Amaze Data Protection and Confidentiality Policy

1. Purpose:

In order to function as an organisation, we need to collect and store personal data about the people we work with, who they support and those working with or supporting Amaze.

Personal data is collected for the following “Data Subjects”:

- Parent Carers
- Professionals
- Children of parent carers/those supporting children
- Young People engaging with Amaze
- Staff and volunteers of Amaze
- Other people supporting Amaze such as fundraisers and trustees

The purpose of this policy is to provide knowledge and guidance for staff, volunteers and users of Amaze on how to ensure that all the data we collect, store and transmit follows the organisational policy and legal requirements. Including what to do should data be lost or shared inappropriately and how to respond to requests for information sharing or a Subject Access Request. We are obliged by law to meet the requirements of the Data Protection Act (DPA) 2018 and the UK General Data Protection Regulation (UK GDPR) which came into effect in June 2021. Despite the legal obligations, as an organisation we hold data protection and confidentiality as a high priority, we acknowledge that people are entrusting highly personal information about themselves and their families, we must look after this information carefully and not share it inappropriately and without consent.

2: Data Protection Statement:

Amaze is committed to complying with the DPA 2018 and the UK GDPR as well as following good practice in order to protect our Data Subjects and Amaze as an organisation.

We commit to respecting the rights of our Data Subjects with regards to data access and to be open and honest with individuals about what we will use their personal data for. We will only store personal data about an individual if we have received their consent to do so.

Any data breaches will be reviewed immediately and acted on swiftly. All breaches will be reported to the Commissioner’s Office (ICO) within 72 hours if it reaches their reporting threshold.

We commit to never sharing personal data about our Data Subjects with other organisations, without the explicit and current consent of the individual (or their guardian for children). The only exception would be where a failure to share someone’s personal information would lead to a risk of significant harm to themselves or others. In such an event, the decision would not be taken lightly and would be reviewed by a Senior Manager before proceeding.

On any form where we are asking Data Subjects to share their personal information with us, we will insert a Data Protection statement which will inform them how their personal information will be stored and used.

We will ensure that Data Subjects opt in, to any additional communications outside their immediate support, such as receiving newsletters or updates, with the option to easily opt out at any time.

We commit to provide training and support for all staff and volunteers to ensure personal data is handled confidentially, consistently and securely at all times. All staff and volunteers must read this policy when initially engaged with Amaze and on any subsequent changes to the policy.

More detail about how we carry out these commitments are within the policy.

3: Data Protection Principles:

Amaze will adhere to the seven key principles of Data Protection, as detailed in the DPA 2018 and the UK GDPR when processing personal data.

Personal data is information that relates to an identified or identifiable individual. If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

Sensitive data (special category data) which Amaze may keep about a person are:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Data concerning health
- Sexual Orientation

The data protection principles are:

1. **Lawfulness, fairness and transparency:** personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. **Purpose limitation:** personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. **Data minimisation:** personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy:** personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. **Storage limitation:** personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest,

scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

6. **Integrity and confidentiality (security):** 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, using appropriate technical or organisational measures
7. **Accountability:** The controller shall be responsible for, and be able to demonstrate compliance.

Amaze will, through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal data
- Meet its legal obligations to specify the purposes for which personal data is used
- Collect and process appropriate personal data, and only to the extent that it is necessary to its operational needs or to comply with any legal requirements
- Ensure the quality of personal data processed
- Ensure that the rights of people about whom personal data is held, can be fully exercised under the UK GDPR. These include:
    i. The right to be informed that processing of one's own personal data is being undertaken
    ii. The right of access to one's own personal data
    iii. The right to object to the processing of one's own personal data in certain circumstances
    iv. The right to correct, rectify, restrict or erase one's own personal data
    v. The right to obtain and re-use one's own personal data
- Take appropriate technical and organisational security measures to safeguard personal data
- Ensure that personal data is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for personal data
- Set out clear procedures for responding to requests for personal data

Lawfulness: Under Article 6, the lawful basis for processing personal data is **consent**, whereby an individual gives clear consent for Amaze to process their personal data for a specific purpose, that is support from Amaze, with the right to withdraw that consent.

Staff and volunteer records are processed under the valid reasons of **contract** and **legal obligation**.

For special category data, in compliance with Article 9, as well as processing data with the lawful basis of **consent**, the special category conditions for doing so are: (a) Explicit consent, (d) Not-for-profit bodies.

4: Data Controller:

Amaze (the organisation) is the Data Controller under the Data Protection Act 2018, which

means that it determines what purposes personal data will be held and used for. Amaze is required under the Act, as an organisation processing personal information, to pay a data protection fee to ICO on an annual basis.

Where Amaze enters into partnership work with other agencies/organisations, it will clearly set out who takes responsibility for the Data Controller role on a case by case basis.

5: Responsibilities:

Amaze trustees will have overall responsibility for ensuring that Amaze complies with its legal obligations and follows this policy.

Data Protection Officer - The Amaze Data and Performance Manager will take on the role of the Data Protection Officer, and will be responsible for reviewing this policy, advising the staff, volunteers and trustees on data protection issues, ensuring data protection training takes place, handling subject access requests etc. Amaze will ensure that the Data Protection Officer has expert knowledge on data protection law and practices and they are provided with appropriate resources to carry out their tasks and maintain their expert knowledge. The Data Protection Officer will report any concerns about Data Protection to the Amaze Board of Trustees and must not carry out any other tasks that could result in a conflict of interest.

All Amaze staff and volunteers will be responsible for following this policy, including safe keeping of confidential records, personal data and files.

Where this policy is breached, this will lead to a disciplinary investigation and the Amaze disciplinary procedure will be followed.

6: Data Recording and Storage:

The main client management system used by Amaze is called CharityLog. Where possible all records will be recorded on this system avoiding the replication of information in other formats that are hard to control.

It is acknowledged that at times this will not be possible, when notes are made by hand, files are saved in different places and data exported from CharityLog. It is therefore vital that this policy is applied to all data containing personal information.

Data may also be processed via third party websites/cloud services. Whilst using third party services, we should minimise the collecting of personal data, for example, when asking someone to complete a survey, do we need to collect any person identifiable data?

Whilst it is the responsibility of the third party to keep data safe, Amaze must verify that they are UK GDPR compliant. This includes verifying in which country the third party stores their data. By preference the server would be based in the UK. A decision was made in June 2021 by the EU Commission to accept the adequacy of UK GDPR, this means that currently any data held on a server within the EU is ok. However, this will be reviewed and may only last until **27 June 2025**. If the server is held outside the EU such as in the USA, this will have to be considered on an individual basis.

Any staff member signing up to a third party needs to take this into account and it is best practice to inform the DPO about the subscription, to review what data is being collected,

that the site is GDPR compliant and that the servers are held in the UK or the EU. A plan should also be put in place to periodically delete data on these third party apps.

We will ensure all staff and volunteers follow good practice in:

Consent – we will ensure that when personal data is collected from families that we have consent from them to process this information. We will ensure that information we supply about the processing of personal data will be:

- concise, transparent, intelligible and easily accessible
- written in clear and plain language, particularly if addressed to a child
- free of charge
- consent is current

Data Accuracy – when personal data is collected from families we will ensure that this is checked back with the individual for accuracy. Should it become apparent data is inaccurate or out of date we will rectify immediately.

Security checks – when interacting with families and drawing up their personal data from Amaze's systems to process a query, staff will first seek the following information to verify the identity of a family, prior to proceeding with the enquiry:

- Child/young person's name, date of birth, address and email address
- Family last name

If an enquiry is received via social media, unless it is generic info/advice, staff will generally ask the parent carer to email their query to enable appropriate security checks to be completed. Though care will be taken to advise the correspondent to minimise personal identifiable information in the email content.

Data Storage – personal data about families will be stored electronically on the Amaze Charitylog Database. This database is password protected with a two-stage login process and should only be accessed by staff or volunteers who have been given individual user names and passwords. Staff and volunteers must not share their individual login details with any other person. When a staff member leaves, the Data and Performance Manager should be informed promptly and their CharityLog account closed.

Whenever possible, any file containing personal data will be stored electronically on the Amaze Charitylog database, rather than on individual computers or on paper. Any personal data stored in computer files instead of the Amaze Charitylog database should be password protected.

If working remotely on a computer, laptop, smartphone or other device not belonging to Amaze, all records can and should be accessed and stored via Office 365 portal. Because Office 365 does not currently allow for attaching documents to emails, it may be necessary to download a version of the file to a local device for the purposes of attaching to an email and sending. When downloading information containing personal data, as soon as the attachment has been made and the email is sent, the file should then be electronically shredded from the local PC or laptop. Any files downloaded onto a local computer, laptop, smartphone or other device should be electronically shredded when the staff member finishes work for the day. Staff failing to delete files will be in breach of Amaze's IT policy which may lead to disciplinary action. Details of shredding software options are available

from the Data and Performance Manager.

Staff and volunteers carrying out casework will need to use personal data about families away from the office for the duration of the period of work with that parent. Trainers may need the personal data of attendees away from the office. All staff, volunteers and trainers who hold personal data for the purpose of providing a service on behalf of Amaze will be given guidance about safe storage, transmission and disposal of that personal data outside the office on a temporary basis. At all times only the amount of data taken out of Amaze offices should be kept to an absolute minimum. **For more information, see the Amaze Information Management Policy.**

Whilst password protecting Microsoft Office documents adds a level of security it is not infallible, where possible information should be accessed via the Amaze shared drive or using Egress Switch. For an added level of security files should be zipped with a second password. It is important when agreeing passwords to not share them via email otherwise they do not offer protection, agreeing them in person, phone, video call is preferential. (Staff will password-protect any electronic documents supplied to trustees if they contain personal data and trustees will not remove these passwords.)

We will also operate a 'clear desk' policy in Amaze offices - all paper containing personal data will be removed from desk surfaces and locked away in a lockable desk drawer or filing cabinet whenever that desk is left unattended. Staff and volunteers will not leave papers containing personal data out in visible sight in any office space used by Amaze and will not leave any such papers on or next to office printers/photocopiers/scanners.

Data Retention of Client Records – Most casework records will be kept for 7 years after our last contact with a family. This period has been determined due to the developmental changes a child or young person goes through, when support from Amaze may be needed. In particular, support around benefits and mandatory considerations would benefit from access to historical records.

Where casework has not been provided, for example a Compass Card only and we have had no further contact with a family, data will be kept for 3 years from the last contact or Compass expiry date.

If the young person supported directly or via a parent carer, associated records will retained for 3 years from the last contact.

The Records Retention Schedule can be found in the Amaze Information Management Policy (Appendix 1).

Right to be Forgotten/Erasure If an individual asks us to erase their personal data at any time, we will do this without delay. Ensuring all sources of personal information are removed, such as emails, photographs, saved files.

Data Archiving – after the retention period has ended, records held on the client management system, CharityLog, will be retained but anonymised; so all personal information is removed, but we can continue to use non-personal data e.g. service referrals for statistical reporting. The DPO will manage this process on a quarterly basis. All other records such as documents will be deleted. Records in any other systems, must also be regularly deleted/destroyed. Where possible records should be kept on CharityLog so that

other files can be deleted sooner.

Business Continuity –The Amaze Charitylog database is owned by Dizions cloud-based, therefore none of its contents are stored locally. All of the data in the database is regularly backed up off-site by Charitylog. Charitylog has systems in place to ensure continuity of access to its services.

As of October 2020:

- Dizions servers are held with Rackspace in the UK.
- SkillsLogic system is hosted by memset (with UK servers): https://www.memset.com/support/my-memset/gdpr/. SkillsLogic maintain the online form to collect Compass form submissions.

7: Subject Access:

Anyone with information being processed by Amaze has the right to ask Amaze to confirm whether or not personal data concerning them is being processed, where and for what purpose and to see a copy of some or all records pertaining to them. The Data Protection Officer has the responsibility for responding to data access requests from individuals and this must be within the legal time limit of one month from receipt of the request. Amaze agrees not to charge for this service and also agrees to provide this personal data in a commonly-used and machine readable electronic format if requested.

Subject access requests may be made verbally or in writing, and all such requests must be passed to the Data Protection Officer as soon as possible. It is important for staff to recognise such a request as it may not be presented formally, it could be made in a casual way. The member of staff should clarify that they are making a formal request. The Data Protection Officer will keep a central log of all requests and if they have any doubts about the identity of the person making the request they will ask for more information in order to confirm who they are, for example asking them to provide copies of their driver's licence or passport. This will be done as soon as possible. If Amaze needs to request additional information from the Data Subject before releasing the personal data (for example to confirm their identity) the period for responding to the request will begin when Amaze receives the additional information.

Please see separate '2021 Subject Access Request Policy'.

8: Disclosure:

Amaze will be transparent with all Data Subjects about who we will share their personal data with. Amaze will share aggregated, anonymised data with our funders, commissioners and other voluntary agencies. Amaze may share personal data with other agencies such as the local authority, funding bodies and other voluntary agencies, with the consent of the Data Subject. The Data Subject will be made aware in most circumstances how and with whom their information will be shared. However, there are certain circumstances where the law requires Amaze to disclose data (including sensitive data) without the subject's consent, such as:

- **A vital Interest:** where disclosure would be used to protect the life of the individual or the life of someone else.
- **A vital Interest:** where data is shared in a safeguarding situation to protect a

vulnerable person.

- **A legal obligation:** Amaze has evidence of criminal activity

9: Confidentiality:

Confidentiality applies to a much wider range of information and data than the above Data Protection Act including: information about Amaze (finances, strategy), information about other organisations, information which is held on paper but not sufficiently structured to be a 'relevant filing system' in the Data Protection Act.

Access to all confidential information will be on a 'need to know' basis and no one should be given access to confidential information unless it is relevant to their work.

Limits to confidentiality:

There may be instances where Amaze feels it is right to break confidentiality but this will be decided on a case by case basis – e.g. if a parent was to disclose that they intended to seriously harm themselves or another person, and would have to be agreed with a Senior Manager.

Confidentiality Statement:

All staff (including temporary staff and trainers), volunteers and Trustees will be required to read and sign the Amaze Data Protection and Confidentiality statement when they take up their role with the organisation – see appendix 1 below.

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.

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.

Related Forms / Associated Documents:

Staff, Trustee, Parent Reps and Volunteer Confidentiality Agreement (see below)

Related Policies:

Please also see the following related policies:

- **Disciplinary Policy**
- **Subject Access Request Policy**
- **Information Management Policy**
- **IT Policy**

VERSION CONTROL / RECORD OF CHANGES

Review date	Version	Section	Changes/Comments
April 2022	2	All	Full Review of Policy

APPENDIX 1

STAFF, TRUSTEE, PARENT REPS AND VOLUNTEER CONFIDENTIALITY AGREEMENT

As a member of the Amaze team I understand that I must not disclose to any unauthorised person any confidential information about Amaze or any of its users (clients and their families), volunteers or staff. Exceptions can only be made with the consent of the user, volunteer or staff member, or in exceptional circumstances where there is a perceived risk to personal or public safety as laid out in the Amaze Data Protection & Confidentiality Policy. Should such a concern arise this must be discussed with a Senior Manager or the Safe-guarding lead to decide if and what information should be disclosed.

The information divulged by users or volunteers is to be regarded as privileged. Privileged information is any personal information acquired by staff affecting users or other staff members or affecting Amaze operations. It is my duty to ensure that privileged information which is divulged to them, or which they have access to, is not disclosed to any person not entitled to have such information. I understand that this continues indefinitely beyond my working/volunteering time at Amaze.

I understand that although users and volunteers may give information to, or apply for help from an individual, this information is in fact given to the organisation and any staff member giving assistance does so on behalf of Amaze as its representative. I am obliged to share privileged information with supervisors and team members who may need to be involved in providing the best possible service for a particular user or volunteer.

I understand that breach of this code of confidentiality will lead to disciplinary action.

I understand that I have a responsibility to process all personal information responsibly at all times, this includes ensuring information is accurate and kept safely within Amaze systems.

If I use personal electronic devices to view confidential information I am responsible for ensuring all files are electronically shredded promptly after use.

On termination of employment or voluntary involvement, I will return any files, documents or other papers and property of every description within my possession belonging to Amaze.

I have read and understood the Data Protection & Confidentiality Policy.

Signed…….

Print Name…….

Date…….