Data Protection Policy

Galleywood Infant School

Approved by:	Sarah Manning & FGB	**Date:** May 2024
Last reviewed on:	May 2024	
Next review due by:	May 2026	

Contents

---

1. Aims

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act 2018, the Privacy in Electronic Communications Regulations (PECR) and the UK General Data Protection Regulation (UK GDPR). It is based on guidance published by the Information Commissioner's Office (ICO) on the ico.org.uk website and the ICO's code of practice for subject access requests.

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

It applies to anyone who handles or has access to people's personal information, regardless of the way it is collected, used, stored and disposed-of in either physical or electronic form.

2. 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
Confidential personal data	Personal data, which is used to confirm identity and so needs more protection, including information about an individual's: › national insurance number; › date of birth; › bank account details; › credit card details; and › copies of government issued documents (Passport, driving license etc.).
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.

TERM	DEFINITION
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3. Principles of data processing

3.1 The school will process personal data in accordance with the 7 principles of data processing including:

1) Lawfulness, Fairness, and Transparency – The school will ensure that all personal data is collected, processed, and shared in a lawful, fair and transparent manner to uphold the privacy and rights of the data subject.

2) Purpose Limitation – The school will ensure that all personal data will only be collected for specific, explicit, and legitimate purposes. The data subjects will be notified prior to any processing for any purpose other than the one disclosed at the time of collection.

3) Data Minimisation – The school will ensure that all personal data is adequate, relevant and limited to what is necessary to carry out its declared purpose.

4) Data Accuracy – The school will ensure that all personal data held is accurate and where necessary, kept up to date.

5) Storage Limitation – The school will retain personal data only as long as it is necessary to fulfil the stated purpose or to fulfil a legal obligation.

6) Integrity and Confidentiality (Security) – The school will ensure that all personal data is processed in an appropriate manner to maintain security.

7) Accountability – The school will maintain all required records, documentation and registers required to demonstrate its compliance with the data protection laws.

3.2 To fulfil these principles, the school will:

- ensure all personal data is fairly obtained in accordance with the school "Privacy Notice for Pupils and Parents", Privacy Notice for School Workforce and Privacy Notice for Governors" and lawfully processed in accordance with the "Conditions for Processing".
- ensure parents are asked, at regular intervals, to confirm the data the school holds about them or their child is correct through data collection sheets;
- apply the records management policies and procedures to ensure that information is not held longer than is necessary;

- ensure that when information is authorised for disposal it is done appropriately;
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system;
- only share personal information with others when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act;
- train all staff so that they are aware of their responsibilities and of the schools' relevant policies and procedures.

4. Roles and responsibilities

This policy applies to all staff employed by the school including volunteers, and to external organisations or individuals working on behalf of the school. Staff, who do not comply with this policy may face disciplinary action.

4.1 Data Controller

The school determines the purpose and means for the processing of personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered, as a data controller, on the ICO's register of fee payers, registration number **5776013**.

4.2 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

4.3 Data protection officer

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

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

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

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

Our DPO is The ONTO Group Data Protection Team - GDPR@theontogroup.com

4.4 Named Individuals

The Headteacher and Office & Finance manager, act as representatives of the data controller on a day-to-day basis.

4.5 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy

- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they intend to engage in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

5. Collecting personal data

5.1 Lawfulness, fairness and transparency

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

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school 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 one 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.

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.

5.2 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 school's record retention schedule.

5.3 Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents /carers of all *pupils / students* of the data they collect, process and hold on *pupils / students*, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed.

This privacy notice will be passed to parents / carers through the school website and will be available from the school office on request. Parents / carers of young people who are new to the

school will be provided with the privacy notice through the school website or a hard copy can be obtained from the school office on request. Information informing Parents about the Privacy Notice will be included on the school registration form and data collection forms.

In some circumstances additional information may be collected and processed or a person's image captured, during a school event such as school fund raising activities, school performances, parents volunteering as a responsible adult on a school trip etc, in these instances personal data will be processed in accordance with the school policies and procedures but the individual will be informed via a dedicated privacy notice either during or prior to the event or activity as appropriate.

6. Secure storage and access to information

6.1 The school 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 that contain sensitive personal data are kept under lock and key when not in use;
- Papers containing sensitive or confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- All users will use strong passwords which must be changed regularly. User passwords must never be shared;
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for 15 minutes;
- Personal data can only be stored on school equipment (this includes computers and portable storage media.

6.2 The school will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

6.3 When personal data is stored on any laptop, other portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected;
- the device must be password protected;
- where possible, the device must offer approved virus and malware checking software; and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

6.4 The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

6.5 The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example: *2Simple Software EYFS Profiles; Redstor Backup*) and is aware that data held in remote and cloud storage is still required to be protected in line with the data protection laws. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

6.6 Access out of school

The school recognises that personal data may be accessed by teachers and other users out of school. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location;
- Users must take particular care that computers or removable devices which contain personal data are not accessed by other users (eg family members) when out of school;
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and

7. Sharing personal data

7.1 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 which 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

7.2 The school will also share personal data with law enforcement and government bodies where legally required to do so, including for:

- The prevention or detection of crime and/or fraud;
- The apprehension or prosecution of offenders;
- The assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- Where the disclosure is required to satisfy our safeguarding obligations;
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

7.3 The school may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects pupils or staff, including in the containment of a contagious disease.

7.4 Where the school transfers personal data to a country or territory outside the United Kingdom, it will do so in accordance with data protection law.

8. Subject access requests (SAR) and other rights of individuals

8.1 Subject access requests

The school recognises that under the UK GDPR data subjects have a number of rights in connection with their personal data, the main one being the right of access. The Procedures are set out in Appendix 2 to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data, relating to the data subject and held by the data controller.

8.2 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, individuals may also, depending on the lawful basis of processing, 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 which 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

9. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

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

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.

10. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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

Any enquiries about the CCTV system should be directed to Head Teacher.

11. Photographs and videos

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

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 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 for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school 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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not include in future distribution.

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.

12. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection 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 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 school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, 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

13. 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.

14. Personal data breaches

The school 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 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

15. Complaints

Complaints will be dealt with in accordance with the school's complaints policy and procedures. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator) if appropriate.

16. Training

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

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

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every two years and approved by the full governing board.

18. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online Safety Policy

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) either via email **GDPR@theontogroup.com** or phone **0161 504 6921**.

- The DPO will consider the report and determine whether a breach has occurred, and if it is reportable or just recordable in the school compliance records.. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Accessed by an unauthorised individual.
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been.
    - Made available to an unauthorised individual.
- Staff and governors will cooperate with any investigation (including allowing access to information and responding to questions). Any 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 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. 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 on the school's network in a secure area. 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 school'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 school 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 on the school's secure network.
- 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.
- The DPO and named individual will meet termly 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 school or the DPO will ask the ITHelpdirect to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence). ~~from external recipients and remove it from the school's email system (retaining a copy if required as evidence).~~
-

- In any cases where the recall is unsuccessful or cannot be confirmed as successful ~~or cannot be confirmed as successful~~, the DPO will consider whether it's appropriate to ~~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 designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website.
- Non-anonymised pupil exam results or staff pay information being shared with governors.
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked.
- The school's cashless payment provider being hacked, and parents' financial details stolen.
- Hardcopy reports sent to the wrong pupils or families.

Appendix 2: Procedures for responding to subject access requests made under the UK GDPR.

Rights of access to information

1. There are two distinct rights of access to information held by schools about pupils:
   i. Under the UK General Data Protection Regulation (UK GDPR) any individual has the right to make a request to access the personal information relating to them.
   ii. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (England) Regulations 2004.

   These procedures relate to subject access requests made under the UK GDPR.
2. Under the legislation data subjects have the right to know:
   - if the data controller holds personal data about them;
   - a description of that data;
   - the purpose for which the data is processed;
   - the sources of that data;
   - to whom the data may be disclosed; and
   - a copy of all the personal data that relates to them.

Undertaking a subject access request

3. To ensure the best response, requests for information should be made in writing; which includes email and be addressed to the Headteacher. If the initial request does not provide adequate proof of identity or clearly identify the information required, then further enquiries will be made.

4. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
   - passport
   - driving licence
   - utility bills with the current address
   - Birth / Marriage certificate
   - P45/P60
   - Credit Card or Mortgage statement

   This list is not exhaustive.

5. Any individual has the right of access to information relating to them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

6. The school may make a charge for the provision of information, dependent upon the following:
   - The request is deemed to be unfounded or excessive by the school and the subject still desires the information.
   - The request is for additional copies of a completed previous request. The school can charge a reasonable fee for the provision of the additional copies.
7. The response time for subject access requests, will be a maximum of 1 month, but without undue delay. The 1-month period will not commence until the requesters identity and relationship are confirmed.

   *Not working or school days but calendar days, irrespective of school holiday periods.
8. If the request is complex or multiple (from the same subject) then it will be fulfilled within 3 months of the request, but without undue delay.
9. The Data Protection Act 2018 allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.
10. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the statutory timescales.
11. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil, or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.
12. If there are concerns over the disclosure of information, then additional advice should be sought (in the case of Local Authority schools from the Borough Solicitor).
13. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
14. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
15. Information can be provided at the school with a member of staff on hand to help and explain matters if requested or provided at face to face handover.
16. The views of the applicant should be considered when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.
17. Complaints will be dealt with in accordance with the school's complaints policy and procedures.