**INTERNAL SUBJECT ACCESS REQUEST POLICY**

**This procedure deals with the handling of subject access requests under the General Data Protection Regulation**

1. Introduction
	1. [NAME OF ORGANISATION] holds personal data about job applicants, employees, [clients], [customers], [members], suppliers, business contacts and other individuals for a variety of purposes.
	2. Under data protection law, individuals (known as **‘data subjects’**) have a general right of access to personal data which we process about them. Such a request is known as a Subject Access Request (‘SAR’).
	3. This right of access is subject to certain exceptions where personal data may be exempt from this right of access under data protection law.
	4. This procedure sets out how SARs received by [NAME OF ORGANISATION] should be dealt with.
	5. This policy provides guidance for staff members on how SARs should be dealt with, and is intended for internal use. It is not to be made routinely available to third parties.
	6. This policy is aimed primarily at those members of staff who are authorised to handle SARs. For other staff members, it provides guidance on:
		1. How to decide whether a request for information is a SAR; and
		2. What to do if you receive a SAR.
	7. A failure to comply with an SAR in accordance with data protection law could result in a significant risk to [NAME OF ORGANISATION], as such a failure to comply with this policy may lead to disciplinary action, which may result in dismissal (see section 15 below).

Handling Subject Access Requests

1. Identifying a request
	1. A SAR is a request from an individual to be given access to personal data which [NAME OF ORGANISATION] processes about them. An SAR does not need to expressly refer to personal data, any Data Protection Act, the General Data Protection Regulation or other relevant data protection law.

For example: A letter which states *‘please provide me with a copy of all the information that you have about me’* will be an SAR.

* 1. All requests for access (in whatever form they are received e.g. e-mail, fax, social media etc.) should be immediately directed to an authorised member of staff, which include the following:
		1. [Data Protection Officer or equivalent],
		2. [Head of legal]
		3. [Head of HR]
		4. [Other]
	2. There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the Information Commissioner and/or legal action by the affected individual.
1. Requirements for a valid request
	1. For a SAR to be valid, it must satisfy the following requirements:
		1. Be in writing[[1]](#footnote-1), this could potentially be by letter, email, text, twitter or other social media forum.
		2. If an individual makes a request by telephone or in person, they should be asked to put that request in writing using the **Subject Access Request Form** (as set out in Appendix 1);
		3. Identify the individual making the request. We must take reasonable steps to verify the identity of the individual. The **Subject Access Request Form** contains examples of the type of documents that can be used to do this.
		4. The information requested must be able to be identified from the SAR.

*For example: if the request relates to CCTV images, the SAR can be clarified by asking for details of the date, time and location (if such information is available) to help narrow the scope of the request.*

The **Subject Access Request Form** contains questions designed to identify the information being requested and should be used wherever possible. ***However*,** any written request will be sufficient, it is not necessary for the Subject Access Request Form to be completed in every instance. Provided the request is in writing, proof of the requestor’s identity has been provided and the information requested can be identified, the 1 month timescale for compliance will begin to run from the date the written request is received by [NAME OF ORGANISATION].

* 1. If the individual makes a request that does not satisfy the above requirements the individual should be notified of this using the standard form letter (as set out in Appendix 2) and enclosing the relevant **Subject Access Request Form.**
	2. Unless the above requirements are met, [NAME OF ORGANISATION] is not obliged to comply with an SAR. However, we are obliged to notify the individual promptly if further information is required in order to fulfil the request.
1. The timescale for responding to a SAR
	1. A valid SAR should be responded to it as soon as possible and at least within **1 calendar month**.
	2. In exceptional circumstances it may be possible to extend this period by a further 2 calendar months, providing 3 calendar months in total to respond. Such an extension will only be applicable where an SAR is received in conjunction with requests to exercise other individual rights under data protection law (such as the right to have personal data rectified or erased) and the complexity and the number of those requests is taken into account. In such circumstances, you should consult the **[Data Protection Officer or other]** to determine whether an extension can be applied. If an extension is applied, the individual must be notified of that fact and the reasons for the extension.
2. Requests that involve a large amount of personal data
	1. An extension (as set out in 4.2) will not be permitted merely because an SAR is made which involves large amounts of personal data. In such circumstances the individual can be asked to specify the information the SAR relates to and it may be necessary to consider whether the request is manifestly unfounded or excessive (see sections 11.3 and 11.4 below).
3. Information to be provided in response to an SAR
	1. The individual is entitled to receive the following:
		1. Confirmation as to whether or not personal data concerning them is being processed.
		2. The purposes of the processing.
		3. The information constituting their personal data (see section 8 below)
		4. The recipients to whom the individual’s personal data has been or will be disclosed, including and in particular any recipients in countries outside the European Economic Area.
		5. The envisaged period for which the personal data will be stored, or if this is not possible, the criteria used to determine that period.
		6. Confirmation that the individual has the right to request that their personal data is rectified or erased, and the right to request that the processing of their personal data is restricted or to object to the processing of their personal data.
		7. Confirmation that the individual has the right to lodge a complaint with a supervisory authority (i.e. the Information Commissioner).
		8. If the personal data was not collected from the individual directly (i.e. it has been provided by a 3rd party) any available information as to the source of the data.
		9. Where automated decision making (including profiling) has been applied to the individual, the logic involved and the consequences of such processing for the individual. The automated decision must constitute the sole basis for the decision, if there is an element of human discretion the decision would cease to be wholly automated and the individual will not be entitled to a description of the logic. In providing a description of the logic [NAME OF ORGANISATION] is not required to reveal any information which constitutes a trade secret, intellectual property or copyright.
	2. The above must be provided in an intelligible form, using clear and plain language. Any technical terms, abbreviations or codes must be explained to the individual. The standard form letter (as set out in Appendix 3) should be used when responding to an SAR.
4. How to locate the information requested
	1. The personal data we need to provide in response to an SAR may be located in electronic and other filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be as focused as possible.
	2. Depending upon the type of information requested it will be necessary to search some or all of the following:
		1. Electronic systems (e.g. databases, networked computers, mobile telephones, servers, [customer] [membership] records, human resources systems, email data, back up data, CCTV and audio recordings);
		2. Personal devices (e.g. laptops, tablets, telephones, personal email accounts). This will be necessary where personal data has been transferred from [NAME OF ORGANISATION]’s network to any staff personal devices. **[See [NAME OF ORGANISATION]’s Bring Your Own Device Policy].**
		3. Non-electronic filing systems (e.g. personnel records or customer records) which allow specific personal data about an individual to be searched according to specific criteria e.g. name, reference number, job title or other identifier.
		4. Data systems held externally by our data processors (e.g. external payroll providers or IT service providers).
		5. Occupational health records held by the Occupational Health Department
		6. **[specify any other type of system which your organisation might have].**

These systems should be searched using the following, where relevant:

* Name (including common variations of the name e.g. initials or abbreviations)
* Employee number
* [Customer account number]
* [Membership number]
* Other personal identifier (such as online identifiers e.g. email address)
1. What is personal data?
	1. Once you have carried out the search and gathered the results, you will need to select the information to be supplied in response to the SAR. The individual is only entitled to receive information which constitutes their personal data.
	2. The type of information that will be classified as personal data is any information which identifies the individual (either directly from the data or from that data and other information which is in [NAME OF ORGANISATION]’s possession or that is likely to come into the organisation’s possession) such as information held by subsidiaries, other offices or branches or [*specify as appropriate*] and:
		1. Relates to the individual, or
		2. Has the individual as its focus (i.e. the information relates to the data subject personally e.g. notes of a disciplinary or grievance meeting relating to the data subject), a mere record of the individual’s involvement in a matter or event, such as the individual’s attendance at a meeting where their name appears in the list of attendees will not have the individual as its focus, or
		3. Is an expression of opinion about the individual, or
		4. Is an indication of the intentions of [NAME OF ORGANISATION] or any other person towards the data subject (e.g. promotion prospects or redundancies). **NB. Information of this type may be subject to an exemption and may not need to be provided see section 13 below.**

|  |
| --- |
| **Examples of information likely to constitute personal data include:** |
| Marketing lists containing a name together with contact details (e.g. address, telephone number, email) |
| Customer profile information (e.g. shopping preferences of the data subject) |
| Human resources information (e.g. salary details, appraisals) |
| Financial information (e.g. information about the data subject's tax liabilities, income, expenditure) |
| Medical information (e.g. medical history or condition, including pregnancy) |
| Images caught on CCTV camera or audio recordings |

|  |
| --- |
| **Examples of information unlikely to constitute personal data** |
| Reference to the individual’s name in a document that contains no other personal data about that data subject (e.g. the data subject's name in a list of attendees in the minutes of a meeting where the individual simply attended in his or her official capacity) |
| Where the individual’s name appears in an email that has been sent to or copied to him or her, but where the content is not about him or her (e.g. emails sent to the data subject about [NAME OF ORGANISATION]'s dealings). |
| Information about the performance of a department or branch office where no reference is made personally to the individual. |

1. The personal data of other individuals
	1. As this policy has highlighted, the data subject is only entitled to receive information which constitutes their own personal data. There will be instances where the individual’s personal data includes data that identifies another person (this is referred to in this procedure as 3rd party data).
	2. It will be necessary where 3rd party data is included to consider whether the 3rd party’s information constitutes personal data relating to the data subject.

*For example, an expression of opinion about the individual by the 3rd party which identifies the 3rd party.*

* 1. Where the 3rd party’s information forms part of the individual’s personal data then you should consider:
		1. Whether the 3rd party has consented to the disclosure of their information; or
		2. Whether it is reasonable in all the circumstances to comply with the request without the consent of the 3rd party (for example because consent has been withheld or cannot be obtained)
	2. In order to determine whether it is reasonable in all the circumstances to provide the 3rd party’s information you must consider:
		1. Any duty of confidentiality [NAME OF ORGANISATION] owes to the 3rd party;
		2. Any steps that have been taken to obtain the consent of the 3rd party;
		3. Whether the 3rd party is capable of giving consent;
		4. Any express refusal to give consent by the 3rd party and the reasons for that refusal;
		5. Whether the information is generally known to the data subject; and
		6. Whether the individual has a legitimate interest in the disclosure of the 3rd party’s information.
	3. Ultimately, whether or not it is reasonable to disclose the 3rd party’s information will depend upon all the circumstances and each SAR should be considered on a case-by-case basis.
	4. If a decision is taken to withhold the 3rd party’s information, [NAME OF ORGANISATION] still has an obligation to provide as much of the information requested as possible without disclosing the identity of the 3rd party. This can usually be achieved by redacting the 3rd party’s data (i.e. blanking out names or other identifying particulars such as job title).
	5. It is important to document any redactions made and the reasons for those redactions.
1. Providing the information
	1. The data subject is entitled to be provided with a copy of their personal data together with the information outlined in 6 above.
	2. Where the data subject has made a request by electronic means the information shall be provided in electronic form. In all other situations the information shall be provided in electronic form unless the data subject has requested otherwise.
	3. A copy of the information **must** be provided to the data subject unless this is not possible. If necessary, following consideration of the point in 9 above, the information may need to be redacted where appropriate.
	4. If a copy of the information cannot be provided, then alternative ways of enabling the data subject to have access to the information must be considered. Alternatives might include:
		1. Allowing the data subject to come to our premises to view their personal data on screen or a hard copy;
		2. Allowing the data subject to have copies of the data that are of most interest (if this is possible);
		3. Allowing the data subject to view CCTV images or listen to telephone recordings on site.
	5. If data subjects are allowed to view personal data on our premises, it is necessary to ensure that they are supervised and to not have inadvertent access to confidential information or the personal data of others.
2. Refusing a request or charging a fee
	1. In the majority of cases a response to an SAR will be provided free of charge.
	2. A reasonable fee can be charged to comply with requests for further copies of the same information which has been requested under an SAR. This does not mean however that a fee can be charged for all subsequent SARs.
	3. If a request from a data subject is **manifestly unfounded** or **excessive in nature** (for example because a request is repetitive)[[2]](#footnote-2),it is possible to:
		1. Charge a reasonable fee taking into account the administrative costs of providing the information; or
		2. Refuse to act on the request.
	4. If an SAR is suspected of being manifestly unfounded or excessive in nature it should be referred to the [Data Protection Officer or other] without delay.

The [Data Protection Officer or other] should determine:

* + 1. Whether the SAR is in fact manifestly unfounded or excessive in nature, if so:
		2. Whether a fee should be charged in relation to the provision of the information and the level of that fee (the fee should be based on the administrative cost of providing the information); or
		3. Whether to refuse to act on the request.
	1. If it is determined that a fee should be charged, the data subject should be notified, in writing, of that fact, the level of the fee, and the reason for requesting the fee, without delay. The time limit as set out in section 4 above will not begin to run until the fee is received by [NAME OF ORGANISATION].
	2. If it is determined that the request will be refused, the data subject should be notified, in writing, of that fact and the reasons for the refusal to act on the request, without delay.
1. Requests made by third parties on behalf of the data subject
	1. Occasionally we may receive an request for subject access by a third party (an 'agent') acting on behalf of a data subject. These agents may include parents, guardians, legal representatives and those acting under a power of attorney or other legal authority. The agent must provide sufficient evidence that he or she is authorised to act on behalf of the data subject.
	2. [There are special rules for SARs regarding children and mentally and physically incapacitated adults. If the request you have received relates to an individual within either of these categories specific advice should be sought from the [Data Protection Officer or other].]
2. Exemptions to the right of subject access
	1. In certain circumstances [NAME OF ORGANISATION] may be exempt from providing some or all of the personal data requested.
	2. The most relevant exemptions are described below and should only be applied on a case by case basis after careful consideration of the facts. This is not an exhaustive list of exemptions and in particular circumstances other exemptions under Data Protection legislation may require consideration. In such circumstances you should contact [Data Protection Officer, other].

Crime detection and prevention

* 1. We do not have to disclose any personal data which is being processed for the purposes of preventing or detecting crime, apprehending or prosecuting offenders, or assessing or collecting any tax or duty. This is not an absolute exemption. It only applies to the extent to which providing the information to the data subject would prejudice any of these purposes. We are still required to provide as much of the personal data as we are able to.

*For example: if the disclosure of personal data in response to an SAR could alert the data subject to the fact that they are being investigated for illegal activity then that data would not need to be disclosed, because such a disclosure would likely prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.*

Confidential references

* 1. We do not have to disclose any confidential references that have been provided ***to*** 3rd parties for the purpose of:
		1. Education, training or employment of the data subject;
		2. Appointment of the data subject to any office; or
		3. Provision by the data subject of any service.
	2. This exemption does not apply to confidential references that we received ***from*** 3rd 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 the considerations regarding the disclosure of 3rd party data as set out in 9 above must be taken into account before disclosing the reference.

Legal privilege

* 1. We do not have to disclose any personal data which is subject to legal professional privilege. There are two types of legal privilege:
		1. Advice privilege: this covers confidential communications between [NAME OF ORGANISATION] and our legal representatives where the dominant purpose of the communication is the seeking or giving of legal advice;
		2. **Litigation privilege:** this covers any document which was created with the dominant purpose of being used in actual or anticipated litigation (e.g. legal proceedings before a court or tribunal).
	2. If you think the legal privilege exemption could apply to the personal data that have been requested, you should refer the matter to **[Head of Legal/other]** for further advice.

Management forecasting

* 1. We do not have to disclose any personal data which is processed for the purposes of management forecasting or management planning to assist in the conduct of any business or any other activity.
	2. For example: staff relocations, redundancies, succession planning, promotions and demotions.
	3. This exemption must be considered on a case-by-case basis and must only be applied to the extent to which disclosing the personal data would be likely to prejudice the conduct of that business or activity.

Negotiations

* 1. We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the data subject where doing so would be likely to prejudice those negotiations.
	2. For example, if HR is negotiating with an employee in order to agree the terms of a redundancy package and the employee makes an SAR, HR can legitimately withhold giving access to information which would prejudice those redundancy negotiations.
	3. The HR department must, however, disclose all other personal data relating to the data subject unless those other personal data are also exempt from disclosure.
1. Failure to comply with a request
	1. A failure to comply with an SAR, or a failure to provide a copy of all the personal data requested (without a valid reason such as the application of an exemption, considerations relating to 3rd party data, or the fact that an SAR is manifestly unfounded or excessive in nature) will be in breach of the law. This has several potential consequences.
	2. The data subject may complain to the Information Commissioner and this may lead the ICO to investigate the complaint. If [NAME OF ORGANISATION] is found to be in breach, enforcement action could follow (which could include monetary penalties) and if an individual has suffered damage or distress as a result of the breach, they may bring a claim for damages.
2. Disciplinary action
	1. A failure to comply with this guidance may be a disciplinary offence, which could result in summary dismissal.
3. [Review of response to SAR
	1. A data subject will be informed of their right to review the response they receive to an SAR. They will be provided with details of how to request a review of the response, in the event that:
		1. they consider the information provided to them to be incomplete; and/or
		2. they do not agree that an exemption applies to their personal data.

The review will be undertaken by the [Data Protection Officer or other][[3]](#footnote-3).]

1. Review of this policy
	1. This procedure will be reviewed [specify period] by the [Data Protection Officer or other].
	2. Any questions regarding this procedure should be addressed to the [Data Protection Officer or other] [insert contact details].

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
| **Data Subject Access Request Form** |
| Under the General Data Protection Regulation (GDPR) you are entitled to a copy of information constituting your personal data which is held by **[NAME OF ORGANISATION].**In order to deal with your request we can ask for proof of identity and enough information to enable us to locate the personal data that you request.Please complete this form and return it to us with proof of your identity to [[NAME OF ORGANISATION]’s postal/email address]. We will acknowledge safe receipt and respond within 1 calendar month (unless your request is particularly complex). |
| **Part 1: Person that the request relates to (the data subject)**Title: Mr / Mrs / Miss / Ms / OtherSurname:Forenames:Any other names that you are known by that may assist in the search:Address:Postcode:Telephone:E-mail:Date of birth:If you are an employee or former employee of [NAME OF ORGANISATION] please provide your staff number: |
| **Part 2: Proof of identity**To help us establish your identity your application must be accompanied by two pieces of identification that between them clearly show your name, date of birth and current address.Please enclose a copy of one of the following as proof of identity: passport or photocard driving licence, birth or adoption certificate and a copy of a bank statement or utility bill dated within the last three months.This is to ensure that we are only sending information to the data subject and not to a third party. If none of these are available, please contact [CONTACT NAME AND DETAILS] for advice on other acceptable forms of identification |
| **Part 3: Information requested**To help us to deal with your request quickly and efficiently please provide as much detail as possible about the information you want. If possible, restrict your request to a particular service, department, teams or individuals or incident. Please include time frames, dates, names or types of documents, any file reference and any other information that may enable us to locate your data, for example, for e-mails, the names of senders and recipients and approximate dates.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Please continue on a separate sheet of paper, if necessary. |
| I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, confirm that the information provided on this form is correct and that I am the data subject whose name appears on this form. I understand that **[NAME OF ORGANISATION]** must confirm proof of identity and that it may be necessary to contact me again for further information to locate the personal data I want. I also understand that my request will not be valid until all of the information requested is received by **[NAME OF ORGANISATION]**.**Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

 |
|  |
|  |
|  |

**APPENDIX 2 – Acknowledgement of Subject Access Request and request for further information using Subject Access Request Form.**

Dear [name]

**Acknowledgment of your subject access request**

Thank you for your letter of [date] in which you make a request for access to [personal data which we process about you [or specify].

In order to assist us to deal with your enquiry, please would you complete and return the attached Subject Access Request Form. This will enable us to locate more easily the information you are seeking.

**EITHER**

We also acknowledge receipt of your [driving licence or passport or other document showing your name and signature & recent bill] as confirmation of your identity.

**OR**

We also ask that you provide us with some proof of your identity. Please send us a copy of:

1. your driving licence or passport or other document showing your name and signature; and
2. a recent bill (e.g. credit card bill, bank statement or utility bill) or insurance document (e.g. house or car insurance certificate) showing your name and address.

We hope that you will understand that we need to check your identity to ensure that we do not disclose your personal data to any unauthorised person.

Once you have completed the attached Subject Access Request Form, please return it to us at [insert the address/email address] marked for the attention of the Data Information & Protection Co-Ordinator. We will then respond to your request as soon as possible and, in any case, within 1 calendar month.

Please note that the deadline of 1 month for us to respond to your request may be extended by the time it takes you to provide the information we have requested.

Yours sincerely

[NAME]

[POSITION]

**Appendix 3 – Subject access request response**

Dear [Name]

The following is in response to your letter of [date] in which you made a request for access to personal data which we process about you [and your subsequent correspondence containing the Subject Access Request Form].

We can confirm that your personal data is being processed by [NAME OF ORGANISATION] [and our agents *include names of organisations processing data on controller’s behalf*] for the purposes of [insert description of the purposes].

A copy of the personal data which we hold about you is attached in [format e.g. paper, electronic etc. with reasons for choosing that format].

[We have contacted the following departments [list departments e.g. Marketing, IT, Human Resources etc.] within the organisation to locate the personal data which is within the scope of your subject access request. In general terms, your personal data comprises information relating to [insert general description of the personal data of which that individual is the data subject].

We disclose your personal data to [insert description of recipients or categories of recipients to whom those data are or may be disclosed]. This includes the following recipients [list recipients] in countries outside the European Economic Area.

We obtained your personal data from you, or [insert the type of sources from which the data was obtained; generic descriptions are sufficient, e.g. banks, previous employer].

[You have specifically requested information describing the logic behind an automated decision which was taken about you in respect of [insert description of why the decision was taken, e.g. an application for credit]. The logic behind such automated decision is [insert description].

We envisage retaining your data in storage for [list data and retention period] in compliance with our retention policy a copy of which is available [upon request or link to website].

We confirm that you have the right to request that your personal data is rectified or erased, and the right to request that the processing of your personal data is restricted or to object to the processing of your personal data.

[You have the right to request a review of our response to your subject access request in the event that:

• you consider the information provided to you to be incomplete; and/or

• you do not agree that an exemption applies to your personal data.

Please address any request for a review to [NAME OF ORGANISATION]’s [Data Protection Officer or other] within 14 days of the date of this letter.]

You [also] have the right to lodge a complaint with the Information Commissioner if you do not consider that your subject access request has been dealt with correctly.

Yours sincerely

(signature)

1. The GDPR is silent as to whether the request must be made in writing. We are currently awaiting ICO guidance on this issue and will update this document once we receive clarification on this point. Should verbal requests be valid SARs under the GDPR this section 3 will need to be amended. [↑](#footnote-ref-1)
2. There is currently no guidance as to what manifestly unfounded or excessive in nature will mean in practice. This policy will be updated with further information when it is available. [↑](#footnote-ref-2)
3. There is no requirement to provide a review, but it can prove useful to rectify any errors in the initial response before a requester potentially complains to the ICO. [↑](#footnote-ref-3)