DATA PROTECTION POLICY

COLLEGE TOWN PRIMARY SCHOOL

Adopted by Governing Body	Sept 2026
Approved by FGB v2	Sept 2026
Date of next review	Sept 2028
Statutory	YES
Adopted from Bracknell Forest	YES

1. Introduction

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.

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.

Some changes have been made to UK Data Protection Law through the Data (Use & Access) Act 2025. These changes have been incorporated into this policy in the appropriate sections.

2. Principles of data processing

2.1 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 a compatible purpose to 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.

2.2 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.

3 Definition of Personal Data

The school and individuals will have access to a wide range of personal data which may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identify or could identify an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils / students*, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records;
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references;
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references;
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

3.1 **Special categories of personal data**

Certain categories of personal data are defined within the data protection laws as special categories of data, sometimes referred to as sensitive personal data, due to the possible impact if it is lost or stolen. These include:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- data concerning **health**;

- data concerning a person's **sex life or sexual orientation**;
- **genetic data**; and
- **biometric data** (where used for identification purposes).

3.2 **Criminal offenses**

Personal information detailing criminal offences or prosecutions is defined in the data protection laws as requiring additional safeguards to uphold an individual's privacy and prevent possible persecution.

The data protection laws require that any personal information containing special categories of personal data or criminal offences or prosecutions are:

- only accessed by authorised individuals, relevant to their role within the school;
- stored securely when not in use; and
- destroyed or disposed of securely if no longer required.

3.2 **Confidential personal data**

Certain items of personal data are not defined as special categories of personal data however they would still have a potential severe impact if lost, stolen, or accidentally disclosed such as identity theft, criminal impersonation, or financial fraud. This data will include:

- the date of birth of an adult;
- national insurance number;
- bank account details;
- credit card details; and
- copies of officially issued documentation (passport, driving licence, MOD90 etc.).

The school will process confidential personal data using the same safeguards as used for sensitive personal data including:

- only allow access by authorised individuals, relevant to their role within the school;
- stored securely when not in use; and
- destroyed or disposed of securely if no longer required.

4 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.

a. The Data Controller

The school determines the purpose and means of processing for the personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. As such, the school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

b. Governing body

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

c. 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 report directly to the Governing body and operate independently and cannot be dismissed or penalised for performing their duties.

They will hold a termly review meeting with the school and provide an annual report of their activities to the Governing body and, where relevant, report 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.

The Name and contact details of the DPO are provided in Appendix One

d. Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

e. Information Asset Owners

The school will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information as been amended or added to over time, and
- who has access to protected data and why.

f. 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 United Kingdom
    - 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

g. Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

5 Collecting and using Information

5.1 Lawfulness, fairness and transparency

The school will only process personal data where it has 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 e.g. to protect someone's life;
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions;
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden);
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent** .

For criminal offence data and special categories of personal data, the school will also meet one of the special category conditions for processing which are set out in UK GDPR: Article(9)& Article(10) as well as schedule 1 of the Data Protection Act 2018.

5.2 Limitation, minimisation and accuracy

The school will only collect personal data for specified, explicit and legitimate reasons. These reasons will be explained to the individuals when their data is first collected.

If the school wants to use personal data for reasons other than those compatible to the original reason (purpose) given when the information was first obtained, the school will inform the individuals concerned before it does so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

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 personal data are kept under lock and key when not in use;
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- Where personal information needs to be taken off site, staff must sign it in and out from the school office; must be held in lockable storage, whether on or off site.
- 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. **Private equipment (i.e. owned by the users) must not be used for the storage of personal data, the exception to this is personal phones which can be used for the purpose of accessing school email only.**
- Any portable or mobile devices or removeable media, likely to contain personal data must be encrypted.

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 that is removed from site, 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
- Particular care should be taken if data is taken or transferred to another country outside of the United Kingdom.

7 Sharing data

7.1 The school will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- There is a need to liaise with other agencies – the school will seek consent as necessary before doing this;
- Suppliers or contractors need data to enable the school to provide services to staff and *pupils/students* – for example, IT companies. When doing this, the school will:
  - o Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
  - o 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 shared;
  - o Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the school.

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.

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 3 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 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 may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

8.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information about how information will be used and processed at the time it is collected, individuals also have the right to:

- Withdraw their consent to processing at any time;
- Request the school to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Challenge processing which has been justified on the basis of public interest;
- Request a copy of agreements under which their personal data is transferred outside of the United Kingdom;
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- Prevent processing that is likely to cause damage or distress;
- Be notified of a data breach in certain circumstances;

- Make a complaint to the Information Commissioner's Office;
- 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.

8.4 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.

9 Disposal of Information

9.1 Personal data that is no longer required 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.

9.2 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.

10 Personal Data Breeches

10.1 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 2.

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

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

11 Data Protection Complaints

Under changes introduced as part of the Data (Use & Access) Act the school is required to provide a means for recording complaints, acknowledge complaints within 30 days, make appropriate enquiries, keep complainants informed and communicate the outcome without undue delay. There are no general exemptions from having a complaints process.

The ICO also states that people may complain through channels other than the organisation's preferred form or email address. Staff should therefore be trained to recognise and promptly route complaints received verbally, by social media or through general customer-service channels.

The school has a data protection complaints form which can be downloaded from the school website.

Summary of complaint stages.

- Logged + ID Assigned
- Acknowledged ≤30 days
- Initial Assessment (Identity + Scope + Risk Score)
- Risk Branch:
  Low/Medium → Standard Review
  High/Critical → Immediate DPO Escalation

- Investigation
- Evidence Review
- Decision Drafted
- DPO Approval
- Outcome Sent
- Closed
- Lessons Learned Recorded

Mandated deadlines.

- Acknowledgement ≤30 days
- Assessment ≤5 working days
- Investigation ≤30 days

- High Risk Immediate
- Outcome Without Undue Delay

12 Training

12.1 All staff and governors will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy, as part of their induction.

12.2 Data protection will also form part of continuing education with all staff taking part in further training at least annually to maintain awareness of responsibilities, particularly where changes to legislation, guidance or school processes make this necessary.

13 Monitoring

13.1 The DPO is responsible for monitoring and reviewing this policy and its implementation.

13.2 The school will maintain a record of all information collected including its destruction and any data breaches, including those that are not reportable.

13.3 This policy will be reviewed **every 2 years** and shared with the full governing board.

Appendix One

Name and contact details of the Data Protection Officer (DPO)

Name	**DHR Consultancy**
Address	**50b Manchester Road**
	Huddersfield, HD7 5JA
Email	**darren.rose@dhrconsultancy.co.uk**

Appendix Two

Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1) On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
2) 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
3) The DPO will alert the headteacher and the chair of governors
4) The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
5) The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
6) The DPO will undertake a risk assessment to establish whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

    If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
7) 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. This information will be retained as set out in the Information Assets Register (IAR).
8) Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

9) 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

10) The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

11) The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

12) 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)

13) 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

Actions to minimise the impact of data breaches

14) The school will take action to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The actions taken will be recorded and their effectiveness subsequently reviewed to establish whether further improvements can be made to systems and procedures.

Appendix Three

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.

   Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

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, dependant 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. Where a request is unclear, very broad, or likely to involve a large volume of information, the organisation may seek clarification from the requester before proceeding.

   Clarification may be sought to:

   - identify the specific personal data or processing activities of interest;
   - narrow the scope of the request to manageable and relevant data; and
   - enable a timely and accurate response.

   Where clarification is requested, the statutory response timeframe may be paused until clarification is received, in line with data protection law.

   The organisation will use the SAR clarification letter 1 [SAR-CLR01] to seek clarification on the initial request, the statutory response timeframe will remain paused for a period of 30 days, on no response the SAR clarification letter 2 [SAR-CLR02] will be sent. If following a further 30 day period, a response is still not received, the request will be assessed to determine if it can be fulfilled without the clarification, even in part. If it can, the request will continue to be collated using the reasonable and proportionate assessments mentioned previously. If it is not possible to continue with the request, a notification will be sent to the requester detailing the decisions made in closing the request.

9. All clarification requests and responses must be documented.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.

10. When responding to a Subject Access Request (SAR), the organisation will take reasonable and proportionate steps to identify, locate, and provide the requester's personal data, in accordance with applicable data protection law.

    The organisation is not required to carry out searches that would be excessive or disproportionate, taking into account the nature of the request, the systems involved, the resources required, and the likelihood that relevant personal data would be identified.

    When assessing reasonable and proportionate effort the SAR Proportionality Assessment Tool [SAR-PAT01] must be used for both consistency and compliance evidence.

Assessing the Scope of a Search

At the outset of each SAR, the case handler must assess:

- the wording and scope of the request;
- the types of personal data likely to be in scope;
- the systems, repositories, and business areas where the data is reasonably likely to be held;
- the time period covered by the request; and
- whether any limitations or refinements can reasonably be applied.

Searches must be targeted, documented, and proportionate to the request. There is no obligation to search every system or data source if it would not be reasonable to do so.

An example of an unreasonable or disproportionate search would be a search conducted on all staff email accounts for documentation or discussion as part of a HR-related subject access request. It could be determined that it is unlikely that any documents or discussion, in regard to HR functions relating to the requester, would be present in the email accounts of other staff members who are not part of the HR function.

Reasonable and Proportionate Searches

In practice, this may include:

- searching core systems, databases, and records that are known to contain personal data relevant to the requester;
- applying reasonable parameters such as date ranges, data categories, or business functions; and
- excluding systems or records where searches would be technically impractical, disproportionately burdensome, or unlikely to yield relevant personal data.

Where search limitations are applied, the rationale must be recorded in the SAR case file.

11. The Data Protection Act 2018 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

12. 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.

13. 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.

14. 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).

15. 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.

16. 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.

17. 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.

18. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

19. Complaints

Complaints will be dealt with in accordance with the school's complaints policy and procedures.