



LORD
WANDSWORTH
COLLEGE

DATA PROTECTION POLICY

Staff member responsible	Revision Date	Approved By	Approval Date	Reason
RDG	N/A	SLT	Apr 2018	GDPR Introduction
RDG	October 2019	SLT	Dec 2019	Review
DJJ/BWB	March 2023	RSC	3 May 2023	Updated
CJA/RWS	April 2024	RSC	2 May 2024	Updated

Data Protection Policy

1. Background

Data protection is an important legal compliance issue for Lord Wandsworth College. During the course of the College's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors, alumni and donors, and other third parties. The College, as "data controller", is liable for the actions of its staff and governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes specific provisions of relevance to independent Schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including s that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and will typically look into individuals' complaints routinely and without cost and has various powers to take action for breaches of the law.

2. Definitions

Key data protection terms used in this data protection policy are:

- **Data controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the College (including its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Personal information (or 'personal data')**: any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the College's, or any person's, intentions towards that individual.
- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

Data Protection Policy

- **Special categories of personal data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

3. Application of this policy

This policy sets out the College's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or governors of the College are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the College or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the College's personal data as contractors, whether they are acting as "data processors" on the College's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the College shares personal data with third party data controllers – which may range from other Colleges, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy. Volunteer and contractors are data controllers in their own right, but the same legal regime and best practice standards set out in this policy will apply by law.

4. Person responsible for Data Protection at the College

The Director of IT Services is responsible for ensuring that all personal data is processed in compliance with this Policy and the principles of applicable data protection legislation. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Compliance Team at datacompliance@lordwandsworth.org.

5. The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

- Processed **lawfully, fairly** and in a **transparent** manner.
- Collected for **specific and explicit purposes** and only for the purposes it was collected for.
- **Relevant** and **limited** to what is necessary for the purposes it is processed.
- **Accurate** and kept **up to date**.
- **Kept for no longer than is necessary** for the purposes for which it is processed; and
- Processed in a manner that ensures **appropriate security** of the personal data.

Data Protection Policy

The GDPR's broader 'accountability' principle also requires that the College not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies.
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

6. Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the College to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the College. It can be challenged by data subjects and also means the College is taking on extra responsibility for considering and protecting people's rights and interests. The College's legitimate interests are set out in its Privacy Notice, as GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity.
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors.
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

7. Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the College is accurate, fair and adequate. Staff are required to inform the College if they believe that *any* personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents, and alumni and donors – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on College business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the College's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to **record every**

Data Protection Policy

document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.

8. Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with all relevant College policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the College's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Admissions Policy.
- CCTV Policy.
- Use of IT and Devices (Acceptable Use).
- Bring Your Own Device (BYOD).
- Safeguarding and Child Protection Policy.
- Security and Access Control Policy.
- Taking, Storing and Use of Images Policy.

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

9. Data Processors

The College contracts with various organisations who provide services to us including:

- Educational providers and resources, such as College trip providers and educational apps.
- Human resources providers, such as those who pension providers of those who carry out searches in relation to prospective staff.
- IT providers, such as those who provide systems that support education such as our management information system.

In order that these services can be provided effectively, the College is required to transfer personal data of data subjects to these data processors.

Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to our satisfaction.

The College will always undertake appropriate due diligence of any data processor before transferring the personal data of data subjects to them. Contracts with data processors will comply with relevant legislation and contain explicit obligations on and expectations of the data processor. This due process includes carrying out a data processing impact assessment and completing a data sharing agreement with any 3rd party processor.

The College will not transfer or share personal information with countries outside of the European Economic Area (EEA) unless that country has a recognised adequate level of protection in place.

10. Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

Data Protection Policy

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the College must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach they must notify the Data Compliance Team. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the College always needs to know about them to make a decision.

As stated above, the College may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the College, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

11. Care and data security

More generally, we require all College staff (and expect all our contractors) to remain mindful of the data protection principles (see section 3 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the College to the Data Compliance Team, and to identify the need for (and implement) regular staff training. Staff must attend any training we require them to.

12. Rights of Individuals

In addition to the College's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the College). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Data Compliance Team as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate.
- request that we erase their personal data (in certain circumstances).
- request that we restrict our data processing activities (in certain circumstances).
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention).
- object to direct marketing; and

Data Protection Policy

- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Data Compliance Team as soon as possible.

13. Data Security: online and digital

The College must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

- No member of staff is permitted to remove personal data from College premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or COO.
- No member of staff should provide personal data of pupils or parents or alumni or donors to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- Where a worker is permitted to take data offsite on memory sticks or personal devices it will need to be encrypted.
- Use of personal email accounts or [unencrypted] personal devices by governors or staff for official College business is not permitted.

14. Processing of Financial / Credit Card Data

The College complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Data Compliance Team or College Director of Finance. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

SUMMARY / POLICY STATEMENT

“It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- *Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?*
- *Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?*
- *What would be the consequences of my losing or misdirecting this personal data?*

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the College's culture, and all its staff and representatives need to be mindful of it.”

Data Protection Policy

ANNEX A Guidance to Staff when Handling Personal Data

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of data protection our culture and all staff and representatives need to support it and ensure that:

1. All mandatory data protection training as well as any refresher training is completed.
2. All personal data is kept securely and processed in line with policy.
3. They only process personal data where it is necessary in order to do their jobs.
4. Personal data is not disclosed to any unauthorised third party.
5. Personal data is kept in accordance with the retention schedule. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised in accordance with the Foundation retention schedule.
6. Physical records containing personal data is kept in secure cabinets, locked cupboards or rooms with restricted access.
7. Use a shredder or the confidential waste disposal bins to dispose of any document containing personal data, whether or not you consider it to be confidential.
8. The personal data we hold is accurate and up to date and take steps to correct any inaccuracies.
9. They are aware that records e.g. minutes, reports, references, emails may be viewed by those identified in them.
10. They seek express consent for any sensitive information to be processed, unless the College/Foundation has a specific legal requirement to process such data.
11. Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Compliance Team.
12. Data protection breaches are reported and brought to the attention of Data Compliance Team and that they support the investigation and resolution of a breach.
13. Protect their network account with an appropriate password.
14. Only use College owned equipment to process and store personal data.
15. Ensure any portable device containing personal data is password protected and/or encrypted.

Data Protection Policy

16. Changes to their own personal data, such as a change of address are notified to the People Team.

Staff must not:

17. Disclose passwords to anyone else, including other members of staff.
18. Leave computers, laptops or tablets unattended without locking the screen or switching off. Make sure paperwork is not left on desks, printers and documents are always filed away or shredded after use.
19. Record information about data subjects which is irrelevant or excessive.
20. Take photographs of pupils on personally owned devices.
21. Attempt to access personal data which is beyond what is necessary for the performance of their duties.
22. Do not write any comment about any individual that is unfair or untrue and that you would not be able to defend if challenged. Remember anything that you write about a person will be seen by them should they make a data subject access request (DSAR).
23. Remove or copy any personal data from the College by any insecure means including but not limited to USB sticks, email, or paper records.
24. Retain personal data longer than required for the effective functioning of the College.
25. Disclose any personal information without the consent of the person concerned.
26. Transfer personal data to countries outside the European Economic Area (EEA) unless additional conditions are met.

ANNEX B Data Sharing Agreement Template

Guidelines on the use of this template

A data sharing agreement should be completed when the College shares personal data with third party data controllers. This may range from other Schools, to parents, to appropriate authorities, to casual workers and volunteers. Each party will need a lawful basis to process that personal data and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy. If you are a volunteer or contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

NB: When personal data is shared, the individuals should normally be notified in the form of a privacy notice which gives the chance to object.

DATA SHARING AGREEMENT

1. Data Sharing Parties

This agreement sets out the arrangements for processing data between Lord Wandsworth College and

..... (name of third party)

2. Basis of processing Legitimate Interest

Legitimate interest is the most flexible lawful basis for processing personal data and is likely to be the most appropriate where data subjects would reasonably expect a minimal impact on their privacy. The College should consider its own legitimate interests for example to promote its aims and ideals, and to balance this against the individual's privacy rights.

3. Data Controller

For the purpose of this agreement, both parties are considered joint data controllers as defined under the UK General Data Protection Regulations.

4. Context of Data Sharing

A couple of sentences to describe the purpose of the agreement, for example:

“Lord Wandsworth College has agreed to undertake combined activities with another College. Senior pupils from both Colleges will join together and be led by staff from both organisations. To enable efficient co-ordination, the Colleges will share lists of pupil names with staff from the other College. All staff involved will be DBS checked and meet the safeguarding policies of both Colleges which includes annual KCSIE training.”

5. Personal Data Shared

Data Protection Policy

The personal data: e.g. names of pupils from each College, their year group, and tutors.

..... (list the types of data)

6. Details of how the data will be shared

Data will be shared using the LWC SharePoint Portal. This provides a secure password protected platform with permissions configured to only permit staff who are explicitly authorised to access this site. Any hard copies of data will be shredded. Digital records will be deleted and purged within 12 months after the activity completion.

7. Names (or roles) of those accessing the data

List names or roles as appropriate, e.g. the staff and registered volunteers from both Colleges.

8. Data Sharing Date(s)

It is intended the data will be shared from

Start Date:

End Date:

9. Data security breaches

Both parties must notify each other of any potential or actual losses of shared personal data as soon as possible and in any event within 24 hours. The parties will provide reasonable assistance as is necessary to each other to facilitate the handling of any data security breach in an expeditious and compliant manner.

The data sharing agreement must be signed by an authorised representative of both parties before any data sharing takes place.

On behalf of Lord Wandsworth College

Signature.....

Position:

Date:

On behalf of the 3rd Party

Signature.....

Position:

Date: