William Austin Junior School

Subject Access Request Policy

Introduction and purpose

The Data Protection Act 2018 (the Act) gives individuals rights of access to their personal records held by William Austin Junior School. Subject access is a fundamental right for individuals. But it is also an opportunity for the school to provide excellent customer service by responding to Subject Access Requests (SARs) efficiently and transparently and by maximising the quality of the personal information you hold. This Policy explains how the school will fulfil its obligations under the Act.

Policy Statement

The school regards the Act as an important mechanism in achieving an honest, safe and open relationship with its students and employees.

Subject access is most often used by individuals who want to see a copy of the information the school holds about them. However, subject access goes further than this and an individual is entitled to be:

- Told whether any personal data is being processed;
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- Given a copy of the personal data; and
- Given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions taken about him or her, such as a computer-generated decision for benefit or a grant entitlement, or an assessment of performance at work.

The aim of this policy is to ensure that the school complies with its legal obligations under the Data Protection Act 2018 and can evidence that you have done so. It also aims to ensure that you:

- Have robust processes in place for dealing with SARs, saving time and effort;
- Increase levels of trust and confidence by being open with individuals about the personal information you hold;
- Improve the transparency of your activities in line with public policy requirements.

This policy should be read in conjunction with the **Subject Access Request Procedure (Appendix 1)**

Scope of the Policy

This document outlines how an applicant can make a request for their personal information under the Act and how it will be processed.

This is not a legal document. It does not confer rights nor override any legal or statutory provisions which either require or prevent disclosure of personal information.

This document takes into account the key features of the Act and outlines how the school will take steps to ensure compliance in relation to requests for personal information.

Requests for access to the records of people who are deceased are not within scope of this Policy as the Act only applies to the data of living individuals. Such requests will be treated as requests for access to information under the Freedom of Information Act or as miscellaneous requests, depending on the nature of the data and the reason the data is being requested.

Key Definitions

Subject Access Request or SAR	A request for access to data by a living person under the Act is known as a Subject Access Request or SAR. All records that contain the personal data of the subject will be made available, subject to certain exemptions.
Freedom of Information Request or FOI.	A request for access to data held is dealt with under the Freedom of Information Act 2000 and is known as a Freedom of Information Request or FOI. Requests for the data of deceased people may be processed under this legislation.
Personal Data	Personal data means data which relates to a living individual who can be identified directly or indirectly from the data, particularly be reference to an identifier. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).
Special Category Data	Certain personal data, special category data, is given special protections under the Act because misuse could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Special category data includes: a person's racial or ethnic origin; political opinions; religious or similar beliefs; trade union membership; physical or mental health or condition or sexual life; biometric or genetic data.
Data Controller	The organisation which determines the purposes and the manner in which, any personal data is processed is known as the data controller. The school is the data controller of all personal data used and held within each part of the school

Data Processors	Organisations or individuals who process personal data on behalf of a data controller are known as data processors. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.
Data Subject	A living individual who is the subject of personal data is known as the data subject. This need not be a UK national or resident. Provided that the data controller is subject to the Act, rights with regards to personal data are available to every data subject, wherever his nationality or residence.
Third Party	An individual who is not the subject of the data but may be connected to or affected by it is known as a third party.
Relevant Professional	The practitioners who supply information held on Social Services records, and various other medical and educational records. A relevant professional will consider where disclosure is likely to cause serious physical or mental harm to the applicant or any third party.

Duties of the Information Commissioners Office

The Information Commissioner's Office is the UK's independent public body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals, ruling on complaints and taking appropriate action when the law is broken.

The Information Commissioners Office is responsible for ensuring compliance with the Act and Data Protection in practice for all organisations in England, Scotland, Northern Ireland and Wales.

There are a number of tools available to the Information Commissioners Office for taking action to change the behaviour of organisations that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audits. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller for breaches of the Act.

If organisations are found to be in breach of the Act the Information Commissioners Office may issue undertakings committing an organisation to a particular course of action in order to improve its compliance.

The Information Commissioners Office can serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law.

The Information Commissioners Office conduct consensual assessments (audits) to check organisations are complying. In cases of serious breaches the Information Commissioners Office may issue a monetary penalty notice, requiring organisations to pay a fine of up to €20 million.

The Information Commissioners Office can prosecute those who commit criminal offences under the Act. This includes organisations and individuals.

Roles and Responsibilities

Adhering to the Data Protection Act 2018 is the responsibility of every member of staff acting for or on behalf of the school. Subject Access requests fall within the data protection statutory framework and the ability to identify and appropriately handle a request for information is considered to be part of every employee's role.

Your primary responsibility is to ensure that Subject Access Requests are in the first instance directed to the School Business Manager. The team will log the request, acknowledge it and pass the case to the school department for response. It is important that requests are processed as soon as they are received to assist in meeting the statutory deadline.

Head teacher	The head teacher holds overall responsibility for compliance with the Act.
School Business Manager	The School Business Manager has responsibility for the management of Subject Access Requests; this includes assisting your Data Protection Officer in dealing with complaints from the Information Commissioners Office, general compliance issues and data subject queries and concerns. Ensures that SARs are responded to in a timely manner and that only data that the data subject is entitled to access are sent out. Also responsible for completing a double check of all SAR's before they are securely dispatched.
Employees	All employees, including temporary staff, must understand their duty of care to ensure the confidentiality of all personal data. In addition they must have an understanding of this policy and where to direct individuals enquiring about subject access requests.

How can an individual make a SAR?

A valid SAR must always be made in writing. Most SAR requests are made by parents and members of staff via email or post.

It is quite common that a request for personal data can be linked with a complaint, or a Freedom of Information request.

NOTE: No matter how a request is received there is no requirement for the requester to mention either the Data Protection Act or Subject Access for it to be a valid request. In some cases the requester may even state the wrong legislation e.g. Freedom of Information Act, but the request will still be valid.

Either way, it is the responsibility of the staff member dealing with the request to appropriately recognise a request as one for personal data, i.e. information relating to the requester, and process it accordingly. Failing to recognise a SAR is not an excuse for non-response and the school will still fall foul of the Data Protection Act should a response not be provided in a prompt and appropriate manner.

Can individuals request personal information on behalf of another person?

Yes they can. The Act allows for an individual to make a request on behalf of another person. This may be a solicitor acting on behalf of the individual, a parent making a request for their child's information, a third party making the request for someone who has limited capacity, or indeed many other reasons. However, whilst the Act allows us in certain circumstances to process a request in this way, there are a number of considerations and checks that need to be undertaken before you process a request which is made on behalf of another person. For example, a parent is not necessarily automatically entitled to information about their children. Further information with regards to SARs made on behalf of another person can be found in the Subject Access Procedure

How long do we have to respond?

The school has a maximum of a month starting from the day the request and identification (if required) is received. This is a statutory requirement which must be adhered to. In exceptional circumstances an extension can be agreed.

Can I charge for the request?

No - you must provide a copy of the information free of charge.

However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

What do I do if I receive a request?

In practice, if someone wants to see a small part of their data (an exam result or written consent); you need to apply common sense. You should not require a formal SAR if the individual can prove their identity, the information is readily available there and then, and no other third party data will be unreasonably released. Such requests should be dealt with quickly, as business as usual and with little formality.

All other ("non-routine") requests for personal data which are likely to take a reasonable amount of resource must be directed to the School Business Manager and be logged.

How do I locate the information requested?

Processing a subject access request can prove very difficult if you do not have adequate information systems in place. Well-structured file plans and standard file naming conventions within schools should be in place to assist in locating information easily.

Poor file management / knowledge of systems cannot be used as a reason for being unable to respond to a SAR effectively.

Requests for information are not limited to "live" files. SARs cover all information held by the school regardless of the format it is in or where it is stored, closed, archived, and in some cases even deleted information (e.g. located in outlook deleted items) should be considered as part of a request.

Unfortunately, there is no outright exemption or time threshold with regards to the amount of time it may take members of staff to locate SAR information. Further information with regards to resource intensive or complex SARs can be found in the Subject Access Procedure.

Can I provide all information found relating to the data subject?

The simple answer is no.

The school must consider whether it is possible to comply with the SAR without revealing information that relates to and identifies a third party individual or any other exempt information.

Examples of third party information that cannot be shared routinely without specialist consideration are:

- Safeguarding concerns which may contain information about multiple children including siblings and estranged parents
- Files containing legally privileged information
- Files containing advice from relevant professionals such as doctors, police or probation services
- Employee files containing information identifying managers or colleagues who have contributed to (or are discussed in) that file.

Special consideration should be given to sharing this type of information. More information can be found in the Subject Access Procedure (Appendix 1).

What is a double check?

Before a SAR is sent out to the data subject Senior Management are required to carry out a double check. This is done to ensure that all third party data has been removed appropriately and that any documents have been redacted appropriately.

Third party data sent out in error to the wrong person constitutes a data breach under the Data Protection Act 2018 and can have very serious consequences for the school (see section 5 above).

Senior Management are responsible for completing a double check of the information to be provided to the data subject. For further guidance on the double check please refer to the Subject Access Request Procedure.

NOTE: Occasionally schools will outsource the redaction of SARs to a third party provider such as LBC's IG team, a solicitor or barrister. A double check of the work completed must be carried out by Senior Management before any documents are sent out to the data subject. This is to ensure that the work is completed to the standards expected by the school.

How do I respond to a SAR?

Once all of the information has been collated (duplicates and third party information has been removed or redacted and a double check has been carried out) the information will be provided either in paper copy, electronically or during a meeting with the Data Subject and sent securely.

The school is required to provide the copies in a format requested by the data subject. For further information on how to respond securely to a SAR please refer to the Subject Access Request Procedure (Appendix 1).

Complaints

The school will provide a right of complaint to all applicants in the event they are dissatisfied with the handling of their request. If an applicant is unhappy with the service they have received they should firstly contact the School Business Manager.

If the applicant is dissatisfied with the content of the information they have received they should also make a complaint in writing to the Head teacher. If an applicant remains dissatisfied with the outcome of their Stage 1 complaint, the school should seek advice from your Data Protection Officer at LBC.

The Data Protection Officer will make an independent assessment of the case. If the applicant remains dissatisfied they may ask the Information Commissioners Office to carry out an independent investigation.

Appealing a decision to refuse disclosure of Information

If the school refuses to disclose information in response to a subject access request, the school should offer the applicant an opportunity to appeal the initial decision. If the applicant believes that an error has been made in the response to their SAR they are able to appeal the schools decision by seeking an internal review which will be undertaken by members of the Governing Body. Once an appeal has been received the complainant will receive an acknowledgment receipt and the request and response to it will be reconsidered.

The applicant will be notified of the outcomes of the internal review as soon as possible. All internal reviews should be concluded within 20 working days.

If an applicant's appeal is successful they will receive the information they requested as soon as possible. If the appeal is unsuccessful the school will provide a detailed explanation of the findings and supply further information on how to take the matter further.

Complaining to the Information Commissioners Office

If an applicant is not satisfied with the outcomes of the schools decisions they have the right to submit a complaint to the Information Commissioners Office. The Information Commissioners Office will make an initial assessment of the case before carrying out an investigation.

The Information Commissioners Office has written guidance notes for applicants on how to complain to the Information Commissioners Office and published it on their website, www.ico.gov.uk

Related documents

- Data Breach Policy
- Data Protection Policy
- Freedom of Information Policy
- Document Retention Policy
- Information Security Policy

Review of the Policy

This policy will be reviewed as a minimum every 2 years to ensure that the school meets statutory requirements and any codes of practice made under the Act.

This policy will be monitored and reviewed by the Governors on an annual basis.

Policy updated: April 2020

Staff responsible: Sally Bacon

This policy was ratified by the Governing body/Local Authority on:

Signed on behalf of the Governing Body: _____(signature)

_____(Printed)

Subject Access Request Procedure **Appendix 1**

Introduction and purpose
The Data Protection Act 2018 gives individuals rights of access to their personal records held by schools.
This guidance aims to help employees deal with Subject Access Requests (SARs) in compliance with school policy.
This document should be read in conjunction with the Subject Access Request Policy

How long do I have to complete a SAR
The school has a maximum of a month starting from the day the request and identification (if required) is received. This is a statutory requirement which must be adhered to. As there is no definition of a month, the school is adopting 20 working days, to ensure consistency.
You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary. You should contact the SAR owner as soon as possible if an extension is required. Extensions will only be granted in exceptional circumstances.
In any event the request should be responded to as quickly as possible. The deadline is a maximum and any deliberate or unjustified delay to hold back a response until nearer the deadline expiry is not acceptable.

For example data such as CCTV footage is subject to "automatic / routine" deletion, which means that after 28 days the data is automatically wiped. If a request is received for data that is subject to automatic deletion such as this, you must not delay the request until after the deletion date, but instead consider responding within the 20 days in a timely manner, or where this is not possible due to other priorities you should mark the footage for non-deletion to allow the request to be fulfilled after the deletion date but still within the 20 days.

Who can submit a SAR
An application for a Subject Access Request must be made by either of the following:

- **The Data Subject;**

A data subject is entitled to make a request in writing to see any personal data held about them under the Act. The school must ensure they only provide data to the data subject of an authorised person on their behalf and so may require the data subject to provide proof of identity and current residence before the request is processed, this must been in the form of photographic ID, such as driver's license or passport and a recent utility bill or bank statement as proof of address. This is to prevent unauthorised disclosure to third parties. The documents must be brought in to the school so that the identity of the person can be verified. Only in exceptional circumstances can this requirement be waived. Contact the Information Governance Team if ID cannot be provided face to face.

- **On Behalf of the Data Subject**

Anyone applying for a Subject Access Request on behalf of someone else must apply in writing together with written authorisation from the data subject, which must be signed by the data subjects themselves, if they have capacity. The school requires both the data subject and the person making the request to bring in photographic ID and proof of address. Only in exceptional circumstances can this requirement be waived. Contact the Information Governance Team if ID cannot be provided face to face.

- **A Person with Parental Responsibility**

An individual only has a right to access the records of a minor if they have either parental responsibility or legal guardianship of the child. Parental responsibility is defined in the Children Act 1989 and updated by the Adoption & Children Act 2002. A person with parental responsibility is:

- The natural mother;

- The natural father, if married to the mother either before or after the birth, even if divorced or separated;
- The natural father, if unmarried, and he registered the birth along with the mother after December 2003;
- The natural father, if unmarried, by agreement with the mother (evidenced by a form provided by a solicitor, signed by both parents and witnessed by an Officer of the Court) or by a court order (parental responsibility order);
- The natural father, if unmarried, and appointed as the child's guardian on the death of the natural mother;
- An individual (generally a family member) with a residence order for the child (if the order is for a period of time, then parental responsibility is removed at the end of the period);
- An individual who has legally adopted the child;
- A local authority under a care order - individual acting as a Children's
- Guardian: If the application for access to a child's record is made by someone having parental responsibility access shall only be given where:
- The child is capable of understanding what the application is about and has consented to it.
- The child is not capable of understanding the nature of the application and giving access would be in his/her best interests. The relevant professionals will decide on the child's capacity to understand the application.
- If an individual is claiming parental responsibility then they must provide a copy of the necessary evidence such as a parental responsibility order or the long version of the birth certificate of the child.

- **A Person Appointed by the Courts**

Where the data subject is incapable of managing their affairs someone appointed to act on their behalf by a court of law may submit a subject access request. Proof of the court order must be given.

- **Solicitors acting on behalf of a Client or Insurance Companies**

Where a solicitor or other legal professional requests access on behalf of a client they are representing, the appropriate form of authority containing the signed consent of their client must be obtained and evidenced. The request must be dealt with in the same way as if it had come direct from the Data Subject.

- **Third Party Requests**

In addition to subject access requests the school may also receive third party requests submitted under the Data Protection Act. All third party requests should be submitted in the same manner as Subject Access Requests. They will be considered by the [Business Manager] and will be given the same level of confidentiality as a subject access request**.**

- **The Police**

The police may from time to time submit requests for information relating to a specific individual, these requests are made in order to prevent or detect crime or for taxation purposes. In these circumstances the school will not be required to obtain the consent of the data subject. Requests should be made using s29 form and authorised by a senior officer**.**

- **Other Government Agencies**

In some circumstances the school may be asked to provide information to other Government Agencies. Government Departments require a range of information to carry out their functions. Unless there is a legal requirement to disclose, for example for the prevention or detection of crime or for safeguarding reasons, the Data Subject will be informed and their consent obtained in writing.

What should I do when I receive a SAR?

If you receive a SAR direct from a member of the public you should determine whether you can deal with the request immediately or whether the request is complex and needs further consideration.

Simple requests:

I. Decide if it is something that you can provide quickly yourself. For example copies of consent form, exam result, their own letter of complaint.
II. If you can provide it quickly do so.
III. Put a note on file of what is provided, to whom it went and when the request was completed.

Complex requests:

IV. Make sure the request is in writing and send it to your Business Manager.
V. Most SAR requests are made by parents
VI. Alternatively you can ask the requestor to email your Business Manager or write to the school at: Austin Road, Luton LU3 1UA
VII. Your Business Manager will log the SAR and will allocate the case according to the subject matter

What should I do when I am allocated a SAR by the Business Manager?

I. Think about where the information requested will be kept
II. What types of records you are looking for
III. Do you need to do a search of emails?
IV. Are there any duplicate records?
V. Allocate sufficient time to process the request

- **How do I find the information requested**

Requests for information are not limited to "live" files. SARs cover all information held by the school regardless of where it is stored, closed, archived.

You should first consider which system the information requested will be stored on. For example information about pupils will be kept on SIMS. Information about safeguarding will be kept on CPOMS or paper files.

In some cases multiple systems will need to be checked in order that all relevant data is located.

You should do searches using the minimum data fields possible. For example, using common surnames such as Khan or Smith will result in a significant number of hits, many of which will be unrelated. However, using the DOB and Surname will limit the number of search results significantly.

It can often be helpful to speak to the requestor to find out if there is something specific that they are looking for. For example a requestor might ask for everything the school holds about them, but they may only want to see information relating to a specific issue such as a disciplinary matter.

Often limiting the search to a specific timeframe also helps reduce the search.

In most cases this information will need to be printed manually. **NOTE:** make sure that you print securely and lock away any documents printed until you have completed the entire search.

- **Are there any duplicate records?**

Once you are satisfied that you have access to all of the relevant documents related to the SAR request you should take time to remove all duplicates.

Email trails forwarded numerous times can result in a number of duplicates. You should spend time to find the latest email and remove any others that contain the same information.

A document may have been attached to a number of emails and printed out numerous times you only need to print a document once. In addition, numerous drafts of the same document do not need to be provided. The school is only required to provide the final draft of documents.

Reducing the volume of documents in this way will reduce the risk of making a mistake and sending out incorrect information.

It is good practice to produce a schedule of the documents which you have identified, which will help you organise how you work, keeping track of which documents need redacting, which are later considered not relevant etc. It is also very helpful to refer to any complaint made about the handling of the request.

What information is exempt from disclosure and needs to be removed?

- **Third party information**

A data subject is not entitled to see what we hold on any third party, including a partner or relative, unless that third party has consented. You can contact the third party and ask for their consent, and should keep a record of their response. In some circumstances we can decide to disclose without that consent e.g. if it is not possible to obtain; the information is already known to the requester or there is no prospect of harm from the disclosure. Decisions need to be made on a case by case basis.

We cannot refuse to provide access to personal data about an individual simply because it was obtained from a third party. The rules about third-party information apply only to personal data that includes information about the individual who is the subject of the request and information about someone else.

- **Exemptions**

For other personal data, there are exemptions provided by the Act (set out below) and you should familiarise yourself with these exemptions before you start to redact.

Not all of the exemptions apply in the same way, and you should look at each exemption carefully to see how it applies in a particular SAR. Some exemptions apply because of the nature of the personal data in question, e.g. information contained in a confidential reference. Others apply because disclosure of the information would be likely to prejudice a particular function of the school. The DPA does not explain what is meant by 'likely to prejudice'. However, the Information Commissioner's view is that it requires there to be a substantial chance (rather than a mere risk) that complying with the SAR would noticeably damage the discharge of the function concerned.

- **Confidentiality and references**

We do not need to disclose information which was provided to us in confidence. Whether or not information is confidential is subject to a number of defined conditions. The information needs to be confidential in nature and provided in circumstances which create an expectation of confidentiality. Something simply being marked "Confidential" does not make it confidential, if the information is not actually confidential in nature.

If information is widely known elsewhere, it cannot be considered confidential, and the passage of time may mean that the confidential nature of information has elapsed.

Where something may be confidential, we should ask the person whose information it is, whether they consent to the disclosure, and keep a record of that. In some circumstances, set out above, we may decide that we should disclose the information.

You may give or receive references about an individual, e.g. in connection with their employment, or educational purposes. Such references are often given 'in confidence', but that fact alone does not mean the personal data included in the reference is exempt from subject access.

The DPA distinguishes between references we give and references we receive. References we give are exempt from subject access if we give them in confidence and for the purposes of an individual's education, training or employment or the provision of a service by them.

There is no such exemption for references we receive from a third party. If we receive a SAR relating to such a reference, we must apply the usual principles about subject access to decide whether to provide some or all of the information contained in the reference.

If a question of confidentiality arises, you should contact the author to find out whether they object to the reference being disclosed and, if so, why.

Even if the provider of a reference objects to its disclosure in response to a SAR, we will need to supply the personal data it contains to the requester if it is reasonable to do so in all the circumstances. You will therefore need to weigh the referee's interest in having their comments treated confidentially against the requester's interest in seeing what has been said about them. Relevant considerations are likely to include:

- Any clearly stated assurance of confidentiality given to the referee;

- Any reasons the referee gives for withholding consent;
- The likely impact of the reference on the requester;
- The requester's interest in being able to satisfy himself or herself that the reference is truthful and accurate; and
- Any risk that disclosure may pose to the referee.

- **Publicly available information**

If the law says we must make information available to the public, any personal data included in it is exempt from the right of subject access.

The exemption only applies to the information that we are required to publish. If it holds additional personal data about an individual, the additional data is not exempt from the right of subject access.

- **Crime and taxation**

Personal data processed for certain purposes related to crime and taxation is exempt from the right of subject access. These purposes are:

- The prevention or detection of crime;
- The capture or prosecution of offenders; and
- The assessment or collection of tax or duty.

However, the exemption applies only to the extent that complying with a SAR would be likely to prejudice the crime and taxation purposes set out above. You need to judge whether or not this is likely in each case – you should not use the exemption to justify denying subject access to whole categories of personal data if for some individuals the crime and taxation purposes are unlikely to be prejudiced.

Personal data that is (1) processed for the purpose of discharging statutory functions and (2) consists of information obtained for this purpose from someone who held it for any of the crime and taxation purposes described above is also exempt from the right of subject access.

This is only to the extent that providing subject access to the personal data would be likely to prejudice any of the crime and taxation purposes. This prevents the right applying to personal data that is passed to statutory review bodies by law-enforcement agencies, and ensures that the exemption is not lost when the information is disclosed during a review.

Section 29(4) of the DPA provides an additional exemption from the right of subject access that is designed to prevent the right being used to force relevant authorities to disclose information about the operation of crime detection and anti-fraud systems, where such disclosure may undermine the operation of those systems.

- **Management information**

A further exemption applies to personal data that is processed for management forecasting or management planning. Such data is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the business or other activity of the organisation.

- **Negotiations with the requester**

Personal data that consists of a record of your intentions in negotiations with an individual is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the negotiations.

- **Regulatory activity**

This exemption only applies to personal data processed for core regulatory activities, and then only to the extent that granting subject access to the information concerned would be likely to prejudice the proper discharge of those functions.

- **Health and education records**

The exemptions that may apply when a SAR relates to personal data included in health and education records are explained in chapter 10 of the code.

'The Secretary of State may, by order, exempt certain personal data required for the purposes of health, education, social work from the subject information provisions or modify those provisions in relation to this personal data. [see note 10]'

- **Other exemptions**

The exemptions mentioned above are those most likely to apply in practice. However, the DPA contains additional exemptions that may be relevant when dealing with a SAR.

For more information about exemptions, contact the Complaints and Information Governance team on 6398 or by emailing GDPR@luton.gov.uk or see the ICO Guide to Data Protection – How to disclose information safely

How do I complete redactions?
Much of the data we hold and which needs to be provided in response to an SAR, may contain information which is not the personal data of the data subject or is covered by an exemption and not to be disclosed.

Where the personal data that needs to be disclosed is contained within the same document that the exempt information you need to redact. Redaction is the process of blocking out information so that the data subject cannot read it. Most redaction is done by covering the exempt information with a dark black line.

When you redact a document or remove exempt information you should make notes on the redaction template providing a description of the document and the reason for the redaction/removal, using the redaction template. Redaction can be completed using the following methods:

- Cover large blocks of text with plain paper - If there are large blocks of information to be redacted you can cover these with plain paper before photocopying. The original copy should be destroyed using confidential waste.
- Manual redaction – This is useful were there are only small pieces of text that need to be removed. Manual redaction can be done using an indelible black marker to cover the relevant text. NOTE: be careful that you have covered the text completed by holding the document to the light. Often a document redacted manually needs to be re copied to ensure that the marked text cannot be read. Also note that manual redaction can only be done on single sided copies.
- Redaction using specialist software – this type of reaction is useful when you need to large pieces of text on a large SAR. Adobe redaction software or Rapid Redact are available.

NOTE: redaction should not be done using Word as this can be removed by the data subject, thereby making us responsible for a data breach as we would not have put in place adequate security measures when releasing the data.

What is a double check?
Once you are satisfied that the documents are ready for despatch to the data subject you must get your Business Manager to complete a double check of the SAR.

This is done to ensure that all third party or other exempt data has been removed appropriately and that any documents have been redacted correctly.

Third party data sent out in error to the wrong person constitutes a data breach under the Data Protection Act 2018 and can have very serious consequences for the school (see section 5 of the SAR policy).

You should ask your Business Manager to do a double check of the information you are providing to the data subject. Provide your Business Manager with copies of the documents ready for despatch and a copy of the original SAR request. This double check must be done within the time limits allowed for the SAR and therefore must be built into the process.

NOTE: Occasionally schools will outsource the redaction of SARs to a third party provider such as LBC's IG team a solicitor or barrister. A double check of the work completed must be carried out by the [Business Manager] before any documents are sent out to the data subject. This is to ensure that the work is completed to the standards expected by the school.

How do I respond to a SAR?
Once all of the information has been collated (duplicates and third party information has been removed or redacted and a double check has been carried out) the SAR is ready for despatch.
The school is required to provide copies in a format requested by the data subject.

- Do not provide original documents only copies
- Always keep a copy of the documents provided to the SAR. Best practice is to add the documents to a file alongside the original request.
- Remember if you have scanned the documents into a shared folder you should delete them as soon as they have been moved to their new secure location. This is to ensure that unauthorised parties do not gain access.

You can then send the documents securely using the following methods:

Requested by:	Method:
Hard copy	Documents should be hand delivered to the data subject wherever possible. Check ID and address for sending before handing over documents. Make sure that the documents are securely contained in a sealed envelope. If it not possible for the data subject to collect the documents themselves use the **special delivery service** and include the name of the data subject on the envelope to ensure that they sign for the documents. **NOTE**: Check you have the correct address before posting
Encrypted device	Where the data is especially sensitive you may want to consider saving the documents on a password protected, encrypted memory device rather than posting hard copies. You can send the password to the data subject once they have received the device by post to ensure that only they have access.
Email	If the school has a secure email system this is the school's preferred method. Scan a copy of the file and move it to a secure location on the network. Send the file by secure data transfer (currently Egress). Ask the data subject to confirm receipt of the documents as soon as possible

NOTE: If any of the data goes missing or the data subject complains about the data sent out refer to the school's data breach policy immediately. If you have used Egress or similar to send the data you can revoke access at any time to stop the data file from being opened or shared.

Complaints
For information on how data subjects can complain about a SAR refer to section 15 of the SAR Policy

Further information

If you need any more information about this procedure or any other aspect of Subject Access requests, please contact us.

Complaints and Information Governance
Luton Borough Council
Town Hall
Luton
Bedfordshire
LU1 2BQ

Email: GDPR@luton.gov.uk
Phone: 01582 546398