GREENE'S COLLEGE OXFORD

Data Protection Policy Statement and Procedures

This policy was adopted in August 2026.

This policy is due to be reviewed in August 2027.

The person responsible for the implementation of this policy is the College Principal.

It is the responsibility of the College's Governing Body to ensure that this policy is reviewed and updated annually.

Greene's is committed to full compliance with the Principles and requirements of the Data Protection Act 2018, the UK's implementation of the General Data Protection Regulation (GDPR). Greene's will therefore follow procedures which aim to ensure that all staff (including part-time and full-time staff and self-employed suppliers such as tutors

and invigilators) and students who have access to any personal data held by or on behalf of Greene's are fully aware of and abide by their duties under the Data Protection Act 2018 and that they are also aware of their rights under the Act regarding their own personal data.

Statement of Policy

Greene's needs to collect and use information about past, current and prospective students and their parents and tutors and others with whom it works in order to operate and carry out its functions. In addition, Greene's may be required to collect and use personal information in order to comply with its statutory legal, professional and other obligations – such, for example, as relates to the retention examination data. This personal information will be handled and dealt with properly however it is collected, recorded and used and whether it is on paper, in computer records or recorded by other means.

Greene's regards the lawful and appropriate treatment of personal information as very important to its successful operation and essential to maintaining confidence between Greene's, its staff and those with whom it carries out business.

Handling personal and sensitive data

Greene's will, through management and use of appropriate controls, monitoring and review:

- Use personal data with sensitivity and in the most efficient and effective way to deliver its services
- Collect and process only the personal information which is needed
- Use personal information for such purposes as are described at the point of collection, or for purposes which are legally permitted and limited to what is necessary
- Strive to ensure personal information is accurate and up to date
- Not keep information for longer than is necessary
- Securely destroy data which is no longer needed
- Take appropriate security measures to safeguard information - including the unauthorised or unlawful processing and accidental loss or damage of data
- Ensure that there is general information of rights to access of personal information
- Ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 2018. These rights include: the right to access their own personal information within 30 days of request[1]; the right to prevent processing in certain circumstances; and the right to correct, rectify, block or erase personal information regarded as wrong information or personal information that is being used in ways that have not contractually been agreed to.
- Ensure that any breaches of this policy are dealt with appropriately

[1] For particularly complex requests Greene's make take a further 60 days to provide a response. Under such circumstances Greene's will inform the person concerned within 30 days.

Principles of Data Protection

In its handling of personal data Greene's applies eight (8) principles of good practice. These are that personal data:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
4. Shall be accurate and where necessary, kept up to date
5. Shall not be kept for longer than is necessary for that purpose or those purposes
6. Shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018
7. Shall be kept secure, i.e. protected by an appropriate degree of security
8. Shall not, without adequate consideration, be transferred to a country or territory outside the UK or the European Economic Area (EEA), unless that country or territory ensures an adequate level of data protection

The Data Protection Act 2018 provides conditions for the processing of any personal information. It also makes a distinction between personal data and "sensitive" personal information.

Personal information is defined as data relating to a living individual who can be identified from:

- That information and other data which is in the possession of, or is likely to come into the possession of Greene's and includes an expression of opinion about the individual – such as a reference

Sensitive personal information is defined as personal information consisting of data as to:

- Racial or ethnic origin
- Political opinion
- Religious beliefs
- Trade union membership
- Genetics and biometrics
- Physical or mental health or condition
- Sexual life or orientation
- Criminal convictions and offences

How to contact Greene's

For any questions about this policy or data requests the Data Protection Officer (DPO) at Greene's College can best be contacted by email:

alex.gray@greenes.org.uk Please mark all correspondence for the attention of the Data Protection Officer.

Implications and procedures for staff

All documents, reports and personal information whether recorded on paper or electronically, and which relate to past, current and prospective students and their parents and tutors and others with whom Greene's works in order to operate and carry out its functions are therefore covered by the Data Protection Act 2018.

This has a number of implications for staff.

Greene's may need to process and retain staff personal information and/or staff sensitive personal information for:

1. Administering and maintaining personnel records;
2. Paying and revising salary and other remuneration and benefits;
3. Providing and administering benefits – such as pension contributions;
4. Undertaking performance appraisals and reviews and setting performance targets;
5. Maintaining training records – especially those related to compliance such as: safeguarding, anti-radicalisation, first aid, fire prevention, health & safety, etc.
6. Maintaining sickness and other absence records;
7. Taking decisions as to fitness to work;
8. Ensuring accurate contact information is held in case of emergencies;
9. Providing references and information to future employers and if necessary, to governmental and quasi-governmental bodies for social security, tax and other purposes;
10. Providing information to future purchasers of the business;
11. Transferring information to a country or territory outside the UK or EEA.

This list is not meant to be exhaustive. Personal data must be accurate and kept up to date. Therefore staff should inform the DPO or their manager should their personal details or circumstances change. Records will then be updated accordingly.

Data Security

Both staff (you) and we (Greene's) must work together to ensure that appropriate security measures are taken against unlawful or unauthorized processing of personal information, and against the accidental loss of, or damage to, personal information.

Individuals may apply to the courts for compensation if they have suffered damage from a loss of personal information.

It is recognised that an increasing amount of work is done using the internet. Therefore, and in the context of this Policy staff should be aware of the additional guidance provided by Greene's e-Safety Policy.

Certain staff should also be aware of the Greene's Information Security policy that concerns the collection and treatment of data related to card payments.

Maintaining personal data security means guaranteeing the confidentiality, integrity and availability of personal data as follows:

- Confidentiality means that only staff who are authorised to use the personal data can access it.
- Integrity means that personal data should be accurate and appropriate for and limited to the purpose for which it is being used.
- Availability means that authorised staff should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual computers or other devices.

General day-to-day work practice should include the following:
Clear desks: Your desk should be cleared of any paperwork in your absence. Paperwork should be either disposed of or put away in desk drawers or in cupboards. Paperwork may often show personal data and is a fire hazard. Tutors or students should not be allowed or given access to any personal data they are not authorised to see.

Secure lockable desks and cupboards: Personal information that is also sensitive should be kept securely – preferably electronically or, if in paper form, in locked desks or cupboards.

Methods of disposal: Paperwork that is sensitive should always be shredded before disposal.

Computer equipment: Please be aware of who might be looking at your computer screen whilst you are working – passers-by should not be able to see personal data. Your computer should not be "browsed" by anyone, for example bored students or tutors sitting at an empty desk and whiling away the time. Nor should anyone stand behind you to watch while you work on your computer. A computer gives access to the details of every individual connected with Greene's Tutorial College: students, tutors, parents and employed staff.

You should ensure that your security setting turns your screen off after five minutes of inactivity and which can only be reactivated with a password.

Protecting data: You should not send external "group" emails without using the BCC facility – this includes emails to groups of staff, students or tutors. It is considered good practice to use the BCC facility for all group emails to avoid mistakes.

Emails: It can be easy to make mistakes when forwarding emails. Please be careful to whom you forward emails – not least because the email will often contain a record of previous correspondence. If you are the recipient of an email from another member of staff it is good practice not to forward the email in question to someone else who is not a member of staff.

Giving out personal information: Without their written permission, you should not give out any personal data; including: addresses, telephone numbers, email addresses, etc. to anyone not directly concerned with the individual – including those purporting to be "friends" of the individual. Those having a professional need to know can be given the relevant information. For example, a tutor may be given the name and contact details of a student they have agreed to teach and for whom Greene's has agreed tuition may take place. Similarly a client may be given the name and contact details of a tutor should Greene's agree that teaching may take place. Under no other circumstances should names or contact details be exchanged between client, tutor or other enquirers. Under such circumstances, please take the enquirer's name and contact details and say that you will pass on a message.

The same principle applies to giving out any information or data, concerning Greene's. Unsolicited "market researchers" may try to engage you on the telephone and ask numerous questions about numbers of students, tutors, etc. Please make it clear you have no authority to give out such information but, if necessary, you will see if the DPO is available to talk or ring them back.

Empathy: Please remember, that whatever your own views about how relaxed or otherwise you are about what details people know about you, other people's personal data should be viewed as their property – and so it is not yours to make available to a third party.

Access to data: The other side of the fence is that individuals on whom we hold information have the right to know what that particular information is.

Students, tutors, parents, clients, suppliers all have the right to access the information we hold on them. This means that data should be recorded accurately and without bias. It should be up to date.

Whether entering information on databases, writing letters, memos or emails (internal or otherwise), we should remember at all times that the

individuals to whom we are referring have every right to see our comments.

Concerns and questions Any concerns and questions that staff may have in relation to this policy and procedures should be addressed to the DPO.