Early Education
The British Association for Early Childhood Education

Data protection policy

This policy sets out what personal data we hold, how we store and process it, how we maintain it including when we delete data. It includes as annexes additional policies on how users can request to see what data we hold about them (a "subject access request") and what we will do if any data is disclosed to people who should not have access to it (our "data breach policy").

Personal data and how we collect it

Information collected via the website and cookies

Our website we may collect information about users through recording information put into the website, users' IP address and also through the use of cookies. Cookies are small files stored on a computer, which tell us about the user's browsing history. Our site uses cookies to keep track of users' online shopping cart. We use cookies to identify users so they can retrieve information and don't have to re-enter it each time they visit our site.

If users register with us or if continue to use our site, they agree to our use of cookies. They can stop cookies from being downloaded by changing the settings in their internet browser. This may affect the functionality of the site

Customers and service users

If users register to receive our emails or purchase a product or service from us, including becoming a member or supporter, we will store the information which we need to process their mailing subscription request and/or order, which they may give us via online forms, on paper or by phone, on our contact database and online shop. We also hold details about customers and suppliers on our finance database. We are required to keep financial records for six years.

Staff, volunteers, contractors and suppliers

To comply with contractual and legal requirements, we may hold personal data about staff, volunteers and contractors including where relevant national insurance number, UTR, evidence of right to work, bank account details for payment of salaries or expenses. Where suppliers are sole traders, we may hold personal details such as contact and bank details.

What data we collect

The information we collect is likely to include name (first name, surname, title, honours), contact details (address, phone, fax, email), job title/role, organisation (if applicable) and mailing preferences such as whether users wish to receive email updates about campaigns, products and services or local branch events. In the case of event bookings, we may also collect data such as dietary and access requirements. If one individual books an event on behalf of another person we will hold the details supplied for that person as well.

We may also hold information about bank details (if members pay via direct debit, or if suppliers/contractors have asked us to pay them direct to a bank). Any bank details are held securely and are separate from our main contact database. In the case of Direct Debit payments, these are either held securely via a third-party system (Go Cardless) or for legacy users of our previous Direct Debit arrangements, these are held within our own systems in a restricted access area of the server until all users have transferred over.

For those closely involved with Early Education, we hold information as to their roles eg trustee, patron, Associate, branch officer, staff member, and any branches with which they are associated. In the case of trustees and Associates we hold a professional profile and (for Associates only) a photograph.

We may also collect and store digital images of indivduals eg pictures of children used on our website and publications. We will obtain permission to store and use these photos from the individual or the child's parent/carer and will inform them of their right to contact us and retract that permission at any point in future.

On what basis we process data

If users have purchased a product or service from us, we process their data on a contractual basis in relation to the contract with us to deliver that product or service to you. Their data must only be processed in relation to that purchase and any relevant follow up.

For all other purposes, we will only process users' data if they give us explicit consent for us to use it for specific purposes, namely to keep them informed about our campaigns, to send updates about our products or services, or to receive updates about their local branch's activities.

All mailings must therefore be made using pre-agreed filters on the database to ensure they are targeted only to those to whom they may legitimately be sent. Where possible, these filters are pre-set.

What we do with users' data

We use the information we collect about users to:

- improve their browsing experience of our website
- process orders for goods or services, eg membership, books, training courses or events
- send relevant news and updates to those who have opted in to receive these
- analyse use of our services.

We will only use data to contact individuals to tell them about new products and services that may be of interest, or to send updates about our activities if users have given us consent to by opting in to receive such updates, or if we have a contractual basis to do so (eg membership), or a legitimate interest justification eg that headteachers of nursery schools should be kept informed of the activities of the APPG for nursery schools. Such emails will be sent in a format that ensures users cannot see other recipients' email addresses (usually via a managed email service,

or alternatively by “bcc-ing”), and will include information about how to unsubscribe from future mailings.

We will not pass information to any third parties for their own use, but we do contract some of our services to third-parties, eg our mailing house and outsourced finance provider, who process data on our behalf in order to send out our mailings and process our financial transactions as required. Any organisations which process data on our behalf are required to comply with the General Data Protection Regulations and our data protection policies. Any data sent to such organisations must be sent securely eg in password protected files, with the password emailed separately.

Updating and deleting data

All data must be stored in line with legal requirements, such as that we must keep records of all financial transaction for six years. We will delete personal data once we no longer need to store it for such purposes, if we do not have current permission to use the data to keep users in touch with our activities and services.

We will aim to keep our records up to date through periodically asking users to reconfirm that their details are correct and that they still wish to hear from us. We will monitor bouncebacks from emails and returned post and attempt where possible to obtain updated contact details in such cases. Where updated contact details cannot be obtained, we delete from individual records on our database any contact details which are no longer current, or mark records to indicate where emails have bounced.

Requests to update or delete information

Users can unsubscribe from our email list, update their mailing preferences or correct the contact information we hold by logging into their user account or contacting us by phone, email or post. They may request deletion of data, and this will be actioned unless we are legally required to keep those records to meet legislative requirements eg in relation to keeping financial data. Where this is the case, we will let users know what data we are holding, why we cannot yet delete it and when we will be able to do so.

Where there is a financial transaction attached, user accounts may be deleted, provided that the order details are retained. Where the user is a former member, basic membership details can be retained but anonymised, ie personal data can be removed such as phone numbers and postal addresses. Email addresses can be deleted, but as the database requires a unique email address as the identifier for each user account, it must be replaced with a placeholder eg “no-email@formermember123.com”. Our database has facilities for bulk automated deletion and anonymisation of user accounts which should be used to ensure the deletion or anonymisation is carried out on a consistent basis.

Who has access to personal data

Access to our contact database is restricted to Early Education staff and volunteers who need this to carry out their work. Early Education branches are given access to

up to date lists of members for their branch, but these do not include contact or other personal details. Our outsourced finance support company has access to our online finance system, which includes contact details for customers and suppliers where needed. Where third parties need access to data to perform outsourced functions such as print or online mailings, we must have agreements in place to ensure they understand their obligation to comply with GDPR regulations as data processors on our behalf. They may have access only to subsets of data which are necessary to carry out the contracted task, and on a time-limited basis, eg in the case of a mailing house they must undertake to delete copies of mailing lists once mailing have been sent out.

When we would disclose data

We must not disclose data to third parties unless legally required to do so. Any requests from authorities such as the police or HMRC for release of data should be referred to the Chief Executive, or in her absence to the Chair of Trustees. The legal basis for any request should be checked – staff should not assume that we are legally required or permitted to hand over personal data just because such as request comes from an official body such as the police or HMRC.

Security and risk management

We have security measures in place to protect the loss, misuse and alteration of the information under our control. We have procedures and security features in place to prevent unauthorised access and use of personal information.

All personal data is kept securely. Our online contact database, online documents and finance system are password protected and restricted to those staff and contractors who require access. Any staff records kept in hard copy are stored in a locked cabinet.

The main risk of data breach would be if an unauthorised party were to hack into any of our online systems. We minimise this risk by ensuring that online security systems are regularly updated against any known weaknesses. Passwords are kept securely and updated periodically. All our data systems are regularly backed-up at a separate location to the online servers on which they are held.

All staff will be familiarised with this policy as part of their induction, and given additional training as needed.

Last updated: 21 September 2018

Annex 1: Data breach policy

The ICO defines a personal data breach as “there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.”

If any staff member discovers that there has been a personal data breach they should inform the Chief Executive who will be responsible for determining whether it poses a risk to the rights and freedoms of those whose data was affected. If so, the Chief Executive will ensure that the organisation:

- informs data subjects of the actual or potential data breach, the data concerned, and the circumstances in which this occurred and any steps which have been taken in mitigation, and to ensure future data security
- informs the Information Commissioner’s Office within 72 hours
- informs the Charity Commission
- informs the Trustees of the data breach and the steps which have been taken in response, including whether the ICO has been informed.

If the data breach is not deemed to pose a risk to the rights and freedoms of the data subject, it may still be necessary to take action in mitigation. The Chief Executive will determine what action is necessary, which may include any of those listed above.

Any data processors acting on Early Education’s behalf will be informed of this policy and required to comply with it as a term of their contract.

Annexe 2: Policy on dealing with subject access requests

Anyone whose personal data we hold is entitled to ask us what information we hold on them. This is called a Subject Access Request in the General Data Protection Regulations, but enquirers may not use that terminology when contacting us. It is important that staff recognise that if anyone requests details of the personal data we hold on them, that we recognise this request must be treated as a Subject Access Request. We are legally required to respond to Subject Access Requests within 30 days.

We must ensure that the person requesting access is the person whose data is being requested eg by ensuring it is sent only to the email address or postal address held on our records, or by requiring the person to provide proof of identity. Enquirers may not make subject access requests for any adult other than themselves. The only circumstance in which we might be asked to provide an individual's data to an enquirer claiming to make a subject access request on their behalf would be where a parent or carer is enquiring about images of their child. Under GDPR they have a right to ask what images they hold, and at any time to withdraw permission for us to hold and use these. Such requests should be dealt with under this policy.

In the first instance, where data is held on our online database, enquirers may be directed to login as a user via www.early-education.org.uk/user to see what data we hold on them. They may need assistance with verifying they are using the correct login, or with resetting their password.

If they are unable to access the database, or we hold additional data about them which they cannot access via that route, eg on the finance system or elsewhere, we need to provide a list of the information held.

If they are enquiring about photographs, they will need to provide sufficient information about the child to allow us to identify any images we might hold of them (eg nurseries which they attended, the approximate date when photographs were taken and permission for their use given, as well as the name of the child). On request, any such images should be removed from our image library and any electronic locations in which they are used or stored.

If the request is manifestly unfounded or excessive, we have the right to refuse it, or to charge the enquirer for the staff time which would be involved in complying. If we do so, we must inform the enquirer they have the right to complain to the Information Commissioner's Office, or to the courts.

Annexe 3: Branch administration FAQs

How do I send out notifications of meetings?

Email details to head office, or ask for training on how to do this via the pre-selected lists on the central database. Emails are sent out via a third-party email service (Mailgun) which ensures that emails are appropriately branded and individualised, including links to allow users to unsubscribe with a simple click.

How can I check whether attendees at a branch event are members, or get a list of branch members?

Branch officers can download the most up to date list whenever needed via:

https://www.early-education.org.uk/reports/branch_officer/

These lists are to be used on a time-limited basis by branch officers for the purposes of branch administration eg to check eligibility for member rates. Updated lists should be downloaded as often as needed, and older versions destroyed. The report lists all current contacts for the branch including names, organisations and membership status.

Will all local members be included on the list?

Any members whose database record flags membership of the branch will be included on the list. If members do not appear on the list or are not receiving branch notifications they should check their record correctly shows the branch link, that the email given is correct, either by logging in to www.early-education.org.uk/user and checking their user profile or by phoning head office. They may also need to check that email is not going to their junk folder.

How can non-member contacts be added to branch circulation lists?

Contacts can sign up and add themselves to the database via www.early-education.org.uk/user where they can specify which branches they want updates about (as well as whether they would like updates from the national organisation).

May branches hold their own contact lists eg of non-member contacts?

Branches may not hold their own lists of contacts because of the data protection issues that this creates and the difficulties of ensuring branch and central records are both up to date. Please talk to head office if this raises any issues.

Can I keep lists if these are solely organisational contacts?

Email addresses containing names of individuals (eg joan.smith@borsetshire.gov.uk) count as personal data and therefore fall under GDPR. Branches should include these in the central database as above. If special arrangements are needed to keep lists of organisation contacts which will circulate event details to their own lists of local schools and settings, ie where these emails include names, please discuss with head office how this can be done in keeping with our GDPR policy.

Email addresses which do not contain names eg (admin@borsetshire.gov.uk) are not covered by GDPR, so lists of these can be kept by branches for circulation purposes if they are not linked to individual named staff in the records held by the branch. If a branch wishes to keep a list of contact names as well as generic emails, as above, please discuss with head office.

What data should we collect when taking bookings for branch events and how should these be stored and processed?

Branch officers will need to collect some personal details from contacts as part of their regular event bookings administration, eg to send confirmation of events, provide invoices or chase up payment. These should include only the personal details needed for the organisation of the meeting (which could include contact details in case of cancellation). Financial records must be kept for six years, including lists of those attending events and the amounts charged, and copies of invoices and receipts. If any personal details (phone number, email, etc) are collected separately to the financial records, these should not be kept.

Do we need to change any practices in relation to email correspondence?

Branches can continue to enter into email correspondence about event bookings etc as normal. However, branches should not keep email circulation lists for the branch (see above), and any lists of emails compiled in relation to a single event should only be used in relation to that event and then deleted, not stored as part of a generic contact database. Where possible branch correspondence should be sent from a branch email address, not a personal one.

Branch officers can respond to those who book onto branch events at whatever email they wish to be contacted on, provided the recipients' addresses are not added to any lists other than those related to the relevant event.

Can branch officers send out event notifications to their own personal contacts?

Anyone sent a notification of an Early Education event could forward that on to their own contacts in a personal capacity. However, branch officers need to have a clear distinction between any records they keep as part of administration of the local branch, and any personal records. Many branches use a dedicated email account for branch correspondence, and this is recommended to avoid confusion. Similarly, any address books or lists including personal data need to be clearly demarcated – branch data must not be used for personal purposes, and must be stored and processed in accordance with our Data Protection Policy.