POLICY:
Data Protection

Review

Approved by:	Board of Trustee	**Date:**	December 2024
Last Review Date:	December 2024	**Next Review Date:**	December 2025

Responsibilities

School Senior Staff	Implementation of policy at school level
Governors	Check school compliance with policy and report breaches or concerns to Trustees
Trustees	Review and approve the policy

Material Changes to the Policy Since the Last Review

Section:	No material changes

Contents

1. Aims

The Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors, and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation & Guidance

This policy meets the requirements of GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO).

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

In addition, this policy complies with Regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right to access their child's educational record.

3. Definitions

Term	Definition
Personal data	Information relating to an individual who can be identified or who is identifiable directly from the information or who can be indirectly identified from that information in combination with other information, such as: • name • identification number • online identifier, e.g. user name.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, such as: • racial or ethnic origin • religious or philosophical beliefs • biometric data (where used for identification purposes, eg fingerprints) • health – physical and mental • pupil premium status • special educational needs.
Processing	Any operation or set of operations which is performed on personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disseminating, erasing or destroying. This can be either automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation which determines the purposes and means of the processing of personal data.
Data processor	A person or organisation which processes personal data on behalf of the controller.
The Trust	Equinox Learning Trust, including any of its member academies.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4. The Data Controller

The Trust processes personal data relating to parents, pupils, staff, governors, and visitors and is, therefore a data controller. The Trust is registered as a data controller with the ICO and will renew its registration annually or as otherwise legally required.

5. Roles & Responsibilities

This policy applies to all staff employed by the Trust and 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's Board of Trustees (through its Local Governing Committees) ensures that our organisation complies with all relevant data protection obligations.

5.2. Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law and developing related policies and guidelines where applicable. The DPO is also the first point of contact for individuals whose data the Trust processes and for the ICO.

5.3. CEO & Headteachers

The CEO and Headteachers act as the representatives 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 DPO in the following circumstances:
  - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - if they have any concerns that this policy is not being followed
  - if they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - if there has been a data breach
  - whenever they are engaging in a new activity which may affect the privacy rights of individuals
  - if they need help with contracts or sharing personal data with third parties.

6. Data Protection Principles

The GDPR is based on data protection principles that our Trust 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 in relation to the purposes for which it is processed
- accurate and, where necessary, kept up-to-date
- kept for no longer than is required for the purposes for which it is processed
- processed in a way which ensures it is appropriately secure.

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

7. Collecting Personal Data

7.1. Lawfulness, Fairness, & Transparency

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

- the data subject (or their parent/carer when appropriate in the case of a pupil) has given **consent** freely to the processing of their personal data
- 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
- 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 data subject, e.g. 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** 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 data subject's rights and freedoms are not overridden).

For special categories of personal data, we will also meet one of the special category conditions for processing set out in the GDPR and DPA 2018.

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

7.2. Limitation, Minimisation & Accuracy

The Trust will only collect personal data for specified, explicit and legitimate reasons. When we first collect their data, we will explain these reasons to data subjects. If we want to use personal data for reasons other than those given when we first collected it, we will inform those concerned and seek specific consent for the new purpose.

Staff must only process personal data where it is necessary for them to perform their roles.

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 Data Retention Policy.

8. Sharing Personal Data

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

- there is an issue with a pupil or parent/carer which puts the safety of our staff at risk
- there is a safeguarding situation
- 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 pupils. When doing this, we will:
  - only appoint suppliers and contractors who 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.

The Trust will also share personal data with law enforcement and government bodies where it is legally required to do so, including:

- the prevention or detection of crime and/or fraud
- the apprehension or prosecution of offenders
- in connection with legal proceedings
- where the disclosure is required to satisfy our safeguarding obligations
- research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

We may also share personal data with emergency services and local authorities to help them respond to an emergency that affects any of our pupils or staff. Where personal data is transferred to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject Access Requests & Other Rights of Individuals

9.1. Subject Access Requests

Data subjects have the right to obtain from the Trust confirmation that their personal data is being processed, and where this is the case, access to that personal data and the following information:

- confirmation that the personal data is being processed
- the categories of personal data concerned
- with whom the data has been, or will be, shared
- the length of time for which the data will be stored, or if this is not possible, the criteria used to determine this period

- the existence of the right to request the Trust to rectify or erase personal data or restrict processing of personal data or object to such processing
- the source of the data, where it has not been obtained directly from the individual
- whether any automated decision-making is being applied to their data.

Subject access requests may be made verbally or in writing. If staff receive a subject access request, they must immediately let the DPO, CEO or their Headteacher know.

9.2. Children & Subject Access Requests

Personal data about a child belongs to that child, not the child's parents or carers. For a parent or carer to make a subject access request concerning 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 considered mature enough to understand the rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at the Trust's primary academies 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 over are generally considered 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 Kennet School may only be granted with 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, the Trust:

- may ask the individual to provide two forms of identification
- may contact the individual via telephone to confirm the request was made
- will respond without delay and within one month of the receipt of the request
- will provide the information free of charge
- may tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary.

The GDPR and DPA 2018 set out some exemptions that will be considered on a case-by-case basis when the Trust responds to a subject access request. Where the Trust believes that an exemption applies, it will justify and document its reasons for relying on an exemption. Examples of exemptions which might apply:

- **protection of the rights of others** - revealing information about another individual who can be identified from that information, except if the other individual has consented to the disclosure or it is reasonable to comply with the request without that individual's consent (i.e. where the information is neither contentious nor sensitive)
- **child abuse data** - revealing that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- **education data – serious harm** – revealing information might cause serious harm to the physical or mental health of any individual (known as the 'serious harm test' for education data)
- **education data – processed by a court** – education data supplied to a court in the course of proceedings, and these proceedings are subject to certain specific statutory rules which allow the education data to be withheld from the individual to whom it relates
- **confidential references** either given or received by the Trust
- **exam scripts and marks** - personal data (answers) recorded by individuals during an exam.

If the request is manifestly unfounded or excessive, the Trust may refuse to act on it or charge a reasonable fee that considers administrative costs. A request will be deemed unfounded or excessive if it is repetitive or overlaps with other requests. Where such a request is refused, we will inform the individual about the reasons for such action and advise them of their right to complain to the ICO.

9.4. Other data protection rights of the individual

In addition to the right to make a subject access request and to receive information when the Trust is collecting their data about how it is used and processed, individuals also have the right to:

- withdraw their consent to processing at any time

- ask us to rectify, erase or restrict the processing of their personal data or object to the processing thereof (in certain circumstances)
- prevent the use of their personal data for direct marketing
- challenge processing, which has been justified based on public interest
- object to decisions based solely on automated decision making or profiling (decision making or profiling (decisions taken with no human involvement, which might negatively affect them)
- prevent processing which is likely to cause damage or distress
- be notified of a data breach in certain circumstances
- make a complaint to the ICO
- ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances).

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

10. Parental Requests to See the Educational Record

Parents, or those with parental responsibility, can request access to their child's educational record (which includes most information about a pupil). Such requests should be made directly to the Trust's CEO.

11. CCTV

We use CCTV in various locations around the Trust's sites to ensure it remains a safe environment for its pupils, staff, parents and visitors. 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 signs explaining that CCTV is in use. CCTV policies can be found on the local school's websites where relevant.

12. Photographs & Videos

Taking photographs and video recordings of the pupils at our schools is a key part of life in the Trust. Where consent is required, we will seek this from pupils and also parents/carers where the pupil is under 16. Parental consent is not required for pupils over 16 years of age. Consent will be sought for more public uses of photographs and videos, including, but not limited to, school websites, newsletters, prospectuses, local newspapers, promotional materials, and social media. Consent is not required in certain circumstances, such as for teaching and welfare purposes.

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.

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 photographs or videos with other pupils are not shared publicly on social media for safeguarding reasons.

13. Data Protection by Design & Default

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

- appointing a DPO and ensuring they have the necessary resources to fulfil their duties
- only processing personal data which is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law;
- completing privacy impact assessments where the Trust's processing of personal data presents a high risk to the rights and freedoms of individuals and when introducing new technologies
- integrating data protection into internal documents, including this policy, any related policy and privacy notices
- 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 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 data type, 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 keep the data secure.

14. Data Security & 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, which contain personal data, are kept under lock and key when not in use
- papers containing confidential personal data must be kept secure at all times, either in a file, desk drawer or cupboard
- where personal information needs to be taken offsite, staff are expected to store it securely at all times
- encryption software is used to protect all portable devices. Use of removable media such as USB devices is restricted, and no personal data is permitted to be saved on such devices
- staff are expected to use the virtual desktop environment when working remotely
- computer screens are locked when staff are away from their desks
- 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.

15. Disposal of Records

Personal data that is no longer needed, outdated or inaccurate will be disposed of securely, where we cannot or do not need to rectify or update it. For example, paper-based records are placed in confidential waste bins and securely disposed of via a third party, which has provided sufficient guarantees that it complies with data protection law.

16. Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the event of a suspected data breach, staff should notify the DPO immediately. When appropriate, the data breach will be reported to the ICO within the legal timeframe of 72 hours.

17. Training

All staff in the Trust receive regular training on data protection law and any other data protection matters.

18. Links with Other Policies & Documents

- Photography and Video Consent Form *(Appendix 1)* – Whitelands Park Primary School & Francis Baily Primary School adapt to suit their own uses.
- Biometric Consent Form *(Appendix 2)* – Kennet School
- Personal Data Breach Procedure *(Appendix 3)* – Equinox Learning Trust
- Subject Access Request Procedure *(Appendix 4)* – Equinox Learning Trust
- CCTV Policy
- Data Retention Schedule
- Acceptable Use Policy
- Bring Your Own Device (BYOD) Policy

Appendix 1

Pupil Consent Form (Years 7-11)

Kennet School & Equinox Learning Trust

Pupil Name: _____ **Tutor Group:** _____

How we use photographs and videos

Taking photographs and video recordings of the pupils at our school is a key part of life at Kennet School and Equinox Learning Trust ("the Trust"), from displaying examples of work and celebrating achievements to providing exam material. The purpose of this form is to explain our practices in this area and also to ask for your consent for certain uses of photographs and videos.

Sometimes photographs and videos may be used to celebrate the success of our pupils. Photographs may be displayed around the school in places that might be seen by visitors.

When we use photographs and videos for teaching and welfare purposes we will not ask for your consent.
For example, we do not seek your consent before taking or using photographs or videos for the following:

- to help with your learning, such as if we record a Drama or Dance lesson;
- to be used for an internal exhibition or display, including digital displays (such as the plasma display in Reception), eg photographs taken on a school trip or at a sporting event;
- for health and safety reasons, eg to help staff to identify children with allergies;
- for praising your achievements within the school eg your name and your tutor group may be used in displays around the school to celebrate success, such as 'Design & Technology Star of the Term'.

If you do **not** want the school to use photographs and videos as described above, please let us know by speaking to your Tutor or Head of House.

- Photographs and videos will remain on our school & Trust websites and social media feeds, possibly after you have left the school.
- The school will not use information about you or your full name (both first name and last name together) next to any public photograph or video, on our website, in our school prospectuses or in any of our printed publications without your specific permission. But we may use group or class photographs or footage with general labels, such as "a Science lesson" or "fundraising".

We would like your consent for more public uses of photographs and videos. These uses are listed in the boxes below**. If you are happy to consent, we ask that you sign and date the form. If you are not happy for us to use photos and videos of you in the ways we list below, that's ok. We will respect your wishes. Please write 'I do not consent' clearly at the top of the form and sign and date it.**

Uses of Photographs and Digital Media	
I am happy for my photograph to be used as follows: • school & Trust websites • school newsletter • school prospectuses • School & Trust social media channels (Twitter, Facebook, LinkedIn)	• www.tes.com (staff recruitment) • recruitment pack • local newspapers & their websites • public relations materials such as flyers • press releases
I am happy for the school to use non-speaking videos of me as follows: • school & Trust websites • school newsletter	• school social media channels (Twitter, Facebook, LinkedIn, YouTube) • school video library (ClickView) • www.tes.com (staff recruitment)
Live streaming: I am happy for the school to live stream an event, such as House Music, in which I am taking part where access to the event (including the link being shared) is limited to the school community. I understand that I will be told in advance if the event is being live streamed and can opt out if I want to.	

If you change your mind at any time and want to change or remove your consent, you can let us know by speaking to your Tutor or Head of House.

If we would like to use photographs or videos of you in different ways to those listed above, we will ask you again separately. For example, if we want to use your photograph in a way which will be used more widely, such as in a newspaper advertisement, or live stream an event where access to the event is not limited to the school community (ie it is available publicly on a streaming website, such as YouTube).

- We sometimes have visits by the media who may take photographs or footage of a visiting person or other high-profile event. Pupils will often appear in these images which may then be used in local or national newspapers, approved websites or on televised news programmes. We will let you know if this will happen and ask for your consent if the photograph or video will prominently feature you.

Signed by Pupil: _____ **Date:** _____
Parental consent:
I have discussed this with my child and agree to their consent.

Signed electronically by Parent via online Frog form: ☐ **Date:** _____
Name: _____ **Relationship to child:** _____

Appendix 2

Consent Form (Biometric Information)

Kennet School Cashless Catering

Pupil Name: _____ **Tutor Group:** _____

Kennet School wishes to use information about your child as part of an automated (i.e. electronically-operated) recognition system. This is for the purpose of using the school catering system. The information from your child that we wish use is referred to as 'biometric information'. Under the Protection of Freedoms Act 2012 (sections 26-28), we are required to notify each parent of a child and obtain the written consent of at least one parent before being able to use a child's biometric information for an automated system.

What is biometric information and how will we use it?
Biometric information is information about a person's physical or behavioural characteristics that can be used to identify them, eg information from their fingerprint. Kennet School would like to take and use information from your child's fingerprint and use it for the purpose of using the school catering system.

The information will be used as part of an automated biometric recognition system. This system will take measurements of your child's fingerprint and convert these measurements into a template to be stored on the system. An image of your child's fingerprint **will not** be stored. The template is used to permit your child to access this service.

You should note that the law places specific requirements on schools when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system. For example:

- Kennet School cannot use the information for any purposes other than those for which it was originally obtained and made known to parents.
- Kennet School must ensure the information is stored securely.
- Kennet School must tell you what it intends to do with the information.
- Unless the law allows it, Kennet School cannot disclose personal information to another person/body. The only person/body that Kennet School will share biometric information with is Cunninghams, the supplier of the automated biometric recognition system.

Providing your consent
As stated above, in order to be able to use your child's biometric information, we require written consent of at least one parent. Consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. If your child objects to this, Kennet School cannot collect or use his/her biometric information.

If you change your mind at any time and want to remove your consent, you must let us know in writing by emailing office@kennetschool.co.uk or writing to the school.

Even if you have consented, your child can object or refuse at any time to their biometric information being collected/used. Their objection does not need to be in writing. Please could you discuss this with your child and explain to them that they can object if they wish. In the event that either you or your child objects to such processing, we offer an alternative in the form of a card.

If you give consent to the processing of your child's biometric information, please tick the box, sign and date this form.

Tick (✓)	Use of biometric information (fingerprint)
	I am happy for my child's biometric information to be used by Kennet School for the purpose of providing catering services

Please note that when your child leaves Kennet School, or if for some other reason he/she ceases to use the biometric system, his/her biometric information will be securely deleted.

Signed: _____**(Parent/Carer)** **Date:** _____

Print Name: _____ **Relationship to child:** _____

Appendix 3

Personal Data Breach Procedure

- On finding or causing a data breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - lost
  - stolen
  - destroyed
  - altered
  - disclosed or made available where it should not have been
  - made available to unauthorised people.
- The DPO will alert the CEO.
- The DPO will make all reasonable efforts to contain and minimise the breach, assisted by relevant members of staff 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 (eg emotional distress), including through:
  - loss of control over their data
  - discrimination
  - identify theft or fraud
  - financial loss
  - unauthorised reversal of pseudonymisation
  - damage to reputation
  - loss of confidentiality
  - any other significant economic or social disadvantage to the individual(s) concerned.

  If it is 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.
- 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 measure which 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 taken, or will be taken, to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The CEO 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 following:
  - facts and cause
  - consequences
  - action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training)

Appendix 4

Subject Access Request (SAR) Procedure

- Subject access requests (SAR) may be made verbally or in writing. If staff receive a subject access request, they must immediately let the DPO, CEO or their Headteacher know. Completing the Subject Access Request form is desirable but not compulsory and will not prevent the Trust from complying with the SAR.

- The DPO, CEO or Headteacher must establish who has made the SAR.

- For parents/carers to make a SAR in respect of their child, the child must either be unable to understand their rights and the implications of a SAR or have given their consent. If the SAR has come from the parents/carers, the CEO or Headteacher will judge whether the child is mature enough to understand their rights and the implications of the SAR and obtain consent from the child.

    - For children aged 12 and over, who are generally regarded as mature enough to understand their rights and the implications of a subject access request, the request should come from the child, or the child should have provided their consent.

    - For children below the age of 12, who are generally not regarded as being mature enough to understand the rights and implications of a subject access request, the request may come from the child's parents or carers and may be granted without the express permission of the child; however, this is not a rule and the child's ability to understand their rights must be judged on a case-by-case basis.

- The DPO, CEO or Headteacher may ask the individual to provide two forms of identification.

- The DPO, CEO or Headteacher may contact the individual via telephone to confirm the request was made.

- The DPO, CEO or Headteacher may contact the individual to clarify the scope of the SAR to establish if they are looking for something specific or whether the SAR covers all personal data relating to that individual.

- The DPO will initiate the SAR Refinement Process to ensure the request falls within reasonable processing bounds.

- The DPO, CEO or Headteacher may exclude correspondence between the individual and the school on the grounds that the individual already has this information.

- If the SAR is manifestly unfounded or excessive, the Trust may refuse to act on it, or charge a reasonable fee that considers administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or overlaps with other requests. Where such a request is refused, the DPO will inform the individual about the reasons for such action and advise them of their right to complain to the ICO.

- The DPO will provide the Head of IT with the scope of the SAR, and 'reasonable' searches of the network and email systems will be carried out to provide the personal data requested within the context of the SAR, including archived documents or emails if applicable. This will not include CCTV unless this has been specifically requested.

- The DPO will request any non-electronic files, such as the pupil paper file or the staff file.

- The DPO will respond without delay and within one month of the receipt of the request unless the SAR is complex or numerous, in which case the period to respond may be extended to three months from receipt of the SAR. In this instance, the DPO will inform the individual of this within one month and explain why the extension is necessary.

- The DPO will review the results of the searches. As individuals are entitled to their own personal data only, data belonging to other data subjects will be removed if it is separate from the individual to whom the SAR relates. Where the data is mixed but not contentious or sensitive, it can be disclosed, but if this is the case, the following considerations will be made prior to disclosure:
    - all the circumstances pertaining to the collection of the data
    - any expectation of confidentiality around the data
    - whether consent has been sought from the other data subjects involved, and whether it is reasonable to do so.

  Where the data is mixed, and the third party is an employee, it is always reasonable to release the staff member's personal data regardless of context.

- The DPO and CEO will consider whether any of the exemptions set out in the GDPR and Data Protection Act 2018 (DPA2018) apply. This will be judged on a case-by-case basis and where an exemption applies, the Trust will justify and document its reasons for relying on an exemption. Examples of exemptions which might apply:
    - **protection of the rights of others** - revealing information about another individual who can be identified from that information, except if the other individual has consented to the disclosure or it is reasonable to comply with the request without that individual's consent (i.e. where the information is neither contentious nor sensitive)
    - **child abuse data** - revealing that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
    - **education data – serious harm** – revealing information might cause serious harm to the physical or mental health of any individual (known as the 'serious harm test' for education data)
    - **education data – processed by a court** – education data supplied to a court in the course of proceedings and these proceedings are subject to certain specific statutory rules which allow the education data to be withheld from the individual to whom it relates
    - **confidential references** either given or received by the Trust
    - **exam scripts and marks** - personal data (answers) recorded by individuals during an exam.

- The DPO or other authorised employee will print out, redact, and collate the information. It will then be scanned in a commonly used electronic format and saved onto the network, clearly named, into a secure folder, to send to the individual, unless they have requested an alternative format.

- The DPO will provide information to the individual, which is concise, transparent, intelligible and in easily accessible form, using clear and plain language. This will include the following:
    - the purpose of processing
    - the categories of personal data processed
    - the recipients of the data (third parties with whom the data has been shared)
    - the retention period
    - their data rights including how to complain to the ICO
    - the source(s) of the information
    - any exemptions which have been applied
    - details of any transfers outside of the EEA.