident?
    - Yes
    - No
    - Maybe

Section 3 – Cyber Incidents.

This section is to be completed where data breaches are related to cyber incidents.

15. Has the system integrity been affected? If yes, please specify what.

16. What is the potential impact to the organisation? Please provide as much information as possible.

17. If the system has been recovered, what was the recovery time?