Subject Access Request Policy 2021
(individuals requesting to see their own personal data)

Introduction

This Policy sets out the obligations of Amaze regarding data subject access requests under the Data Protection Legislation (defined below). This Policy also provides procedural guidance on the handling of data subject access requests which all staff and volunteers must follow.

1. Definitions

"data controller"	means the person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, Amaze is the data controller of all personal data used in our organisation;
"data processor"	means a person or organisation which processes personal data on behalf of a data controller;
"Data Protection Legislation"	means all applicable data protection and privacy laws including, but not limited to, the GDPR, and any applicable national laws, regulations, and secondary legislation in England and Wales concerning the processing of personal data or the privacy of electronic communications, as amended, replaced, or updated from time to time;
"data subject"	means a living, identified, or identifiable individual about whom Amaze holds personal data;
"personal data"	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;
"processing"	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"special category personal data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

2. Data Protection Officer & Scope of Policy

2.1 Amaze collects, holds, and processes personal data about staff, volunteers and our service users (families) and is a 'data controller' for the purposes of the Data Protection Legislation. As Amaze also processes personal data on behalf of other organisations, it is also a 'data processor' for the purposes of the Data Protection Legislation.

2.2 Data subjects have rights with respect to their personal data under the Data Protection Legislation. This Policy deals specifically with the right of access (Article 15 of the GDPR). Data subjects have the right to find out whether Amaze collects, holds, or processes personal data about them, the right to obtain a copy of any such data, and certain other supplementary information. The right of access is designed to help data subjects to understand how and why we use their data, and to check that we are doing so lawfully.

2.3 Individuals are not obliged to disclose their reason for making the subject access request or what they intend to do with the information. However, it often helps to provide the relevant information if they do explain the purpose of the request.

2.4 This Policy is an internal policy designed to provide guidance on handling data subject access requests. It is not a data protection policy, privacy policy, privacy notice, or similar, and is not designed to be made available to third parties (including, but not limited to, data subjects). This Policy should, where appropriate, be read in conjunction with Amaze's Data Protection and Confidentiality Policy.

3. How to Recognise a Data Subject Access Request

3.1 The Data Protection Legislation does not set out a particular format which a data subject access request (hereafter "SAR") must follow. A SAR may be made orally or in writing, to any part of Amaze, and by any means of communication. A SAR does not need to use the words 'subject access request', 'data protection', 'personal data' or similar terms, or refer to Article 15 of the GDPR. This means that anyone in Amaze could receive a SAR and it may not be immediately obvious that a SAR has been received.

3.2 Individuals may make SARs on their own behalf. It is also possible to make an SAR via a third party:

a. This may be a solicitor making a request on behalf of an individual, or it may be one individual making the request on behalf of another. This is permissible, but you must be satisfied that the individual making the request has the authority to act on behalf of the data subject concerned.
b. In certain limited cases, an individual may not have the mental capacity to manage their own affairs. In these cases, the Mental Capacity Act 2005 enables a third party to make a SAR on behalf of that individual.
c. The right to access information about a child is the child's right rather than anyone else's, even if:
    - they are too young to understand the implications of the right of access;

- the right is exercised by those who have parental responsibility for the child; or
- they have authorised another person to exercise the right on their behalf.

However, if the information held by Amaze has been provided by the Parent Carer, such as Compass Card data or through a DLA application it is reasonable to assume this information can be disclosed to the Parent Carer, provided parental responsibility has been ascertained.

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the request is from a child and you are confident that the child can understand their rights, you should usually respond directly to them. You may allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

If a child is competent, they may authorise someone else – other than a parent or guardian – to make a SAR on their behalf. If you are satisfied that the child is not competent and the request is from a person with parental responsibility for the child, then it is usually appropriate to let the holder of parental responsibility exercise the child's rights on their behalf.

4. What to do When a Subject Access Request is Received

4.1 Amaze has a limited timeframe within which to respond to a SAR, so it is important to act quickly. A SAR request must be forwarded to the Data Protection Officer and copied to the CEO and DCEO immediately.

4.2 SARs may come in any form. This will determine how to forward the SAR to the appropriate member of staff:

a. For SARs received by email or via social media, the message, or a link, if appropriate, must be forwarded immediately to Amaze's Data Protection Officer/DCEO.
b. For SARs received by post or in any other hardcopy form, the SAR should first be scanned and emailed immediately to Amaze's Data Protection Officer/DCEO and the original sent to the same recipient using the most direct and secure means possible.
c. For SARs made verbally, the name and contact details of the data subject should first be recorded before informing the data subject that Amaze's Data Protection Officer/DCEO will contact them for full details of their SAR. The data subject's details and any other information provided by the data subject should be emailed immediately to the Data Protection Officer/DCEO including details of the time and date on which the SAR was made.

5. Responding to a Subject Access Request

Part 1: Identifying Data Subjects and Clarifying Requests

5.1 It is essential to be sure that the request is made by the individual concerned and therefore their identity confirmed. If the person is known to the organisation and they make the request in such a way that we are sure they are the individual, such as in person or by phone to a worker they know, then ID is not required. Otherwise the following ID is required:

a. For the person making the SAR, 2 forms of ID one must be a photo ID and both with a current address, such as a utility bill, passport, driving license. Copies are acceptable if of high enough quality.
b. For dependants where permission is not being obtained directly from them, child's birth certificate or parental responsibility certificate. If there is any known history of parental access issues to the children this must be raised by anyone known to the family and extra caution taken.
c. If a SAR is made by a third party on behalf of a data subject (see Section 4.4), the individual acting on behalf of the data subject must be required to provide sufficient evidence that they are authorised to act on the data subject's behalf.

5.2 If additional information is required to confirm an individual's identity, the individual must be informed as soon as possible. If additional information is required, the time limit for responding to an SAR does not begin until that information is received.

5.3 If the SAR involves processing a large amount of personal data about the subject, it is helpful to ask the subject to clarify their request (i.e. to specify the personal data or processing to which their SAR relates). Information requested for such purposes must be reasonable and proportionate. Individuals must not be asked to provide any more information than is reasonably necessary.

5.4 If, having requested additional information to clarify a SAR, the individual does not comply, Amaze must still endeavour to comply with the SAR by making reasonable searches for the personal data relating to the request.

6. Responding to a Subject Access Request

Part 2: Fees

6.1 Under normal circumstances, the Data Protection Legislation prohibits the charging of a fee for handling a SAR. Amaze does not normally charge for SARs. 8.2 In limited cases, it is permissible to charge a 'reasonable fee' in order to cover the administrative costs of complying with a SAR if that SAR is 'manifestly unfounded', 'excessive', or if a data subject requests further copies of their data following the SAR. In certain cases, it may also be permissible to refuse to comply with a SAR, as set out in Section 11(b).

7. Responding to a Subject Access Request

Part 3: Time Limits

7.1 Under normal circumstances, Amaze must respond to a SAR 'without undue delay' and, at the latest, within one month of receipt. The date of receipt of all SARs must be recorded, along with the due date for response.

7.2 Under the Data Protection Legislation, the one-month period begins on the calendar day – not business day – that the request is received and ends on the corresponding calendar day in the following month. Consequently, the time limit set by Amaze for responding to SARs is 28 calendar days. If the last day of the time limit falls on a weekend or bank holiday, the time limit is extended to the next business day.

7.3 If additional information is required from the individual making the SAR to confirm an individual's identity, the time limit begins on the day that such information is received.

7.4 If additional information is required from the individual making the SAR to clarify the SAR, the time limit is unaffected and begins on the day that the SAR is received.

7.5 If the SAR is complex, or if the same data subject makes a number of SARs, it is permissible to extend the time limit by up to two months. If such an extension is necessary, the data subject must be informed, in writing, of the reason(s) for the extension within the original one-month time limit.

8. Responding to a Subject Access Request

Part 4: Information to be Provided

8.1 Data subjects must be provided with the following information in response to a SAR:

a. the purposes for which Amaze collects, holds, and processes their personal data;
b. the categories of personal data involved;
c. the recipients or categories of recipient to whom Amaze discloses their personal data;
d. details of how long Amaze retains their personal data or, if there is no fixed period, our criteria for determining how long it will be retained;
e. details of the data subject's right to ask Amaze to rectify or erase their personal data, or to restrict or object to our processing of it;
f. details of the data subject's right to make a complaint to the ICO or to another supervisory authority;
g. if any of the personal data in question was not obtained from the data subject, details of the source of that data;
h. if Amaze carries out any automated decision-making (including profiling), details of that automated decision-making, including a meaningful explanation of the logic involved and the significance and envisaged consequences for the data subject; and
i. if Amaze transfers their personal data to a third country (i.e. non-EEA) or international organisation, details of the safeguards in place to protect that data.

8.2 The information set out in this section must be provided:

a. in a concise, transparent, intelligible, and easily accessible form, using clear and plain language;
b. in writing; and
c. if the data subject has made the SAR electronically, in a commonly used electronic format unless the data subject requests otherwise.

   Amaze will work hard to provide the information in an accessible format, if the individual has a specific disability.

8.3 It is important to note that data subjects are only entitled to access personal data that Amaze holds about them. If information located in the process of responding to a SAR does not meet the definition of "personal data", the Data Protection Legislation does not entitle the data subject to access it. In certain cases, it may be necessary to separate personal data from non-personal data when responding to a SAR.

8.4 An individual can request access to any personal data held in emails and this can include archived emails. For example, if an employee makes an SAR request for all their emails and they have been copied into many emails but they do not relate to them themselves, the content of these emails does not have to be provided. Their name and email address is their personal data only.

8.5 It is important to consider if the data request will include disclosing personal data about third parties, including other professionals. It is preferable to gain permission from the third party to include their details, if this is not possible, consider if it reasonable to still include the data.

9. Responding to a Subject Access Request

Part 5: Locating Information

9.1 Amaze holds personal data in the following locations and/or systems. It is important to identify the type(s) of personal data to which a SAR relates in order to search in the correct place or all locations if the request is more general:

a. Paper filing at Amaze's offices
b. Amaze's service in the Cloud. For identifying and locating emails and electronic files, SCIP use SAR software to search all data on our system. The Data Protection Officer/DCEO will liaise with SCIP to undertake this search
c. In the Charitylog system stored on the servers of our supplier Dizions Ltd.
d. At the time of receipt of the request Amaze should consider if any other systems have been used to process data for example if the request was made by a member of staff, HR systems.

9.2 Once the information is collated and ready to send, make a SAR record of:

a. The date the individual made their request
b. The date you responded
c. Details of who provided the information

d. What information you provided.

10. Refusing to Respond to a Subject Access Request

10.1 In certain cases, it is permissible for Amaze to refuse to comply with a SAR: a) if it is not possible to identify the individual making the SAR after requesting additional verification; or b) if the request is 'manifestly unfounded' or 'excessive', taking into account whether the request is repetitive in nature. In such cases, it is also possible to request a 'reasonable fee' to handle it.

10.2 If either of the above grounds applies, Amaze's refusal to comply with the SAR must be justified and an explanation must be provided to the individual making the SAR within one calendar month after receiving the SAR. The individual must also be informed of their right to complain to the ICO or another supervisory authority and of possibility of seeking a judicial remedy.

11. Exemptions to the Right of Access

11.1 The Data Protection Legislation provides a number of exemptions which apply to SARs and therefore justify Amaze refusing to comply with a SAR. Those most likely to be applicable within Amaze are situations in which the personal data in question is:

a. subject to legal or litigation privilege; or
b. purely personal or exists for a household activity; or
c. a reference given (or to be given) in confidence for purposes of employment, training, or education; or
d. is processed for management forecasting or management planning purposes in relation to a business or other activity (but only to the extent that complying with the SAR would prejudice the conduct of the business or activity); or
e. consists of records of intentions with respect to negotiations between employer and employee (but only to the extent that complying with the SAR would prejudice such negotiations); or
f. contains personal data concerning a third party; or
g. is of a type likely to prejudice the prevention or detection of a crime, or the apprehension or prosecution of offenders if it is disclosed.

11.2 If any concerns or questions arise with respect to exemptions which may or may not apply during the process of handling a SAR (including, but not limited to those set out above), those questions should be referred to Amaze's Data Protection Officer/DCEO and/or to the ICO. Further guidance on this and redaction is available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access

12. Erasure or Disposal of Personal Data

12.1 If any personal data relevant to a SAR is amended, deleted, or otherwise disposed of between the time at which a SAR is received and the time at which a response is made,

Amaze is able to take this into account in our response provided that amendment, deletion, or disposal would have been made irrespective of our receipt of the SAR in question.

12.2 The Right of Access does not, therefore, prevent Amaze from managing personal data in accordance with normal procedures, in particular those set out in its Data Protection and Confidentiality Policy. It is not, however, permissible to amend, delete, or otherwise dispose of data as an alternative to complying with a SAR.

13. Responsibilities and Breach of Policy

Everyone is responsible for their own compliance with this policy. For staff, breaches of policy may incur disciplinary action, depending on the severity of the issue. Please refer to our **Disciplinary Policy** for further information on disciplinary procedures. Staff who are unsure about whether something they propose to do might breach this policy, should seek advice from their manager or the policy owner.

14. Communication of the Policy

This policy will be available in the policies folder and hard copies will be available on request. New staff and volunteers will be made aware of the policy during their induction with their manager. Training will be available on request. Reminders will be given at staff meetings.

15. Related Forms / Associated Documents

N/a

16. Related Policies

Please also see the following related policies:

- **Disciplinary Policy**
- **Privacy Policy**
- **Data Protection and Confidentiality Policy**

VERSION CONTROL / RECORD OF CHANGES

Review date	Version	Section	Changes/Comments
August 2021	2	All	Rewritten by Sally Polanski
Nov 2021	3	All	Full Review of Policy

Summary procedure to follow

i. As soon as it becomes clear someone is making a SAR, email the Data Protection Officer (DPO), copying in the CEO and DCEO. Forward any supporting documentation (but not IDs). Inform the person making the request that you have done this.

ii. An individual can contact the DPO directly stating:
   a. Name (names of children if relevant to SAR)
   b. Reason for SAR – this is not obligatory but helps us identify the relevant data
   c. Information required, specifying any time periods if relevant

iii. The DPO will:
   a. Log the request here: S:\Administration\Governance\Strategy and Risk\GDPR\Requests for removal or access to data emails\SAR Requests Amaze.xls
   b. Set up a folder for the documentation, all emails about the SAR should be saved here.
   c. Check the request and ascertain if proof of ID is required, if clarification is required about the request.
   d. If the request relates to a dependant the DPO must ascertain if the dependant permission is needed and will discuss with managers/relevant colleagues. It is often preferable that someone who knows the individual liaise within them about any concerns or specifics about the enquiry.
   e. Contact the individual acknowledging the request and requesting ID/clarification. Explaining that information will be provided within a calendar month (from receipt of ID/clarification if required).
   f. The DPO will contact B&HCC and/or WSCC if Compass Card data has been requested.

iv. A manager (this may be the DPO) should be assigned to the SAR and be responsible that the SAR is complete and any third party information is redacted. This person takes responsibility for:
   a. Redacting third party information about other clients/professionals (where relevant). Reasons for information being redacted must be recorded in the SAR file.
   b. The DPO will send the completed SAR file to the individual by email (Egress Switch) or registered post. If information has been redacted this should be explained to the individual. Additionally send a copy of the Amaze Privacy Policy and any additional requirements as laid out in point 8.1 of this policy.