British Association of Educational Audiologists (BAEA)

GDPR Policy

What does GDPR mean for BAEA?

Data Breaches.

A breach – is the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The above can cover anything, from the loss of a laptop, email addresses being shared in error - often using the to: or cc: field - to confidential information sent to the wrong address or access to systems that a BAEA member has no right to access.

It is worth knowing that until breaches are confirmed they are often referred to as data protection incidents. If you suspect a breach has occurred you must contact the BAEA data protection officer (DPO) email: simon_blake@tiscali.co.uk.

If any of these occur then the greatest loss to BAEA will be reputation and trust. The sooner the DPO is aware of an issue, the sooner steps can be taken to limit the amount of damage that a breach could cause.

Where data breaches have the potential to cause a high risk or damage to the individuals affected, they need to be contacted to make them aware of the potential risk.

If action can be taken to help the people affected it should be taken immediately. Not following due processes leaves BAEA open to the risk of fines, for both non-reporting of the breach and for the breach itself.

Remember to always follow these steps:

- Report
- act to protect those affected
- investigate and record

• learn from mistakes.

The most significant change under GDPR is that BAEA must report certain breaches to the Information Commissioner's Office (ICO) within 72 hours. This 72 hour window starts when a BAEA officer is made aware of an incident, not when the BAEA data protection officer is made aware.

Breaches must therefore be notified to the BAEA DPO and the BAEA Chair immediately and certainly within 24 hours.

Breach Notification - Breach notifications are now mandatory and this notification is expected to be made within 72 hours of the breach occurring.

The reporting method for any breach will need to be understood by all BAEA officers and breaches reported as soon as possible.

Sanctions - Previously, under the DPA, the maximum fine that could be issued was £500,000. This will increase to 4% of annual revenue or €20m.

New Rights - Under GDPR, people have enhanced and new rights. Notably it will be easier to access the information an organisation holds on them. There is a right to be forgotten.

Responsibilities - BAEA officers have a responsibility to ensure that :

• they follow the law, and the rules laid down by BAEA

• their actions are honest

• security is an integral part of their duties.

Information Asset Register - BAEA needs to know the information that officers hold therefore officers holding sensitive information will be required to complete an Information Asset Register by 30 September of each calendar year.

Penalties : the ICO issued fines of £3.2 million during 2016, making the UK one of the most fined countries in Europe. Under the GDPR, fines will rise from

£500,000 up to €20,000,000 or 4% of global turnover. The likelihood of compensation claims will also increase as people have the right to bring claims for immaterial damage.

• BAEA must develop and maintain retention inventories of all important information assets.

• It is the responsibility of every individual to ensure that the information they manage or process is kept in accordance with this guidance.

Hard copies of sensitive information (e.g. names and addresses)

Paper copies must not be produced or kept. All historic hard copies should be disposed of securely e.g. using a fine cross cut shredder

Passwords

• Keep your passwords to yourself

• Avoid guessable passwords

• Change your password if you think it's been compromised

PCs and laptops. Laptops handling BAEA data should be encrypted and password protected

• Never let anyone else use your logon details

• Steps should be taken to ensure unauthorised persons cannot access/view BAEA sensitive information

• Lock your workstation (using the Ctl-Alt-Del keys) when leaving your desk

• Switch off if you're away from your device

• Laptops should be securely transported and stored. They should not be left in a vehicle overnight and should not be left in view in a car during the day time

• Personal iCloud storage should not be used.

Emails.

Saved emails from former members should be deleted to ensure that their personal data is no longer held. Personal or sensitive information must not be sent by email. If access to such information is required, then members should contact the Chair who can give temporary access to such information.

Removable media devices

• All data stored on removable media devices must be encrypted. Removable media devices such as USB memory sticks must only be used to transfer information from device to device and the data should be erased immediately. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they have taken reasonable care to avoid damage or loss.

• Damaged or faulty removable media devices must not be used.

• Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data loss.

Backing up data.

All BAEA data should be examined by the DPO to ensure that sensitive information is stored correctly and then either deleted or stored on the BAEA cloud.

Retention policy

BAEA will keep information for the following periods:

INFORMATION	TIMESCALE	WHERE
BAEA minutes of meetings	As long as required (ALAR)	At present held by all NEC officers.
Correspondence relating to decisions.	ALAR	At present held at some officers houses.
General correspondence	ALAR	At present held at some officers houses.
Financial information held by Treasurer.	ALAR ***Financial information relating to the organisation can be held indefinitely. Personal information should be deleted when no longer required.	At present held by the Treasurer. To be transferred to BAEA cloud if storage is needed.
Bank statements & yearly accounts & Treasurer's reports (held by Treasurer)	ALAR ***	At present held by the Treasurer. To be transferred to BAEA cloud if storage is required.
Past BAEA magazines with images.	Indefinitely if hard copies are used as historical records	At present held at some officers houses.
Conference information + names of delegates	Delete. Unless used for historical records : then indefinitely.	Information at present (Nov 2021) held on some officers computers.
Membership databases & lists.	ALAR	All information held by Membership Sec. Lists not in current use to be transferred to BAEA cloud.
Email addresses used by Chairs of regional group and NEC	ALAR. These should have been authorised as safe to be used on application for BAEA membership. Past members email	Past members email addresses should be deleted.

	addresses should be deleted . If wishing to make contact by email/phone after members have left they can be informed of the retention at this point .	
Hard copies of members membership application forms.	As above.	At present held by Membership Sec. Past members email addresses should be deleted.
Videos, past members photos especially on Powerpoint presentations .	Delete if no longer required but can be kept indefinitely.	At present kept on officers computers.

No BAEA information is allowed to be sold or given to anyone else. Photos and video recordings at BAEA events should be deleted unless consent has been given. All participants at BAEA events should be informed prior to any photos or media recordings being taken. They should be informed where these photos or recordings may be used.

It is expected that all BAEA officers read and comply with all procedures contained within this document.

I have read, understand and agree to follow the guidance contained within this document. I understand that if I am unsure about any of this guidance that it is my personal responsibility to seek clarification from the BAEA DPO email: simon_blake@tiscali.co.uk

PRINT NAME _____

SIGNATURE _____

Role within BAEA _____

DATE _____ ➢

Please keep hold of this document for your information and reference.

➢ If you wish to discuss any points raised in this document please contact the BAEA DPO

➢ If you require this information in another format please contact the DPO

Review of this policy to take place in Jan 2023.