



for disabled children  
and young people in Sussex

## Amaze Data Protection and Confidentiality Policy

### 1. Purpose

This policy sets out how Amaze collects, uses, stores and protects (processes) personal data. Amaze is committed to respecting the privacy of our clients and families, supporters, staff, volunteers, trustees and partners. We recognise the importance of handling personal data responsibly and in accordance with data protection laws, including the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018** and the **Data (Use and Access) Act 2025 (DUAA)** which is being phased in between June 2025 and June 2026.

The purpose of this policy is to:

- ensure personal data is handled lawfully, fairly and transparently
- protect the rights of individuals whose data we hold
- provide clear guidance to staff and volunteers on their responsibilities
- demonstrate our commitment to safeguarding personal information
- minimise the risk of data breaches and misuse of personal data.

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. Scope

This policy applies to all Amaze staff, volunteers, trustees and parent representatives. It covers all data processed by Amaze with a focus on our client's data. It should be read in conjunction with the policies listed at the end of this document.

### 3. Data Protection Language

It is useful to understand the language used in data protection. It is important to remember that when we refer to data, this can be in any recorded format paperwork or electronic.

**Personal data** is information that relates to an individual making them identifiable. An obvious example would be someone's name, however, it can be something very minor such as initials but within the context of a small group membership, it could make someone identifiable.

**Sensitive data or special category data** is particularly sensitive personal data about an individual with special laws to protect this information. Amaze may keep the following sensitive data about a person:

- racial or ethnic origin
- religious or philosophical beliefs
- health data

- sexual orientation.

**Data Subject** is the person (subject) data is about. Amaze processes data for the following data subjects:

- parent carers
- children of parent carers/those supporting children
- young people engaging with Amaze
- staff and volunteers of Amaze, including trustees
- other people supporting Amaze such as fundraisers and donors
- professionals.

**Data Controller** has overall control over the purposes and means of the processing of personal data, for our organisation this is usually Amaze. Amaze is required under the Data Protection Act, as an organisation processing personal information, to pay an annual data protection fee to ICO.

**Data Processor** processes personal data. This includes any mechanism we use to process data such as third-party apps, software etc. this includes Charitylog (our client management system), Beacon CRM and Eventbrite.

**Privacy Policy/Statement** – a written statement for data subjects telling them what to expect Amaze to do with their personal information when they make contact with us or use one of our services.

#### **4. Principles of Data Protection**

The UK GDPR sets out seven key principles to handling data which Amaze holds integral to all data it processes. Failure to comply with these principles can lead to substantial fines as well as a loss of trust with our clients and partners.

- 1. Lawfulness, fairness and transparency:** personal data must be processed lawfully, fairly and in a transparent manner. This means that Amaze must have lawful reasons for processing data and be clear and open with data subjects about what personal data we process and why. In practice, all staff and volunteers must understand this for themselves so that they can explain it to our clients and direct clients to the Amaze privacy policy on the Amaze website.
- 2. Purpose limitation:** personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- 3. Data minimisation:** personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. **Accuracy:** personal data must be accurate and, where necessary, kept up to date. This is everyone's responsibility and they should correct any inaccuracies if they become apparent or bring them to the attention of the Data Protection Officer (DPO).
5. **Storage limitation:** personal data must be kept no longer than is necessary for the purpose for which it is processed. To adhere to this principle, Amaze has a records retention policy.
6. **Integrity and confidentiality (security):** personal data must be protected against unauthorised or unlawful processing, as well as against accidental loss, destruction, or damage, by using appropriate security measures. Amaze is responsible for making sure data (in paper or electronic format) is processed in accordance with this policy. Staff and volunteers must also comply by keeping information safe and secure and not to ask clients to use any system/app/software that processes client data which has not been authorised.
7. **Accountability:** requires the organisation to be responsible for and capable of demonstrating compliance.

## 5. Individual Rights

Under UK GDPR all individuals have the following rights concerning their data; there is some overlap with the data protection principles. It is important all staff and volunteers are aware of these and recognise when someone is exercising one of these rights which might be in an informal or casual manner. In all cases they should let the Data Protection Officer (DPO) know immediately, to start an official process to respond to the request.

- **Right to be informed:** the right to be informed about the collection and use of their personal data. Amaze's privacy policy clearly explains how data is collected, used and stored. Staff and volunteers should understand this statement and signpost clients to it.
- **Right to access:** an individual has the right to access their own personal data. This means someone can ask to see a copy of all the records Amaze holds on them, this could include information on Charitylog, Beacon, emails, WhatsApp messages and documents. This is called a Subject Access Request (SAR).
- **Right to rectify:** the right for individuals to have inaccurate personal data rectified or completed if it is incomplete. This links in with the 4<sup>th</sup> data protection principle, accuracy.
- **Right to erasure:** the right for individuals to have personal data erased. An individual can ask for Amaze to delete all data that they hold about them.
- **Right to restrict processing:** Individuals have the right to request the restriction or suppression of their personal data.

- **Right to data portability:** The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. For example, someone may move to a different area of the country and ask for their data to be passed to a more local organisation.
- **Right to object:** the right to object to the processing of their personal data in certain circumstances.
- **Rights related to automated decision-making including profiling:** currently Amaze does not use any automated decision making, this policy will be reviewed should this change.

## 6. Roles and Responsibilities

### Data Controller

Amaze is the Data Controller under the Data Protection Act 2018. 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.

### Trustees

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

### Chief Executive Officer (CEO)

The Amaze CEO has ultimate accountability for ensuring the organisation's compliance with data protection laws and that policies are in place and followed. The CEO oversees the Data Protection Officer (DPO) ensuring they have adequate training and resources to knowledge on data protection law and practices. The CEO with the DPO ensures data protection training takes place within the organisation.

### Head of Services

The Amaze Head of Services supports the DPO in carrying out tasks. Along with the CEO they will lead on DPO tasks such as data breaches when the DPO is unavailable.

### Data Protection Officer (DPO)

The Amaze Data and Performance Manager takes the role of DPO, reporting to CEO and Amaze Board of Trustees on data protection issues, risks and mitigation. The DPO is responsible for:

- monitoring data protection issues
- keeping up to date on data protection law
- reviewing this policy and associated policies
- advising staff and volunteers on data protection issues
- leading on:
  - data breach responses
  - subject access requests
  - data portability requests

- right to erasure requests
- data protection impact statements
- records of processing and lawful basis (ROPA).

### **Amaze staff and volunteers**

All Amaze staff and volunteers are required to read and sign this policy. Training is rolled out periodically when data protection law changes or when a training need/refresher has been identified. Focus sessions are held at team meetings and staff away days as needed. In addition, data protection and information governance are standing items at manager meetings to address any current concerns. Individuals are responsible for following this policy, including safe keeping of all personal data. Where this policy is breached, this will lead to an investigation and the Amaze disciplinary procedure will be followed where necessary.

### **7. What Personal Data We Collect**

Different services and departments collect different data. Client services collect the following information:

- parent carer (PC) and child or young person (CYP) contact details
- demographics including some special category personal data: gender, age, date of birth, ethnicity, sexual orientation, religion, sex at birth
- GP surgery, school or education
- PC and CYP health information including diagnosis, conditions, pathway stages and access needs
- details of contact with Amaze services, including attendance at in-person and online events
- financial information may be held by the DLA and PIP service, including benefit awards.
- Amaze HR and finance department collect:
  - staff and trustee contact details
  - staff demographics including health conditions
  - bank account details, national insurance numbers, eligibility to work in the UK.

### **8. How We Use Personal Data**

#### **Purposes**

The personal data collected for PC and CYP is used to offer support from different Amaze services. The information is consolidated, anonymised and provided in reports for funders and Amaze analysis to evidence the work done by Amaze and to analyse the reach of our services. Any reports containing groups of 20 individuals or less, will have this information redacted if it is to be published in a public forum; to remove the possibility of a person or family being identified. This data informs Amaze and funders on areas of need and can identify gaps in provision. Amaze upholds the protected characteristics defined in the

Equality Act 2010 and its equality duties are applied alongside our data protection obligations under the UK GDPR.

Anonymised case studies may be used to describe the circumstances faced by clients and evidence the impact of our services. If the case study is to be used for publicity such as on the Amaze website, the permission of the client will be sought in writing.

Services funded by the NHS are required to submit partially anonymised data to the Mental Health Services Data Set (MHSDS). Legally consent could be implied as NHS Digital is exempt from some data protection regulations, however, Amaze chooses to be transparent about this, giving clients an option to “opt out” of this dataset. Clients are directed to an Amaze webpage explaining about this consent, <https://amazesussex.org.uk/data-sharing-nhs/>. If a parent carer has chosen not to ‘opt-out’ for one child it will be assumed this applies to all other children they ask for support about. The data shared is about the children and young people directly or indirectly supported by services funded by the NHS. In addition, there is a national data opt-out scheme where individuals can opt out of any of their NHS data (including the data we pass to the NHS) being used for secondary purposes for research and planning. This is the same for all data held by the NHS and they should be directed to <https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/>.

The personal data collected by HR and the finance department, ensure that staff are employed legally and paid and provided with access needs to support their roles. The information, with the consent of the employee may be used to perform a Disclosure and Barring Service (DBS) check. Demographic information is used to analyse the diversity of the Amaze staff team.

### **Legal Bases**

To comply with data principle 1, Amaze must have lawful bases (reasons) for processing client data. We use different lawful bases for different types of data and for different circumstances.

### **Consent Article 6(1)(a)**

Consent has to be explicit; it can be verbal or in writing (including a tick box on an online form). Consent can be withdrawn by an individual at any time.

Consent is the basis for much of the personal data we collect, this is where we ask explicit consent from an individual to process their data and their children’s data. When asking for consent an individual should always be made aware of the Amaze privacy policy. Whenever, someone completes a referral online, they are directed to the privacy policy and must consent to Amaze processing their data. When someone accesses Amaze in another way we will ask and record their consent against their Charitylog or Beacon record.

Amaze collects data about the children with special educational needs and disabilities (SEND) of parent carers they are supporting. Where the child is under 16 years or if the

young person lacks capacity to consent for themselves, we will follow the principles set out in the Mental Capacity Act 2005. We will ask the appropriate decision maker, which is usually the parent carer, to consent to sharing the child or young person's data. Where the young person is over 16 years and has capacity to consent, we ask the parent carer to check the young person does consent. This approach is in line with recommended practice by the SEND Information, Advice and Support Services Network (IASSEN). Once a parent carer has consented for their child's data to be processed by Amaze, and they go on to share details of their other children for Amaze's support, we can assume their original consent applies to these children, as they have already been directed to the Amaze privacy policy.

Where sensitive/special category data such as religion is asked, the client must always be given the option to decline with a "prefer not to say option" this is to ensure their consent is true.

We also ask for consent for certain email communications and to use photos and videos. This consent is granular, meaning that they are all individual statements a person can agree yes or no to.

We ask for consent to contact people about the following:

- Amaze e-newsletter
- targeted emails: emails sent about issues, activities, surveys Amaze thinks the family may be interested in, this might be based on the information they have given us, such as their location or child's needs
- Compass news, offers and updates
- fundraising.

We also provide an option to opt-out of sharing information with NHS MHSDS (section 8).

We may also ask clients if we can use their photographs or videos in publications and marketing and if the photographer can use the images in their portfolio.

### **Legitimate interests Article 6(1)(f)**

We require some data to be able to support a client, if they chose not to consent to this information, we could not provide a service, therefore consent as a legal basis does not apply and for these the legal basis is legitimate interests. A legitimate interest assessment is carried out by Amaze for all data using this legal basis and includes:

- address details
- health data of a child or young person (CYP)
- GP or school of a child or young person
- emergency contact details for a young person accessing an Amaze service directly.

Amaze uses Article 9(a) explicit consent to process CYP health data under this basis.

### **Public Task Article 6(1)(e)**

The SENDIAS service is commissioned by local authorities to carry out the statutory advice service. To carry out this service we need to process data about parent carers and their children with SEND. For the special category health data of a CYP needed to access SENDIASS, Amaze uses substantial public interest condition Article 9(g)(6) Statutory and government purposes.

We still aim to ask for consent for individuals as this allows them to access all Amaze services, but it does allow SENDIASS to process data when consent has not been possible. For example, a parent carer emails SENDIASS asking for advice, the SENDIAS service can record their work on Charitylog without explicit consent. It is important that each service checks consent has been recorded on a client's record when they start working with them and not to assume it has already been obtained.

### **Contract Article 6(1)(b)**

Contract is used as a legal basis for some specific purposes where there is a contract between Amaze and the individual.

- individuals when they sign up to the Amaze lottery
- individuals registering for the Compass card
- employees who have an employment contract with Amaze

**Legal Obligation Article 6(1)(c)** is also used for employee records, for example the legal obligation to report salary records to HMRC.

## **9. Data Security**

Personal data about families are 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 usernames and passwords. All staff must be trained on Charitylog and have read and signed this document before using the system. 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 made inactive.

Whenever possible, any file containing personal data will be stored electronically on the Amaze Charitylog database, in preference to the Amaze SharePoint, One Drive or on paper; avoiding the replication of information in other formats that are hard to control. Any personal data stored in computer files instead of the Charitylog database, must be stored in a folder marked "PERSONAL DATA" and this should be password protected/have limited access.

Any physical client records should be stored in lockable filing cabinets and/or a lockable room, with the key stored in a locked key safe when the office is closed. Client records should only be removed from offices in infrequent circumstances and the minimal paperwork possible. This could be the names and contact details of clients attending an

event or workshop. If an advice worker is attending a meeting about a client or is visiting their home to complete a benefits application a larger case file may be needed. In all circumstances, files must be kept in a folder clearly labelled 'PERSONAL DATA – do not open, if found please contact Amaze immediately'. Extra care should be taken when using public transport, that no one can oversee the file and that it is not left behind accidentally. If left temporarily in a private vehicle, it should be out of view and the vehicle locked. Client records should not be kept at a staff member's home address without the express permission of their manager and safeguards put in place.

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. Even on an Amaze device sometimes it may be necessary to download a file to access it, such as an attachment from Charitylog. Download folders are usually not part of the shared drive. If a file has been downloaded, it must be either moved to a One Drive folder or electronically shredded after use. Details of shredding software options are available from the Data and Performance Manager and how to shred is covered in staff training.

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.

We operate a 'clear desk' policy in Amaze offices which also applies to electronic folders not on the One Drive. No paperwork containing personal data must be left unattended, it must be locked away in approved locked filing cabinets and shredded after use. Care should be taken not to leave any papers on or next to office printers, photocopiers or scanners. Staff should always lock their computers when leaving their desk for any period (Ctrl + L).

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?

Any staff member signing up to a third party needs to assess whether it will be used to hold or process personal data. If it will collect personal data, a Data Protection Impact Assessment must be done, stating what personal data will be held and why. A schedule to delete personal data from the third party must be put in place. The third-party policies must be read to identify if they are UK GDPR compliant, where they store data and if it is transferred outside of the UK.

By preference the server would be based in the UK, if it is not, the country must either meet 'full adequacy' or 'partial adequacy' with safeguards in place. Full and partial adequacy are detailed on the ICO website. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/adequacy-regulations/is-the-restricted-transfer-covered-by-adequacy-regulations/>

## 10. Data Retention

Client records are retained for different periods depending on the level of interaction with Amaze and if a child was under 18 years at the time they first accessed Amaze services

For:

- parent carers and their associated child or young person records
- young people aged 18 years or older when they first access an Amaze service.

Records will be kept for **6 years** from the last contact (referral closure date) where they have received support from an Amaze service including advice, benefits support and in-person activity.

For:

- children or young people aged under 18 years when they first access an Amaze advice service or a young person's activity service.

Records will be kept up to their **25<sup>th</sup>** birthday or **6 years** from their last contact, whichever is longer.

For:

- all other client records where there has been no advice or in-person activity
- a young person record aged over 25 years who Amaze has not supported directly.

Records will be kept for **3 years** after referral closure date. Compass referrals are closed at expiry.

We are required by advice standards to keep records for 6 years. This period also allows for developmental changes a child or young person goes through, when support from Amaze may be needed, providing continuity is beneficial to the family.

Child records for children receiving direct support are retained for a minimum until their 25<sup>th</sup> birthday in line with child protection guidance (Information and Records Management Society (IRMS), 2019).

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

**Data Archiving** – after the retention period has ended, records held on Charitylog, will be anonymised, removing all personal identifiable data. 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.

## 11. Exercising Individual Rights

### Right to Access/Subject Access Request

Anyone with information being processed by Amaze has the right to ask Amaze to confirm whether 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 DPO 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 to provide this personal data in an accessible format.

Subject access requests (SAR) may be made verbally or in writing and must be passed to the DPO immediately. The request may be in an informal way and staff should clarify with the client that they are making a formal request. The DPO will keep a central log of all requests and if there are doubts about the identity of the person making the request, they will ask for formal identification and where applicable proof of relationship to children. 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.

If a request is made by a parent carer about their child and the data Amaze holds has been provided by another parent carer, the case will be considered carefully. Looking at the age of the children and if they are able to consent themselves to the information sharing, the reasons for the request and if it is in the best interests of that child.

For further information see 'Subject Access Request Policy'.

### **Right to be Forgotten/Erasure**

An individual may ask Amaze to erase/remove their personal data at any time; this may be in an informal way and staff should recognise the request and inform the DPO immediately. We will respond promptly (at the very latest within one month) ascertaining the data they want removed. We aim to comply with all requests, but for each we will check the request is not excessive and that information such as safe-guarding evidence will not be lost. Where a parent carer asks for data about their child to be erased, if significant casework has taken place, we will consider whether there are any implications to Amaze in removing that data. If that child is now over 16 years, we may ask them directly if they would like their data removed even if the information was originally obtained by their parent carer. This would be if we thought it might be detrimental to the young person to delete their data, for example, they may want to make a benefit claim themselves. Where information has been given to Amaze about children from another parent carer, then the request will be discussed with them, unless there are safeguarding concerns. A decision to remove the data will be based on the best interests of the child.

### **Right to be informed**

Everyone accessing Amaze should be directed to the Amaze privacy policy. This should be kept up to date and written in a clear and accessible way. An accessible version is made available to young people on the Amazing Futures website. Staff should consider if there are accessibility needs which might stop a client from understanding the policy.

### **Right to Rectify/Accuracy**

All staff and volunteers are responsible for recording client information accurately and recording clear and concise client records. Where possible staff should confirm that details are up to date, especially where someone has not been in contact with Amaze recently. If there are any errors these should be rectified immediately. The Data and Performance

Manager is responsible for data integrity and data cleansing.

## 12. Data Breaches

A data breach is when any personal data is accessed or shared with an unauthorised person. There can also be an 'availability' data breach if information was not available when needed which has a significant negative impact on an individual. For example, if data is locked by Ransomware stopping it becoming available. A breach could be via a cyberattack, theft, loss or accident as well as using unapproved sharing methods (e.g. insecure email). Steps are taken to keep all electronic data secure from cyberattacks by Amaze IT providers and all staff and volunteers must use the authorised software and hardware provided by Amaze. Laptops are protected by BitLocker codes to reduce the likelihood of a data breach should a laptop be lost or stolen.

Staff and volunteers must use the authorised software and hardware provided by Amaze. They must use strong passwords for accounts and shutdown their laptops when moving between sites, to ensure the BitLocker is effective. Use of public Wi-Fi (eg Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) could be unsafe and lead to unauthorised access of personal data. Below are guidelines on using public Wi-Fi to access Amaze records.

- Do not use Wi-Fi that does not require a password or login.
- Usually the public Wi-Fi will ask for an email address and this means a proper guest network is typically in place, where each user is allocated their own space and each device is isolated.
- Do not use public Wi-Fi to access Amaze records on non-Amaze devices, unless this has been risk assessed and approved by a Senior Manager, this is because Amaze devices have inbuilt firewalls to add protection.
- If the Wi-Fi ever asks do you want your device to be "discoverable", always select "no".
- If something is "off" about the Wi-Fi or the establishment offering it, do not use it!

To minimise the risk of an accidental breach in personal data, all staff and volunteers should be trained on data protection, keeping information safe and minimising personal data sources. In particular, only storing personal data in agreed formats such as Charitylog and Beacon. The fewer places containing personal data, the less likely it might be accidentally shared.

Staff must always consider whether a communication contains personal data and if that personal data could be minimised or removed altogether. The Charitylog reference (ID) should always be used instead of names when communicating internally. When emailing or writing to a parent carer make language as generic as possible.

Guidance on emails:

- avoid including personal data in an email subject line
- use the Charitylog reference or Beacon person ID, instead of names in internal communications. Take care if you include initials. Whilst adding initials can be useful, make sure they do not make someone identifiable, for double barrelled names use the first letters only, SH-K is much more identifiable than SH.
- minimise personal data in communications to families, keeping language generic.

When replying or forwarding an email:

- minimise personal data from the original thread by deleting data such as date of birth, this reduces the risk of breaching data someone else has shared and reduces the copies of personal data created by long email threads.
- remove any personal data from the original subject line, such as child name.
- check all the recipients, has anyone been copied in inappropriately? If you are not sure, remove them.
- check the full thread of an email before forwarding that you are not inadvertently passing on anything you should not share.

The most common data breach incident at Amaze is group emails being sent to recipients in using the CC instead of BCC field. Analysis shows that these incidents usually happen when a staff member feels under pressure, is tired, is unwell or is working outside their working hours. The impact of this type of data breach:

- email addresses are shared with others.
- email addresses often show a person's name and may show their place of work in the domain name.
- knowing another person has received the email, implies that person also has a child/ren with those health needs.

Below are steps that can be taken to reduce the risk of this type of data breach and the impact of such a breach if it is made. If a group email must be sent:

- consider using Brevo (bulk email software) to negate the risk altogether. Though for a small number of email recipients this may not be the best choice as emails may go into spam folders.
- using Outlook email merge, negates this risk, but does involve the technical knowledge to do so, you can ask your manager for training
- consider if the emails can be sent as a batch from Charitylog, this can be done in some circumstances, discuss with the Data and Performance Manager
- make sure Outlook is setup so that the BCC field is always visible, as a reminder
- if you have to add the email addresses manually in Outlook, use the BCC field and then ask someone to check that you have done so. *Always* triple check before pressing send.

- consider using Outlook delay delivery function (Options/Delay delivery) to allow for time to fix an issue before the email is sent

Amaze accepts that data breaches do occasionally occur and whilst all employees must exhibit dutiful care, Amaze encourages an open culture where staff and volunteers feel safe to report errors and incidents without a fear of blame. All breaches must be reported to the DPO immediately. Actions will be agreed to minimise the impact of the breach. Each case will be logged, reviewed and investigated. The DPO and CEO review data breach cases, looking at root cause analysis and lessons learned.

### **13. Confidentiality**

There is an overlap in data protection and confidentiality, confidentiality is broader than data protection and extends beyond personal data into organisation plans and finances.

Confidential information does not have to be in a recorded format; it could be part of a conversation.

Confidentiality covers:

- information about Amaze, for example, its plans or finances
- information about other organisations
- information about volunteers and staff whether recorded electronically or in paper form
- information about clients, their files and supporting documents.

Amaze is committed to providing a confidential service for our clients, it is important in establishing a relationship of trust. Ensuring personal details are kept private and not passed on to a third party without the express consent of the individual. All Amaze staff and volunteers must respect the need for the confidentiality of information held about anyone who comes into contact with the organisation; this continues even after contact with a person has finished or someone leaves Amaze.

#### **Example of a breach in confidentiality:**

A parent carer, Mary, attends an Amaze coffee morning, she is feeling isolated and mentions to a staff member, George, that her child goes to a certain nursery. George knows another very friendly parent carer, Amy, whose child with similar needs to Mary's, also goes to that nursery. George sees no harm in sharing this knowledge with Mary, saying he is sure Amy would not mind Mary approaching her, he describes what she looks like and gives Mary's child's name. This is both a breach of confidentiality and data protection law (George has access to this personal data recorded on Charitylog). In this situation, George could have said he would see if he knew anyone in similar circumstances and if so, would Mary like to be put in touch with them. He could then make a similar request to Amy, gaining consent.

## **Breaching Client Confidentiality/Data Sharing**

On rare occasions and in specific circumstances it may become necessary to breach confidentiality. These circumstances include:

- if a member of staff believes that a client could cause danger to themselves or to others
- if a member of staff suspects abuse or has knowledge of abuse
- if a client gives information which indicates that a crime has been committed
- if disclosure is required by law, for example, by the police
- if a person is felt to lack the mental capacity to make a decision. In such cases staff or volunteers will discuss with a manager and they will only act in the client's best interest
- if the client gives information which indicates a possible terrorist threat.

The decision on whether to break confidentiality should be decided on a case-by-case basis and always in conjunction with a senior manager. Details of what is shared and the circumstances must be recorded on Charitylog and/or the safe-guarding log. Appendix 1 holds details of the legislation supporting a breach in confidentiality.

## **Client Consent to Share Information with External Agencies**

Excluding the special circumstances above, information should only be passed to another agency or to anyone outside of Amaze with the explicit consent of the client, where possible this will be with written consent. This should be clearly recorded on their Charitylog record. Similarly, client consent must be gained if an Amaze service intends to get information from another agency.

The benefits service must obtain consent from clients before sharing files with Advice Quality Standard (AQS) assessors carrying out file audits and this must be recorded on the client Charitylog record.

## **Keeping Confidentiality**

Everyone should be aware of their surroundings when discussing a client case or talking with a client, on the phone, in-person or on a video call. Being careful not to accidentally breach confidentiality because someone else can overhear, via an open door, window or someone else in the room. Those working from home should only make client phone calls or discuss a client case in a private room. Those working in an office, should check that there are no other clients or non-Amaze staff in the room, keeping the volume of their voices down.

If a case is to be discussed externally for example, for advice, care must be taken not to share any personal details which could identify the person.

If a client asks someone to act on their behalf, e.g. bringing in or collecting documents, it is the adviser's responsibility to ensure that permission has been given and to record this on Charitylog.

Amaze should be careful not to disclose someone accesses the service without a client's consent. This includes a:

- partner
- members of the extended family
- children
- friends
- the police or social services except where the circumstances in the 'Breaching Client Confidentiality/Data Sharing' has been agreed with a senior manager.

Care should be taken when leaving voice messages or mailing information, if a client has stated there are confidentiality issues, such as a shared residence, or if others can overhear.

### **Confidentiality within Amaze Services**

The client's right to confidentiality applies to prevent details of their case being released outside Amaze. Within Amaze only members of staff and volunteers involved in providing information, giving advice or supervisors:

- should access a client's record
- should take part in discussions relating to the enquiry.

Amaze has not configured Charitylog to limit access to particular records, as the nature of the organisation is such that a family can benefit from multiple Amaze services. However, an audit trail is recorded for every user of Charitylog and what records they have accessed. Anyone found accessing records inappropriately is subject to the disciplinary policy.

Employees who need to raise a concern about the behaviour or practice of colleagues or partner organisations should follow the 'Whistleblowing Policy' to ensure confidentiality is not breached.

### **Trustees and confidentiality**

Trustees do not have access to client records unless they are acting as supervisors, legitimate file reviewers or advisors.

Trustees should:

- read and sign this policy
- have responsibility to deal with any potential breach of confidentiality
- be responsible for ensuring that the confidentiality policy is implemented.

Issues around individual clients should not be discussed by the whole Board of Trustees unless it is to deal with a complaint, breach of confidentiality issue or another issue which fits into the Trustee/Management Committee's strategic role.

## **12. Training and Awareness**

All staff, volunteers, trustees and parent representatives are required to read this policy during their induction. If they understand the policy they must sign the agreement, appendix 2. This will be saved on their HR record. If they do not understand the policy, they

should discuss with their manager before signing. Whenever the policy is significantly changed staff will be required to re-read the policy and this will be monitored via SafeHR. The may exception for volunteers where their interaction with Amaze does not include client contact/contact with client records, for example, volunteering at a fundraising event.

At induction, staff and volunteers must also complete online cybersecurity training, <https://www.ncsc.gov.uk/training/top-tips-for-staff-scorm-v2/scormcontent/index.html#/>

Training and awareness sessions are run at away days and in staff meetings. Information governance is a standing item at SLT, AMT and team meetings where any concerns, issues or questions can be raised.

### 13. Policy Review and Updates

This policy is reviewed every 2 years or sooner if there is a law or policy change.

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.

#### 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
- Privacy Policy
- Subject Access Request Policy
- Information Management Policy
- IT Policy
- Quality Policy
- Whistleblowing Policy

#### VERSION CONTROL / RECORD OF CHANGES

Review date	Version	Section	Changes/Comments
April 2022	2	All	Full Review of Policy
Nov 2025/Feb 2026	3	All	Full Review of Policy/Update

## **Appendix 1**

There are several key pieces of legislation that directly or indirectly relate to when we breach client confidentiality.

### **Terrorism**

The legislation regarding terrorist activities is constantly changing and being updated by Government. **The Terrorism Act 2000, The Anti-Terrorism Crime and Security Act 2001 (ATCSA), Terrorism Act 2006, Counter Terrorism Act 2008, Terrorism Prevention and Investigation Measures Act 2011 and Counter Terrorism Act 2015** and other more recent legislation have made it a criminal offence to fail to disclose information that could help prevent or prosecute terrorism.

### **Drug trafficking**

**The Drug Trafficking Act 1994** makes it a criminal offense to fail to report suspicions of drug-money laundering gained during the course of contact with a client.

### **The Social Security Administration (Fraud) Act 1997**

Amaze must not knowingly assist with a fraudulent claim for benefits in any way.

### **Child Protection Legislation**

The Children Act 1989 (updated 2004), Protection of Children Act 1999 and Safeguarding Vulnerable Groups Act 2006 are just some of the relevant pieces of legislation regarding the protection of children.

### **Police and Criminal Evidence Act 1984 (PACE)**

This Act gives the police powers, lawfully in any premises to seize anything they reasonably believe is evidence in relation to an offence under investigation which otherwise might be concealed, lost, altered or destroyed.

## Appendix 2

### 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 Designated Safeguarding 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 always process all personal information responsibly, 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:	