STAT GDPR & Privacy Policy

Policy last updated:	January 2024
Policy last reviewed:	2023
Register of Systems last Reviewed:	2023
GDPR Officer contact email:	stat@alexandertechnique.co.uk

Definitions

Organisation	Means The Society of Teachers of the Alexander Technique
DPA	means the Data Protection Act 2018 ("DPA") which implements the EU's General Data Protection Regulation.
Responsible Person	means Data Protection Officer
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Organisation.

Contents

1.0 Data Protection Policy

1.1 Data protection principles

The Organisation is committed to processing data in accordance with its responsibilities under the DPA.

DPA requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;

- 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;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- 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;

- 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 DPA in order to safeguard the rights and freedoms of individuals; and

- 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."

2. General provisions

- This policy applies to all personal data processed by the Organisation.
- The Responsible Person shall take responsibility for the Organisation's ongoing compliance with this policy.
- This policy shall be reviewed at least annually.
- The Organisation is registered with the Information Commissioner's Office ("ICO") as an organisation that processes personal data.

3. Lawful, fair and transparent processing

- To ensure its processing of data is lawful, fair and transparent, the Organisation maintains a Register of Systems.
- The Register of Systems shall be reviewed at least annually.
- Individuals have the right to access their personal data and any such requests made to the Organisation shall be dealt with in a timely manner.

4. Lawful purposes

- All data processed by the Organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests).
- The Organisation shall note the appropriate lawful basis in the Register of Systems.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organisation's systems.

5. Data minimisation

- The Organisation shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Members of staff are only given access to data which is needed to fulfil their role. Likewise, data is only shared with relevant external organisations.

6. Accuracy

- The Organisation shall take reasonable steps to ensure personal data is accurate.
- Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

- To ensure that personal data is kept for no longer than necessary, the Organisation shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

- The Organisation shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- When personal data is deleted this should be done safely so that the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data,

the The Data Protection Officer shall assess the risk and report the breach to Office Manager and Council. If appropriate, the breach will be reported to the ICO.

10. Your data protection rights

Under data protection law, you have rights including:

Your right of access: You have the right to ask us for copies of your personal information.
Your right to rectification: You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
Your right to erasure: You have the right to ask us to erase your personal information in certain circumstances.
Your right to restriction of processing: You have the right to ask us to restrict the processing of your personal information in certain circumstances.
Your right to object to processing: You have the right to object to the processing of your personal information in certain circumstances.
Your right to data portability: You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.
You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

11. How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us at:

PO Box 78503
LONDON
N14 9GB
Email: stat@alexandertechnique.co.uk
Telephone: 020 8885 6524

You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO's address:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113
ICO website: https://www.ico.org.uk

2.0 Privacy Policy

This Privacy Policy applies to information The Society of Teachers of the AlexanderTechnique ("STAT") collect about individuals who interact with us. It explains what personal information we collect and how we use it.

If you have any comments or questions about this notice, feel free to contact us at STAT@alexandertechnique.co.uk

2.1 Personal data that we process

The following table explains the types of data we collect and the legal basis, under current data protection legislation, on which this data is processed.

Purpose	Data (key elements)	Basis
Enquiring about our organisation and its work	Name, email, message	Legitimate interests - it is necessary for us to read and store your message so that we can respond in the way that you would expect.
Subscribing to email updates about our work	Name, email	Consent - you have given your active consent.
Making a donation	Name, email, address, payment information	Legitimate interests - this information is necessary for us to fulfill your intention of donating money and your expectation of receiving a confirmation message.
Signing up as a member	Name, email, address, member number, banking details, year of birth	Contract - by paying your membership fees you have entered into a contractual relationship with us as set out in our membership terms and conditions.
Website functionality	Website activity collected through cookies	Legitimate interests - it is necessary for us to store a small amount of information, usually through cookies, to deliver functionality that you would expect, such as remembering the contents of your order before you have fully completed the process.

2.2 How we use your data

We will only use your data in a manner that is appropriate considering the basis on which that data was collected.

How long will STAT keep Personal data?

- Records of payments made by you will be retained for as long as required for STAT to meet its legal obligations to maintain financial records.
- All information (updated as appropriate) will be kept for the length of your membership agreement and for a maximum of 6 years after your membership has ceased.
- The following information will be retained for historical and archive purposes: a) your name, b) your training dates, c) which training school you trained at and d) the name of your head of training.
- In the event of a complaint against you, STAT will retain the relevant information for up to 25 years.

.

We may also use your personal information to:

- reply to enquiries you send to us;
- handle donations or other transactions that you initiate;
- where you have specifically agreed to this, send you marketing communications by email relating to our work which we think may be of interest to you.

2.3 When we share your data

We will only pass your data to third parties in the following circumstances:

- you have provided your explicit consent for us to pass data to a named third party;
- we are using a third party purely for the purposes of processing data on our behalf and we have in place a data processing agreement with that third party that fulfils our legal obligations in relation to the use of third party data processors; or
- we are required by law to share your data.

In addition, we will only pass data to third parties outside of the EU where appropriate safeguards are in place as defined by Article 46 of the General Data Protection Regulation.

4. Rights you have over your data

You have a range of rights over your data, which include the following:

- Where data processing is based on consent, you may revoke this consent at any time and we will make it as easy as possible for you to do this (for example by putting 'unsubscribe' links at the bottom of all our marketing emails).
- You have the right to ask for rectification and/or deletion of your information.
- You have the right of access to your information.
- You have the right to lodge a complaint with the Information Commissioner (details can be found above Section 10 - GDPR Policy) if you feel your rights have been infringed.

A full summary of your legal rights over your data can be found on the Information Commissioner's website here: https://ico.org.uk/

If you would like to access the rights listed above, or any other legal rights you have over your data under current legislation, please contact us on: stat@alexandertechnique.co.uk

Please note that relying on some of these rights, such as the right to delete your data, will make it impossible for us to continue to deliver some services to you. However, where possible we will always try to allow the maximum access to your rights while continuing to deliver as many services to you as possible.

5. Cookies & usage tracking

A cookie is a small file of letters and numbers that is downloaded onto your computer when you visit a website. Cookies are used by many websites and can do a number of things, e.g. remembering your preferences, recording what you have put in your shopping basket, and counting the number of people looking at a website.

Where cookies are used to collect personal data, we list these purposes in section 1 above, along with other personal data that we collect. However, we also use some cookies that do not collect personal information but that do help us collect anonymous information about how people use our website. We use Google Analytics for this purpose. Google Analytics generates statistical and other information about website usage by means of cookies, which are stored on users' computers. The information collected by Google Analytics about usage of our website is not personally identifiable. The data is collected anonymously, stored by Google and used by us to create reports about website usage. Google's privacy policy is available at http://www.google.com/privacypolicy.html.

6. Modifications

We may modify this Privacy Policy from time to time and will publish the most current version on our website. If a modification meaningfully reduces your rights, we'll notify people whose personal data we hold and is affected

3.0 Destruction / Deletion of Records Policy

When it comes to keeping pupil records, some teaching members follow the NHS example and hold records for 8 years but where minors are concerned you will need to keep them for longer. Our insurers recommend 25 years. Please refer to the guidance previously circulated and in the members' section of the STAT website.

The GDPR principle highlights that you can keep anonymised data for as long as you want. In other words, you can either delete or anonymise the personal data once you no longer need it. We would recommend that you should regularly review the information you hold on your pupils and erase or anonymise personal data at the appropriate time.

When removing, returning, deleting or destroying any personal data, every reasonable and affordable step should be taken to ensure it is done in a manner which is secure and ensures privacy; thereby keeping the risk of theft, loss or interception to an absolute minimum.

In general, if personal data can be anonymised, then where possible, identifying data must not be collected in the first place.

On a computer, when data is removed or deleted securely, care must be taken to ensure that:

- Duplications are identified.
- Historical versions are identified (e.g. in computer history).
- Versions held in backup files or servers are identified.
- All identified versions that are no longer required are deleted securely and irrevocably. Professional advice may be needed for example from an IT specialist.

On occasion it may be necessary to retain evidence of the removal, deletion or destruction of personal data, particularly when the pupil has requested information regarding the erasure or has asserted the right to be forgotten.

If you receive a request to have personal data erased or forgotten in accordance with a pupil's statutory right, then you may need to inform any other recipients of that data so that the recipient may make steps to remove, return, delete or destroy the data as appropriate.

You must be prepared to respond to subject access requests (where pupils have the right to access their personal data) for personal data stored offline, and you must still comply with all the other principles and rights. The word 'deletion' can mean different things in relation to electronic data, and we recognise it is not always possible to delete or erase all traces of the data held on a pupil. The key issue is to ensure you put the data beyond use. If it is appropriate to delete personal data from

a live system, you should also delete it from any back-up of the information on that system.

It may be likely that data also exists in a number of other places, including private devices that are not connected to a server (such as laptops, tablets and phones). Please consult the device settings for guidance for erasing of electronic data if and when necessary.

Data may also be printed and kept as paper copies, with no real process for the safe destruction of such data when it is no longer required.

The GDPR does not set a specific size that documents need to be shredded to in order to comply with the regulation. It is true that the GDPR covers far more than the deletion of physical documentation, as the rules apply to the storage of any kind of personal data. However, physical documents are often overlooked when attempting to achieve to GDPR compliance, so it is important that you take the time to understand the processes that you use and to update them accordingly.

If you have any of the following documents in paper format you will need to comply with GDPR:

- Client data
- Medical information
- Personal information

If such documents need to be destroyed, the best device to use for destruction of paper format documents is a cross-cutting shredder. Other shredders may not completely obscure lines of text. Cross-cutting shredders are readily available from all main stationery retailers and online retail companies.

Should this not be an option, complete destruction by burning is another option.

If you are in any doubt about any of this, or would like further information, please contact the STAT office.

Procedure following the death of a member

In the sad event of the death of a STAT teaching member, alongside the natural grieving process and funeral arrangements there is also consideration necessary for the proper winding up of a practice. Some thought may have been put to this if a terminal diagnosis had been given, but the following must apply equally should a death have been unexpected.

Upon a death the majority of personal information should no longer be required and can be shredded. Computer files should be deleted if the password is known to others. Under no circumstances should any personal information be given to another STAT teaching member no matter how well intentioned this is.

If there is a paper diary, those surviving the member should advise the pupils in the most suitable manner and ask them if they wish you any personal notes to be shared before the diary is shredded.

If all contacts were on a computer, which those surviving the member are locked out of, the computer should be decommissioned to prevent pupil confidentiality. Should the password be known, careful deletion of all personal pupil records should be deleted after consideration to the above for paper records is given. It will be worthwhile consulting a local IT specialist with regard to permanent deletion of data to make sure that no-one using the computer will be able to come across the data.

Naturally if the practice was run by a couple or in partnership these steps do not apply so strictly as pupils of the deceased member may consider lessons with the member surviving them.