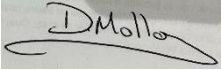
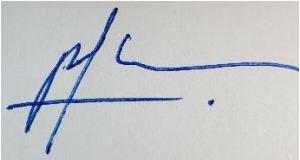




# First **Star** Scholars **UK**

## Data Protection Policy

<b>Date of Last Review</b>	<b>29/10/2024</b>
<b>Review Cycle</b>	<b>Annually</b>
<b>Date (Month/Year) of Next Review</b>	<b>10/2025</b>
<b>Date Policy was Ratified</b>	<b>29/10/2024</b>
<b>Named Lead for Writing/Review</b>	<b>Emily Hollis MBE</b>
<b>Signed:</b>	<b>Date</b>
<b>CEO</b>	<b>29/10/24</b>
	
<b>FSSUK Board of Trustees – Chair</b>	
	

## Introduction and Scope

This policy outlines First Star Scholars UK's (the charity) commitment to data protection and compliance with the UK Data Protection Act, 2018. The purpose of this policy is to ensure that all personal data held by the charity is processed lawfully, fairly, and transparently, and that the rights of data subjects are protected. This policy applies to all individuals working on behalf of the charity, including trustees, staff, and volunteers.

The charity will ensure that all personal data that it holds will be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

## Data Protection Lead/Officer

The charity has a Data Protection Lead/Officer who will be responsible for overseeing data protection and leading on any incident investigation and reporting. The Data Protection Lead/Officer (DPO) will also ensure that all staff and volunteers are provided with any induction, on the job or other training and made aware of their data protection responsibilities. The DPO at the charity is the Director of Operations. They can be contacted via: [info@firststaruk.org](mailto:info@firststaruk.org)

## Data Protection

Data protection is the practice of safeguarding personal information by applying data protection principles and complying with the Data Protection Act. The Data Protection Act is a UK law that regulates the processing of personal data. The UK Information Commissioner's Office (ICO) provides guidelines on data protection that the charity will follow.

UK GDPR: The UK General Data Protection Regulation, which outlines the rules for processing personal data in the UK.

Data Processor: An individual or organisation that processes personal data on behalf of a data controller. We do not knowingly outsource any of our data processing to a third party except as provided in the section 'Third party access to data'.

Data Controller: An individual or organisation that determines how and why personal data is processed. The Director of Operations and the Board of Trustees act as the data controllers for the charity.

Data Subject: An individual whose personal data is being processed.

Processing: Any operation performed on personal data, including collection, storage, use, and disclosure.

Personal Data: Any information that can identify a living individual, such as name, address, or email address.

Sensitive Personal Data: Personal data that requires extra protection, such as health information or ethnic origin.

Direct Marketing: Any communication aimed at promoting a product or service directly to an individual.

PECR: The Privacy and Electronic Communications Regulations, which govern electronic direct marketing.

Valid Consent: Consent given freely, specifically, and informed, and can be withdrawn at any time.

Legitimate Business Purpose: A lawful reason for processing personal data that is necessary for the legitimate interests of the data controller or a third party.

## **Data Protection Principles**

Data is:

- Processed lawfully, fairly and in a transparent manner
  - There are several grounds on which data may be collected, including consent.
  - We are clear that our collection of data is legitimate, and we have obtained consent to hold an individual's data, where appropriate.
  - We are open and honest about how and why we collect data and individuals have a right to access their data.
- Collected for specified, explicit and legitimate purposes and not used for any other purpose
  - We are clear on what data we will collect and the purpose for which it will be used.
  - We only collect data that we need.
  - When data is collected for a specific purpose, it may not be used for any other purpose, without the consent of the person whose data it is.
- Adequate, relevant and limited to what is necessary
  - We collect all the data we need to get the job done.
  - And none that we don't need.
- Accurate and, where necessary, kept up to date
  - We ensure that what we collect is accurate and have processes and/or checks to ensure that data which needs to be kept up-to-date is, such as beneficiary, staff or volunteer records.
  - We correct any mistakes promptly.
- Kept for no longer than is necessary
  - We understand what data we need to retain, for how long and why.
  - We only hold data for as long as we need to.

- That includes both hard copy and electronic data.
- Some data must be kept for specific periods of time (eg accounting, HSE, HR).
- We have some form of archive process that ensures data no longer needed is destroyed.
- Processed to ensure appropriate security, not only to protect against unlawful use, but also loss or damage
  - Data is held securely, so that it can only be accessed by those who need to do so. For example, paper documents are locked away, access to online folders in shared drives is restricted to those who need it, IT systems are password protected, and/or sensitive documents that may be shared (e.g. payroll) are password protected.
  - Data is kept safe. Our IT systems have adequate anti-virus and firewall protection that is up-to-date. Staff understand what they must and must not do to safeguard against cyber-attack, and that passwords must be strong and not written down or shared.
  - Data is recoverable. We have adequate data back-up and disaster recovery processes.

## **Individual Rights**

We recognise that individuals' rights include the right to be informed, of access, to rectification, erasure, restrict processing, data portability and to object.

## **Use of Imagery/Video**

All imagery is protected by copyright and cannot be used without the consent of the owner, usually the person who took the image. We will also need consent from the individuals in images of individuals and small groups, which may well fall within the Data Protection Act.

We will only ever use an image where consent has been received from all parties, always erring on the side of caution. Particular care is to be taken when using images of children or other vulnerable people.

## **Data Breach**

A breach is more than only losing personal data. It is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

We will investigate the circumstances of any loss or breach, to identify if any action needs to be taken. Action might include changes in procedures, where there will help to prevent a re-occurrence or disciplinary or other action, in the event of negligence.

We will notify the ICO within 72 hours of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals. For example:

- Result in discrimination

- Damage to reputation
- Financial loss
- Loss of confidentiality or any other significant economic or social disadvantage

## **Children**

People under 13 years of age are not legally able to give consent. Privacy notices, or other information we give them is written and presented in a way that is understandable and fair. Where consent is required, for example, with use of image, we would seek consent from parents/carers or social worker as required.

## **Vulnerable Groups**

We work with people who may be particularly at risk and therefore include additional provisions to protect them.

Some people are unable, or may be unable to give consent, and this must be obtained from the person who is able to make decisions on their behalf, such as a Lasting Power of Attorney. Any decisions made on their behalf, must always be in their best interests.

## **Special Category Data**

Special category (sensitive) data is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, health or sexual orientation.

The UK GDPR defines special category data as:

- 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
- genetic data
- biometric data (where used for identification purposes – N/A in our setting)
- data concerning health
- data concerning a person's sex life (N/A in our setting)
- data concerning a person's sexual orientation

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply. For further information, please see our separate guidance on criminal offence data.

Special category data includes personal data revealing or concerning the above types of data. Therefore, if you have inferred or guessed details about someone which fall into one of the above categories, this data may count as special category data. It depends on how certain that inference is, and whether you are deliberately drawing that inference.

## Conditions for processing special category data

Article 9 lists the conditions for processing special category data:

- a) Explicit consent
- b) Employment, social security and social protection (if authorised by law)
- c) Vital interests
- d) Not-for-profit bodies
- e) Made public by the data subject
- f) Legal claims or judicial acts
- g) Reasons of substantial public interest (with a basis in law)
- h) Health or social care (with a basis in law)
- i) Public health (with a basis in law)
- j) Archiving, research and statistics (with a basis in law)

If an organisation is relying on conditions (b), (h), (i) or (j), you also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.

If an organisation is relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

The charity processes special category data for conditions:

a, b, d, f, g, j

Special category data is obtained with explicit consent where possible and appropriate.

## What are the substantial public interest conditions?

The 23 substantial public interest conditions are set out in paragraphs 6 to 28 of Schedule 1 of the DPA 2018:

1. Statutory and government purposes
2. Administration of justice and parliamentary purposes
3. Equality of opportunity or treatment
4. Racial and ethnic diversity at senior levels
5. Preventing or detecting unlawful acts
6. Protecting the public
7. Regulatory requirements
8. Journalism, academia, art and literature
9. Preventing fraud
10. Suspicion of terrorist financing or money laundering
11. Support for individuals with a particular disability or medical condition
12. Counselling
13. Safeguarding of children and individuals at risk
14. Safeguarding of economic well-being of certain individuals
15. Insurance

16. Occupational pensions
17. Political parties
18. Elected representatives responding to requests
19. Disclosure to elected representatives
20. Informing elected representatives about prisoners
21. Publication of legal judgments
22. Anti-doping in sport
23. Standards of behaviour in sport

The charity processes special category data based on substantial public interest conditions:

1, 3, 4, 5, 6, 7, 8, 9, 11, 13, 14, 15, 16, 19, 20

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an organisation to have an Appropriate Policy Document (APD) in place. (See Schedule 1 paragraphs 1(1)(b) and 5).

Please refer to our APD for further information.

## **International Data Transfers**

This refers to the movement of personal data from one country to another, particularly when such data is subject to data protection laws.

### Legal Basis for Transfer

1. Adequacy Decisions: Transfers may occur to countries recognised by the Relevant Authority (e.g. the EU) as providing an adequate level of data protection.
2. Appropriate Safeguards: In cases where the receiving country does not have an adequacy decision, data transfers must include appropriate safeguards, such as:
  - Standard Contractual Clauses (SCCs)
  - Binding Corporate Rules (BCRs)
  - Other legal mechanisms approved by the relevant data protection authority.

Risk Assessment - Prior to any international data transfer, a risk assessment must be conducted to evaluate:

- The legal framework of the destination country concerning data protection.
- The specific risks associated with the transfer, including the potential for unauthorized access or data breaches.

## Data Transfer Procedures

1. Documentation: All international data transfers must be documented, including the legal basis for the transfer and any safeguards implemented.
2. Data Processing Agreements: When engaging third-party processors located in another jurisdiction, a Data Processing Agreement (DPA) must be in place to ensure compliance with data protection obligations.
3. Training: Staff involved in international data transfers must receive training on data protection requirements and the importance of safeguarding personal data.

The charity will regularly review and update its international data transfer practices to ensure compliance with evolving legal standards and best practices. Any breaches or issues related to international data transfers must be reported immediately to the Data Protection Officer (DPO).

## **Privacy and Electronic Communications**

Known as PECR, there are special regulations covering electronic marketing messages (by phone, fax, email or text), cookies and electronic communication services to the public.

PECR are the Privacy and Electronic Communications Regulations. Their full title is The Privacy and Electronic Communications (EC Directive) Regulations 2003.

They are derived from European law. PECR implement European Directive 2002/58/EC, also known as 'the e-privacy Directive'.

The e-privacy directive complements the general data protection regime and sets out more specific privacy rights on electronic communications. It recognises that widespread public access to digital mobile networks and the internet opens up new possibilities for businesses and users, but also new risks to their privacy.

## Key Principles - PECR

1. Consent for Marketing Communications:
  - Individuals must provide clear and informed consent before receiving direct marketing communications via electronic means. This applies to emails, SMS, and automated calls.
  - Consent must be freely given, specific, informed, and unambiguous.
2. Opt-Out Mechanism:
  - All marketing communications must include an easy and clear option for recipients to opt-out or unsubscribe from future communications.
  - Opt-out requests must be processed promptly and effectively.
3. Use of Cookies:
  - The charity will comply with cookie regulations by informing users about the use of cookies on our website and obtaining consent where necessary.
  - Our website is built using WordPress. Their cookie policy can be found here: [Cookie Policy | WordPress.org English \(UK\)](#)
  - We display a message regarding cookies / privacy on our website and also within our Privacy Notices.



#### 4. Privacy Notices:

- Individuals must be informed about how their personal data will be used when collecting information for electronic communications, including the purpose of processing and their rights under data protection laws.
- Privacy notices must be easily accessible and written in clear, understandable language.
- Our privacy notices can be found on our website.

#### 5. Data Security:

- Appropriate security measures must be implemented to protect personal data during electronic communications, including encryption and secure transmission protocols.

#### 6. Record Keeping:

- The charity will maintain records of consent and marketing preferences to demonstrate compliance with PECR and facilitate audits.

### **Criminal Offence Data**

- The UK GDPR gives extra protection to the personal data of offenders or suspected offenders in the context of criminal activity, allegations, investigations, and proceedings.
- If you have official authority, you can process personal data about criminal convictions and offences, because you are processing the data in an official capacity.
- If you do not have official authority, you can only process criminal offence data if you can identify a specific condition for processing in Schedule 1 of the DPA 2018.
- You cannot keep a comprehensive register of criminal convictions, unless you do so in an official capacity.
- You must determine your condition for processing criminal offence data, or identify your official authority for the processing, before you begin the processing, and you should document this.
- You must still have a lawful basis for your processing under Article 6.

The charity obtains information via the Disclosure and Barring Service (DBS) and via a 'criminal record self-declaration' to ensure any employees are able to work with children and vulnerable adults and help us to make safer recruitment decisions. Our specific condition for processing this data as a not-for-profit (paragraph 31 of the Schedule 1 of the DPA 2018) is for the "safeguarding of children and individuals at risk" (paragraph 18 of the Schedule 1 of the DPA 2018).

Please refer to our APD for further information.

### **Fundraising**

We will ensure that our fundraising complies with the Data Protection Act and ICO guidelines and also the Fundraising Regulator guidelines including, if applicable, direct marketing and PECR. We will respect the privacy and contact preferences of our donors.

### **Fundraising preference service**

We will respect the privacy and contact preferences of our donors. We will respond promptly to requests to cease contacts or complaints and act to address their causes.

## Third party access to data

We outsource for the purpose of:

- Cloud based services
- Payroll
- IT
- Financial accounting
- HR

## Artificial Intelligence

We have adopted and comply with the Charity AI Ethics & Governance Framework and ICO AI guidance.

## Subject Access Requests (SARs)

Information pertaining to SARs can be found in Appendix A.

## Privacy Notices

The charity has appropriate Privacy Notices in place which it will make available to everyone on whom it holds and processes personal data. These can be found on our website: First Star Scholars UK – Empowering Children In Care

## Version Control - Approval and Review

Version No.	Approved by	Approval Date	Main Change	Review Period
1.0	Diarmuid Molloy	29 October 2024	New policy format approved	Annually

## Appendix A - Subject Access Requests (SARs)

Under Data Protection Law, data subjects have a general right to find out whether the charity hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the charity is undertaking.

This appendix provides guidance on how data subject access requests should be handled and on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts the charity at potentially significant risk and so the charity takes compliance with this policy very seriously.

A data subject has the right to be informed by the charity of the following:

- Confirmation that their data is being processed
- Access to their personal data
- A description of the information that is being processed
- The purpose for which the information is being processed
- The recipients/class of recipients to whom that information is or may be disclosed
- Details of the charity's sources of information obtained
- In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting them, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
- Other supplementary information.

### How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the charity process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information.

A valid SAR can be both in writing (by letter, email) or verbally (e.g., during a telephone conversation).

The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the charity hold about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

### How to Make a Data Subject Access Request

Whilst there is no requirement to do so, the charity encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the charity to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/vague the charity may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

### What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed to the Director of Operations:

[info@firststaruk.org](mailto:info@firststaruk.org)

There are limited timescales within which the charity must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

### Acknowledging the Request

When receiving a SAR the charity will notify the Director of Operations who shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

Before responding to a SAR, the charity will take reasonable steps to verify the identity of the person making the request.

In the case of current employees, this will usually be straightforward. The charity is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the charity has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data, the charity may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The charity shall let the requestor know as soon as possible where more information is needed before responding to the request. In both cases, the period of responding begins when the additional information has been received. If the charity does not receive this information, they will be unable to comply with the request.

### Requests Made by Third Parties or on Behalf of Children

The charity needs to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this

entitlement. This might be a written authority to make the request, or it might be a more general power of attorney. The charity may also require proof of identity in certain circumstances.

If the charity is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data.

Before responding to a SAR for information held about a child, the charity should consider whether the child is mature enough to understand their rights. If the charity is confident that the child can understand their rights, then the charity should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 13 years is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 13 years of age or older, then provided that the charity is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the charity will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The charity may also refuse to provide information to parents/guardians if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

### Fee for Responding to a SAR

The charity will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a

request is considered to be manifestly unfounded or unreasonable the charity will inform the requester why this is considered to be the case and that the charity will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information. If a fee is requested, the period of responding begins when the fee has been received.

### Time Period for Responding to a SAR

The charity has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the charity is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request.

The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period. Where a request is considered to be sufficiently complex as to require an extension of the period for response, the charity will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

### Information to be Provided in Response to a Request

The individual is entitled to receive access to the personal data that is processed about him or her and the following information:

- the purpose for which the data is processed;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
- to request that the charity rectifies, erases or restricts the processing of his personal data; or
- to object to its processing;
- to lodge a complaint with the ICO;
- where the personal data has not been collected from the individual, any information available regarding the source of the data;

- any automated decision the charity have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the charity is required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the charity has one month in which to respond the charity is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR. Therefore, the charity is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The charity is not allowed to amend or delete data to avoid supplying the data.

### How to Locate Information

The personal data the charity needs to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused. Depending on the type of information requested, the charity may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by the data processors;
- occupational health records;
- pensions data;
- insurance benefit information.

The charity should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

### Protection of Third Parties – Exemptions to the Right of Subject Access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The charity will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the charity does not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the charity disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the charity must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

### Other Exemptions to the Right of Subject Access

In certain circumstances the charity may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

**Crime detection and prevention:** The charity does not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

**Confidential references:** The charity does not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the charity receives from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the charity must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

**Legal professional privilege:** The charity does not have to disclose any personal data which is subject to legal professional privilege.

**Management forecasting:** The charity does not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.



Negotiations: The charity does not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

### Refusing to Respond to a Request

The charity can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the charity can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the charity needs to justify the decision and inform the requestor about the decision. The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the charity should contact the individual promptly and inform them. The charity does not need to comply with the request until the fee has been received.

### Record Keeping

A record of all subject access requests shall be kept by the Director of Operations. The record shall include the date the SAR was received, the name of the requester, what data the charity sent to the requester and the date of the response.