DATA PROTECTION POLICY AND PROCEDURE

Foreword

This Policy is not to be confused with Denstone College's Privacy Notice, which is a General Data Protection Regulation (GDPR) requirement, and which is available for all data subjects. It is not aimed at external audiences and is separate from any Staff Privacy Notice introduced.

It is primarily for staff. It determines how, as a matter of good practice and policy, any personal data controlled and processed by Denstone College – covering parents, guardians, pupils, and colleagues (past, present, or prospective) – should be handled by staff.

GDPR does not require us to have this this document in place. However, it does confer general obligations of documentation, data security and staff competence, hence this Policy which will be refined and updated in line with changes to national and sector guidance and Denstone College process or managerial changes.

This Policy will inevitably have some overlap or interaction with other policies concerning how staff handle data, not least in IT policies and staff handbooks, and this Policy is not intended to over-ride what are adequate and appropriate practices.

Summary

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 Denstone College's culture, and all its staff and representatives need to be mindful of it.

Background

Data protection is an important legal compliance issue for Denstone College. During the course of Denstone College's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, alumni, suppliers and other third parties (in a manner more fully detailed in Denstone College's Privacy Notice). 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 is sensitive or routine.

The law (the Data Protection Act 1998) changed on 25 May 2018 with the implementation of the General Data Protection Regulation (GDPR). This is an EU Regulation that is directly effective in Europe and following Brexit there are now two versions of the original EU GDPR including a separate version applicable in the UK. A new Data Protection Act 2018 was passed to deal with certain issues left for national law: which included specific provisions of relevance to independent schools. In the context of our safeguarding obligations, Denstone College has a heightened duty to ensure that the personal data of pupils is at all times handled responsibly and securely.

While this new law set out useful legal grounds in this area, in most ways it strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools and colleges that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and has powers to take action for breaches of the law.

Those who are involved in the processing of personal data are obliged to comply with this Policy when doing so. Accidental breaches will happen and may not be a disciplinary issue, but any serious breach of this Policy may result in disciplinary action.

This Policy sets out Denstone College's expectations and procedures with respect to processing any personal data collected from data subjects (e.g., including parents, pupils, staff, visitors, contractors).

Key data protection terms used in this Data Protection Policy are:

- **Data Controller** – an organisation that determines the purpose and means of the processing of personal data. For example, Denstone College is the controller of people's personal information. As a Data Controller, we are responsible for safeguarding the use of personal data.
- **Data Processor** – an organisation that processes personal data on behalf of a Data Controller, for example a payroll provider or other supplier of services.
- **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), including name, identification number, location, or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone'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.
- **Special categories of personal data** (or **sensitive 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.

Data Protection Co-ordinator
Denstone College has appointed a GDPR & Compliance Manager who will provide advice, guidance, and support to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR. 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 GDPR & Compliance Manager- sturner@denstonecollege.net.

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:

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

The GDPR's 'accountability' principle also requires that Denstone 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; 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, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

Lawful grounds for data processing
Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and the fact that it can be withdrawn by the Data Subject) it is generally considered preferable 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 Controller. It can be challenged by Data Subjects and also means the Controller is taking on extra responsibility for considering and protecting people's rights and interests. Denstone College's legitimate interests are set out in its Privacy Policy, as GDPR requires.

Other lawful grounds include:

- Compliance with a legal obligation, including in connection with employment and diversity;
- Contractual necessity, e.g., to perform a contract with staff or parents;
- 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.

Headline responsibilities of all staff

Record-keeping

It is important that personal data held by Denstone College is accurate, fair, and adequate. You are required to inform Denstone College if you believe that *your* personal data is inaccurate or untrue or if you are dissatisfied with the information in any way. Similarly, it is vital that the way you record the personal data of others – in particular, colleagues, pupils, and their parents – is accurate, professional, and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on College business may have the right to see that information. This absolutely must not discourage staff from recording necessary, factual, and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with Denstone College's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

One of the key data protection principles is storage limitation, therefore personal data should be adequate, relevant, and limited to what is necessary for the purposes for which it is processed. Thus, ensuring that the period for which the personal data are stored is kept to a strict minimum. Denstone College has a Retention Policy which lists guidance for each department on the retention of documentation. It is the owner of the documentation that is responsible for ensuring that the retention policy is followed. You should use the Retention Policy alongside this one to help manage the data within your department. If you wish to add to the retention policy of have any questions, please contact the GDPR & Compliance Manager.

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 the Denstone College Handbook, employment manual and all relevant College policies and procedures. In particular, there are data protection implications across several areas of Denstone College's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with these policies.

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.

When sending personal data externally staff should ensure that secure methods of transfer are used including password protection and encryption. Staff should only transfer data that is essential and should always ask themselves- Do I need to send this?

When sharing sensitive personal data internally staff should always encrypt, or password protect this data and ensure that where possible the information is stored securely on our network with directions for the staff as to where to find this.

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.

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, Denstone College must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If you become aware of a personal data breach, you must notify the GDPR & Compliance Manager and IT Manager. If staff are in any doubt as to whether or not they should report something, 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 Denstone College always needs to know about them to decide. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. This could include losing data, destroying data or corrupted data. A breach could also include someone who is not authorised to do so accessing the data or passing it on without authorisation, it could be accidental or deliberate.

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

All breaches should be recorded on the Incident Management system. An investigation will be undertaken by the IT Manager/Compliance team where possible within 24 hours of the breach being discovered/reported. Denstone College has a Data Breach Management Policy to follow in these circumstances.

Care and data security

More generally, we require all College staff to remain conscious of the data protection principles (see 'The principles' above), to attend any training we require them to, 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 affects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

Staff should mark their emails as "Confidential" if they contain sensitive or highly sensitive information, such emails should only be read when in a private area and staff emails are not to be read when pupils are present. Emails containing personal data that are to be sent externally must be password protected.

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 Denstone College to the Compliance team and to identity the need for, and implement, regular staff training. Key data owners (who are usually department managers) are listed on the Data Protection Roles and Responsibilities Policy, who all have a part to play in operationalising the privacy management programme within the school.

Vendor Management Process

For all new systems, involving the relevant stakeholders in the consultation process across College should ensure a smooth implementation. You must consult with the IT team about the suitability of the College's infrastructure to run a new system, ensure your team are briefed and trained on the new process and explain why new systems are being reviewed - this will help them feel involved and identify issues you may not be aware of. If your activity involves processing personal data you should contact the Compliance team who will give you access to the vendor assessment tool and provide guidance on how

to complete this. The Vendor assessment will be reviewed by the Compliance Team/ IT Manager who will approve, deny or provide feedback on what actions are required before you implement your system. In some cases, a DPIA will also be required. The Compliance team will provide guidance on this matter.

Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment (DPIA) is a way to assess and hopefully mitigate any risks to personal data that a new processing activity could introduce. It is an opportunity to understand how the personal data will be used, who will have access to it and how it will be protected. Any new project that involves the processing of personal data may need a DPIA.

We must complete a Data Protection Screening Checklist when considering a new project involving data processing and consider whether to do a DPIA if we plan to carry out any of the below projects involving:

- Evaluation or scoring
- Automated decision-making
- Systematic Monitoring
- Processing of sensitive data or highly personal natured
- Large scale processing
- Data concerning vulnerable subjects
- Innovative technological solutions
- Processing that involves preventing data subjects from exercising their rights

We must carry out a DPIA if we plan to:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- Process special category data or criminal offence data on a large scale;
- Monitor a publicly accessible place on large scale;
- Use of innovative technology;
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service;
- Carry out profiling on a large scale;
- Process biometric or genetic data;
- Combine, compare, or match data from multiple sources;
- Process data in a way that involves tracking individuals online or offline location or behaviour;
- Process children's personal data for profiling or automated decision making or for marketing purposes;
- Process personal data that could result in physical harm in the event of a breach.

If the DPIA finds that the risks to the data are too high and cannot be mitigated, then Denstone College must consult the ICO (Information Commissioner's Office) before going ahead with the project.

If a member of staff would like to implement a new system which includes the processing of personal data, they are required to follow Denstone College's Vendor Management Process and ensure adequate Data Processing Agreements are in place with the vendor to ensure that data protection is taken seriously and to feel confident in the new systems we implement.

Data Transfers

The UK government has stated that transfers of data from the UK to the EEA are permitted, but this will be kept under review. Currently we have an adequacy decision until June 2025. Adequacy' is a term that the EU uses to describe other countries, territories, sectors or international organisations that it deems to provide an 'essentially equivalent' level of data protection to that which exists within the EU.

An adequacy decision is a formal decision made by the EU which recognises that another country, territory, sector or international organisation provides an equivalent level of protection for personal data as the EU does. Because the EU considers the UK GDPR to be adequate, data can continue to flow as before in the majority of cases, and you don't need to consider another appropriate safeguard. (See Appendix 1) If a country does not have an adequacy agreement then an additional safeguard must be put in place. For further guidance see the below link and speak to the Compliance team:

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/

Rights of Individuals

In addition to Denstone 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., Denstone College). This is known as the Subject Access Request (SAR). Denstone College must comply with a SAR without undue delay and at the latest within one month of receiving the request. The time to respond can be extended by a further two months if the request is complex or the College have received several requests from the individual, e.g., other types of requests relating to individuals' rights. Such a request does not need any formality, an individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact. If you become aware of a SAR (or indeed any communication from an individual about their personal data), you must tell the Compliance team as soon as you become aware. Please refer to the College Subject Access Request Process document for more information.

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;
- 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; and
- Object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data.

Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply. 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 Compliance team as soon as you become aware.

Data Security: online, digital and paper

Denstone 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. As such, staff are discouraged from removing personal data from College premises, whether in paper or electronic form. Where data is stored on a portable device, it must be stored safely, and it must be encrypted, and password protected.

If personal data is taken off site in paper format it should be transported in a lockable container and it should never be left in an unattended vehicle. If staff have taken documents containing personal data off site, i.e., to work on at home or for educational visits it should be locked away in a secure container that only the College member of staff has access to when it is not being worked on.

Processing of Debit / Credit Card Data

Denstone College complies with the requirements of the Payment Card Industry Data Security Standard (PCI DSS). Staff who are required to process card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements.

For any questions regarding this policy please contact compliance@denstonecollege.net.

Appendix 1

What countries or territories are covered by adequacy regulations?

The UK has adequacy regulations about the following countries and territories:

- The European Economic Area (EEA) countries;

These are the EU member states and the EFTA States.

The EU member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

The EFTA states are Iceland, Norway and Liechtenstein.

- EU or EEA institutions, bodies, offices or agencies;
- Gibraltar;
- The Republic of Korea; and
- Countries, territories and sectors covered by the European Commission's adequacy decisions (in force at 31 December 2020).

These include a full finding of adequacy about the following countries and territories:

Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

In addition, the partial findings of adequacy about:

- Canada – only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. Please read the guidance on the scope of PIPEDA from the Office of the Privacy Commissioner of Canada for further information
- Japan – only covers personal data transferred to private sector organisations subject to Japan's Act on the Protection of Personal Information. This does not include transfers of the types listed in the EU's adequacy decision for Japan.
- The United States of America – only covers data which is transferred under the UK Extension to the EU-US Data Privacy Framework. You can find more information about the UK Extension, including a factsheet for UK organisations, on gov.uk and on the US Department of Commerce's Data Privacy Framework Program website.