# Forres Sandle Manor (Non-Academic) Policy

| | |
|---|---|
| Policy Title | **Data Protection Policy** |
| Policy Lead (Appointment (& Initials)) | **Bursar (CIJ)** |
| Date of Last Review | **May 2018** |
| Date of Next Review | **May 2020** |

## DATA PROTECTION POLICY

### FSM COMMITMENT

- FSM is committed to the protection of all personal and sensitive data for which it holds responsibility as the ***Data Controller*** and the handling of such data in line with the data protection principles and the Data Protection Act (DPA). As GDPR[1] continues to mature, changes to data protection legislation from time to time will be monitored and implemented in order to stay compliant with any developing requirements.

- Glossary. A glossary of key *data protection* terms is tabled at Appendix 1.

### DATA PROTECTION RESPONSIBILITIES

- The Data Protection Officer (DPO) (Bursar) has overall responsibility for data protection at FSM. However, all staff must treat all pupil, parent and staff information in a confidential manner and follow the guidelines as set out in this policy document.

- FSM is also committed to ensuring that its staff are aware of the data protection policies and legal imperatives. Sufficient training and briefing will be provided to them.

- The requirements of this policy are mandatory for all staff employed by FSM and any 3rd party contracted to provide services within the school.

### ICO REGISTRATION

- FSM's data processing activities are registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller (Registration Number Z8494481). Any changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the ICO Register.

- FSM's entry on the Register is attached at Appendix 2 to this policy.

[1] GDPR: General Data Protection Regulations.

- Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

## LEGAL BASES FOR PROCESSING DATA

- FSM's legal bases for processing data are:
    - **Consent**. The member of staff, pupil or parent has given clear consent to FSM to process their personal data for a specific purpose.
    - **Contract**. The processing is necessary for the obligations of the parental contract with FSM, a member of staff's employment contract or a 3rd party supplier.
    - **Legal Obligation**. The processing is necessary for FSM to comply with the law (excluding contractual obligations).
    - Other legal bases are shown at Appendix 3.

## PERSONAL, SENSITIVE DATA AND INDIVIDUAL RIGHTS

- All data within FSM's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

- The definitions of personal and sensitive data are shown at Appendix 2 to this Policy as published by the ICO.

- As well setting out different bases for processing personal data, GDPR includes a number of individual rights. These are listed at Appendix 4.

## PRINCIPLES OF THE DATA PROTECTION ACT

- The principles of the Data Protection Act shall be applied to all data processed:
    - ensure that data is fairly and lawfully processed
    - process data only for limited purposes
    - ensure that all data processed is adequate, relevant and not excessive
    - ensure that data processed is accurate
    - not keep data longer than is necessary
    - process the data in accordance with the data subjects rights
    - ensure that data is secure
    - ensure that data is not transferred to other countries without adequate protection

## FSM PRIVACY NOTICE AND FAIR PROCESSING

- FSM will be transparent about the processing of data and notify these intentions to the parent body, pupils and FSM Staff through the **FSM Privacy Notice**.

- There may be circumstances where FSM is required either by law or in the best interests of our students or staff to pass information onto 3rd parties, for example local authorities, ISI, DfE or the Department of Health. These authorities have their own policies relating to the protection of any data that they receive or collect.
- The intention to share data relating to individuals to an organisation outside of FSM will be clearly defined within notifications and details for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

- Any proposed change to the processing of an individual's data **shall first be notified to them**. Consent will always be sought when FSM discloses information or data:

    - that would cause serious harm to the child or anyone else's physical or mental health or condition
    - indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
    - recorded by the pupil in an examination
    - that would allow another person to be identified, or identifies another person or a local authority as the information source unless consent has been given, or it is judged reasonable in the circumstances to disclose the information without consent. The immunity from disclosure does not apply if the information can be edited so that the source name or identifying details are removed
    - in the form of a reference given to another school or any other place of education and training.

## DATA SECURITY

- In order to assure the protection of all data being processed and update decisions on processing activities, FSM will undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

- Risk and impact assessments shall be conducted in accordance with guidance given by the ICO under GDPR Principle 7 (Security)[2].

- Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

[2] ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

- The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

## DATA ACCESS REQUESTS (SUBJECT ACCESS REQUESTS (SAR))

- All individuals whose data is held by FSM , have a legal right to request access to such data or information about what is held. FSM will respond to such requests within **one month**. Evidence of identity will need to be established.

- The requests should be sent in in writing to:

  Roger Dutton
  The Bursar
  Forres Sandle Manor School
  Fordingbridge
  Hampshire SP6 1NS

- A flowchart to assist in correctly complying with a SAR is at Appendix 5 to this Policy.

- FSM reserves the right to charge a fee for this work for requests that are judged to be excessive.

- Personal data about pupils will not be disclosed to 3rd parties without the consent of the pupil's parent or carer, unless it is obliged by law or in the best interest of the child. With that in mind, data may be disclosed to the following 3rd parties <u>without consent</u>:

| | |
|---|---|
| Other schools | If a pupil transfers from FSM to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This supports a smooth transition from FSM to the next and ensures that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the pupil's academic progress as a result of the move |
| Examination authorities | This may be for registration purposes, to allow FSM pupils to sit examinations set by external exam bodies |
| Health authorities | As obliged under health legislation, FSM may pass on information regarding the health of children to monitor and avoid the spread of contagious diseases in the interest of public health |
| Police and courts | If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered |
| Social workers and support agencies | In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies |

| | |
|---|---|
| Educational provision | Schools may be required to pass data on in order to assist the DfE to monitor the national educational system and enforce laws relating to education |

## PHOTOGRAPHS AND VIDEO

- Images of staff and pupils may be captured at appropriate times and as part of educational activities for use at FSM only.

- Unless prior consent from parents/pupils/staff has been expressly given, FSM shall not utilise such images for publication or communication to external sources.

- It is FSM's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

## LOCATION OF INFORMATION AND DATA

- Hard copy data, records, and personal information are stored out of sight and in locked cupboards. The cupboard keys are secured in wall blister safes, the combinations of which are known only to those that need to know them. This includes medical information, stored in the Matrons' Surgery, which might require immediate access at any time, day or night.

- Sensitive or personal information and data should not be removed from the FSM site. However, FSM acknowledges that some staff may need to transport data between FSM and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have off-site meetings, or are on school visits with pupils.

- Taking **Personal** Data Offsite. The following guidelines are in place for staff to reduce the risk of personal data being compromised:

    - Paper copies of data or personal information should not be taken off the FSM site. If these are misplaced they are easily accessed. If it is not possible to avoid taking a paper copy of data off the FSM site, the information should not be on view in public places, or left unattended under any circumstances.
    - Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes make reference to any identifiable staff member, pupil or parent.
    - Extreme care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
    - If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
    - If it is necessary to transport data away from FSM, it is to be downloaded onto a USB stick or portable hard drive. The data should not be transferred from the stick

or portable hard drive onto any home or public computers. Work should be edited from the USB/portable hard drive, and saved onto them only.

- Without exception, every USB stick and portable hard drive used by FSM staff is to be password protected by BitLocker Device Encryption. There will be no latitude over this direction. This will be clearly communicated to all FSM staff, and any individual who is found to be deliberately breaching this conduct will be disciplined in line with the seriousness of their misconduct.

**DATA DISPOSAL**

- FSM recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

- All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

- All data shall be destroyed or eradicated to agreed levels that meet recognised national standards, with confirmation at completion of the disposal process.

- Disposal of IT assets holding data will be overseen by Director ICT through a qualified source for disposal of IT assets and collections in compliance with ICO guidance[3].

Appendices:

1. GDPR – Glossary of Data Protection Terms.
2. FSM Registration with ICO.
3. Legal Basis and Conditions for Processing Information.
4. Individual Rights under GDPR.
5. Subject Access Request (SAR) Flowchart.

[3] ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

# GDPR – GLOSSARY OF DATA PROTECTION TERMS

| | |
|---|---|
| Information Commissioner's Office (ICO) | UK's independent body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. For more information, visit: https://ico.orq.uklabout-the-ico/ |
| Article 29 Working Party | Short name for the Data Protection Working Party established by the European Commission to provide independent advice on data protection matters and help in the development of harmonised policies for data protection in the EU member states |
| General Data Protection Regulations (GDPR) | Legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). |
| Data Protection Bill | Updates data protection laws in the UK, supplementing the GDPR, as well as extending data protection laws to areas which are not covered by the GDPR. It is likely to come into force later this year (2018), although it was meant to take effect alongside GDPR. |
| Privacy and Electronic Communications Regulations (PECR) | Sits alongside the current Data Protection Act (and in the future the Data Protection Bill/GDPR) to give individuals specific privacy rights in relation to electronic communications, including marketing calls, e-mails, texts and faxes |
| ePrivacy regulation | New EU regulation which aims to update the EU's existing e-Privacy framework in light of GDPR and is likely to come into force later this year (2018). |
| Personal data | Information relating to a living individual who can be directly or indirectly identified from it. This include name, address, contact details but could also include two or more non-specific pieces of information that when combined could identify specific individuals, including for example, a combination of gender, birth rate, geographic indicator and descriptors. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. |
| Processing personal data | Means doing something with personal data - this includes personal data acquisition, processing, storage and disposal. |
| Special categories of personal data | Data relating to highly sensitive pieces of information about an individual, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric information, health and a natural person's sex life or sexual orientation. It no longer includes criminal records or allegations, but these are similarly regulated under the Data Protection Bill. |

| | |
|---|---|
| Data Controller | A controller determines the purposes and means of processing personal data. It is possible to have more than one data controller responsible for the same set of data, i.e. a school and alumni association. This may be as independent or joint data controllers: the latter requires more paperwork and regulatory compliance, but the data sharing between the two should be regulated by contract in either case. |
| Data Processor | Responsible for processing personal data on behalf of a controller. An example may be an IT provider or payroll processor. |
| Data audit/data asset register | Assessment of data held by an organisation, in relation to its purpose. |
| Data Protection Impact Assessment (DPIA) | A process which aims to identify and minimise the risks to an individual's privacy. You must do a DPIA for certain types of processing, but also if your processing is likely to result in a high risk to individuals' privacy rights. |
| Information Governance Management Organisation (IGMO) | the overarching data governance and management organisation in a school. |
| Data Protection Officer (DPO) | An individual responsible for monitoring internal compliance. Whilst independent schools may not need to appoint a DPO, all schools should have a data lead, responsible for informing and advising on data protection obligations. |
| Data Handler | Member of staff (or volunteer) within an organisation who is responsible for processing personal data; this could be obtaining, recording or holding the data or carrying out any operation or set of operations on the data. |
| Data Subject | The person that the data relates to. |
| Data Stream | Data relating to a group of individuals within a school community, for example pupils, alumni or staff. |
| Data Set | : is a specific segment or collection of data within a data stream, for example year 7 pupils, alumni from years 2000-2010 or teaching staff. |
| Lawful basis for processing | The specific reasons, set out in law, for which you can process personal data |
| Consent | One of the six lawful bases for processing. Consent is when an individual has freely given clear, informed consent for you to process their personal data for a specific purpose. Under GDPR, consent must be a freely given, specific, informed and unambiguous indication of the individual's wishes. |
| Legitimate interests | One of the six lawful bases for processing. An organisation can rely on legitimate interests when the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data -which overrides thoe legitimate interests. Legitimate interest is the most flexible lawful basis for -processing personal data and is likely to be most appropriate where you are using personal data in |

| | |
|---|---|
| | ways that individuals would reasonably expect and where it has a minimal impact on their privacy. However, to be lawful it does require a prior data risk assessment and specific inclusion within the Privacy Notice. |
| Legitimate Interests Assessment (LIA) | A test carried out by a data controller to decide if they can rely on legitimate interests as the lawful basis for processing personal data. |
| Privacy Notice | A document that explains how you will process an individual's personal data and should include, why you hold data, what data you hold, how you process this, if this data is shared with any other organisations and what rights the individual has. |
| Direct marketing | The promotion of an organisation's aims and ideals, as well as the sale of products and services. |
| Prospect research | Used to learn more about existing or potential donors' backgrounds and their propensity and capacity to give. |
| Wealth screening | A specific form of prospect research which looks at indicators of wealth to understand existing or potential donors' capacity to give. |
| Telephone Preference Service (TPS) | A central opt out register whereby individuals can register their wish not to receive unsolicited sales and marketing telephone calls. It is relevant under PECR as consent is needed to make contact with individuals via telephone numbers registered with the TPS. |
| Subject Access Request (SAR) | is where an individual requests access to the information you hold about them. |
| Data Breach | When there is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Where they reach a certain threshold of likely harm, these will have to reported to the ICO and in some cases those individuals affected |
| Data sharing | The disclosure of data from one or more organisations to a third-party organisation or organisations, so within the context of a school this could be sharing data an ongoing basis with an alumni organisation or could be sharing personal data to a mail-house on a one-off occasion. The data sharing may happen between one or more data controllers, and routine or regular data sharing ought to be captured in a data sharing agreement. Please note that providing data to a data processor to carry out services on the school's behalf is not considered "sharing" in this sense, but must be regulated by a special type of binding contract. |

**FORRES SANDLE MANOR (FSM)**
**REGISTRATION WITH INFORMATION COMMISSIONER'S OFFICE (ICO)**
**REGISTRATION NUMBER Z8494481**

- Nature of Work - Private School

- Description of processing: *The following is a broad description of the way FSM processes personal information. To understand how personal information is processed individuals may need to refer to any personal communications received, check any privacy notices FSM has provided or contact FSM to ask about personal circumstances*.

    - Reasons/purposes for processing personal information: We process personal information to enable us to:
        - provide education and training conducted outside the State system,
        - welfare and educational support services,
        - administer school property and library services,
        - maintain our own accounts and records,
        - provide administration in connection with boarding and the organisation of alumni associations and events and to support and manage our staff.

    - Our processing also includes the use of CCTV to maintain the security of the premises and for preventing and investigating crime.

    - Type/Classes of personal information processed: We process personal information relevant to the above reasons/purposes. This may include:

        - personal details
        - family details
        - lifestyle and social circumstances
        - financial details
        - education and employment details
        - disciplinary and attendance records
        - vetting checks
        - visual images
        - personal appearance and behaviour

    - We also process sensitive classes (special category data) of personal information that could include:

        - physical or mental health details
        - sexual life or sexual orientation
        - health
        - politics
        - racial or ethnic origin

- biometrics (when used for ID purposes)
- religious or other beliefs
- trade union membership
- information relating to offences or alleged offences

- We process personal information about:

  - employees
  - pupils and students
  - professional advisers and consultants
  - governors
  - services providers and suppliers
  - complainants, enquirers
  - individuals captured by CCTV images

- Sharing Personal Information.

  - We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA).

  - We may need to share some of the personal information we process with other organisations for one or more reasons:
    - educators, careers and examining bodies
    - staff, students and governors
    - current, past and prospective employers
    - family, associates and representatives of the person whose personal data we are processing
    - central and local government
    - healthcare professionals, social and welfare organisations
    - police, courts, tribunals and security organisations
    - voluntary and charitable bodies
    - the media
    - financial organisations
    - suppliers
    - service providers
    - professional advisers

  - Transfers. It may sometimes be necessary to transfer personal information overseas. When this is needed information is only shared within the European Economic Area (EEA). Any transfers made will be in full compliance with all aspects of the data protection act.

## GDPR – LAWFUL BASIS AND CONDITIONS FOR PROCESSING INFORMATION

The lawful basis for processing personal data are set out in Article 6 of the General Data Protection Regulation (GDPR).

At least one of these must apply whenever personal data is processed:

| | |
|---|---|
| Consent | The individual has given clear consent for you to process their personal data for a specific purpose. |
| Contract | The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. |
| Legal obligation | The processing is necessary for you to comply with the law (not including contractual obligations). |
| Vital interests | The processing is necessary to protect someone's life |
| Public task | The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. |
| Legitimate interests | The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. This cannot apply if you are a public authority processing data to perform your official tasks. Public authorities will need to rely on official functions. |

## INDIVIDUAL RIGHTS UNDER GDPR

As well as setting out the different bases for processing personal data, GDPR also includes a number of *rights for individuals* which need to be considered:

- **The Right to be Informed** - GDPR is more specific about the information you need to provide to individuals about what you do with their personal data, and whether or not you collect the information from them directly. You must provide this in a way that is easy to access, read and understand. This is where Privacy Notices come in.

- **The Right of Access** - under GDPR, individuals will have the right to obtain confirmation that their data is being processed and access to their personal data. You must provide a copy of the information free of charge (unless a request is clearly excessive or unfounded), within one calendar month of the request.

- **The Right to Rectification** - GDPR includes a right for individuals to have inaccurate data rectified, and if a request is made you have one calendar month to respond

- **The Right to Erasure** - GDPR introduces a new right, the right to erasure (sometimes called **the Right to be Forgotten**). Such a request can be made in writing or verbally and should be responded to within one calendar month. There are however, certain circumstances when the right to erasure will not apply.

- **The Right to Restrict Processing** - this is an alternative to the right to erasure and offers individuals the opportunity to restrict how their personal data is processed; for example where personal data is inaccurate or an individual wants to limit how an organisation uses their data. Again, a request can be made in writing or verbally and should be responded to within one calendar month.

- **The Right to Data Portability** - this allows an individual to obtain and reuse their personal data for their own purposes across different services.

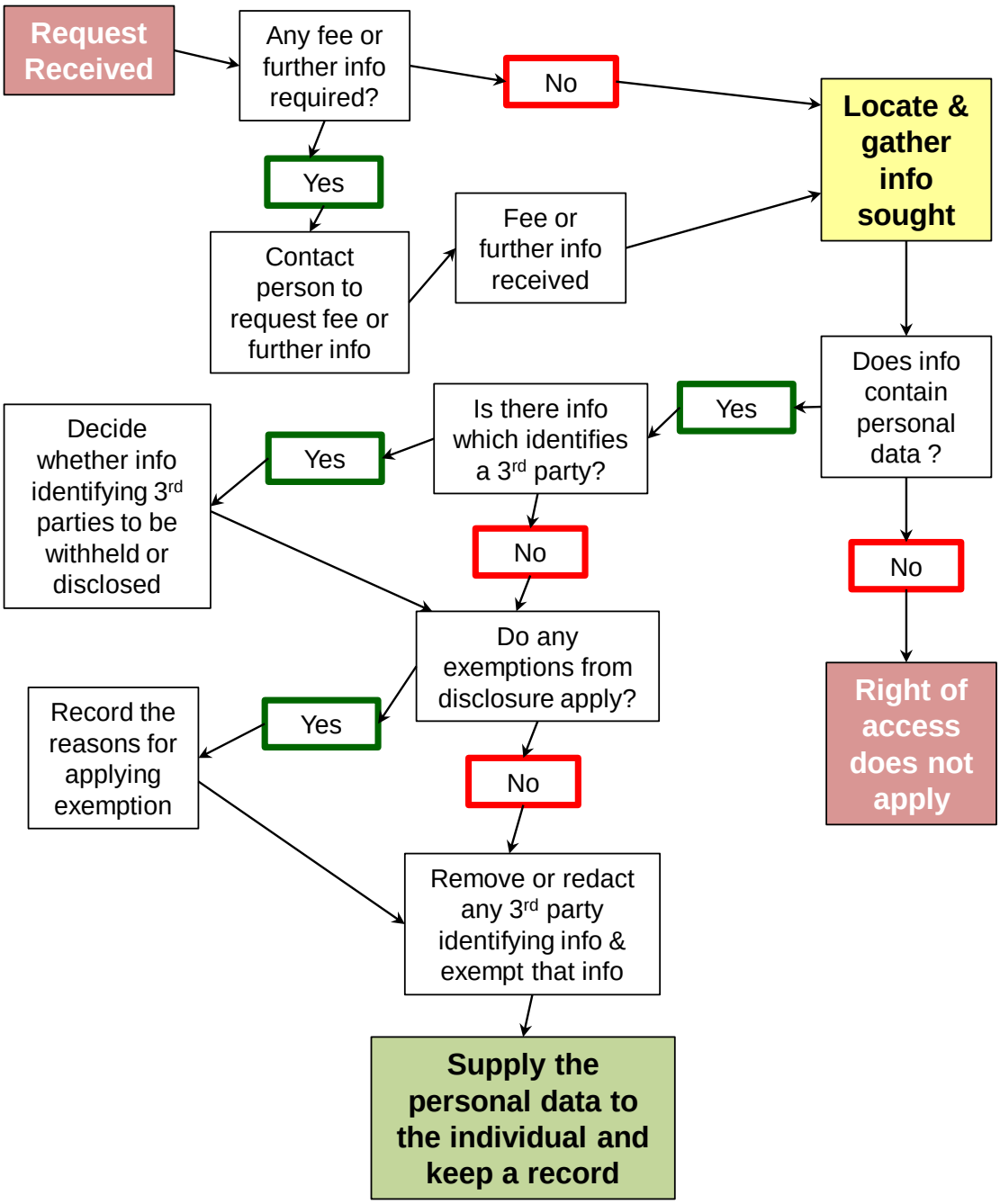
- **The Right to Object (including objecting to direct marketing)** - individuals have the right to object to processing of their personal data based on legitimate interests (to 'opt out) or the performance of a task in the public interest/exercise of official authority. This includes processing of personal data for the purpose of direct marketing, profiling and scientific/historic research and statistics.

- **The Right to Withdraw Consent** - where consent is relied on. This does not mean that any processing previously carried out in reliance on that consent becomes unlawful, or must necessarily always be rectified, but the withdrawal must be respected.

- **Rights in Relation to Automated Decision Making and Profiling** - under GDPR, you can only carry out automated decision making or automated processing of personal data (without any human involvement), including profiling them, where this type of decision-making is necessary for a contract, authorised by Union or Member state law or based on the individual's consent.

# Subject Access Request (SAR) Flowchart

## Complying with a SAR Request




SAR Request