THE SIXTH FORM COLLEGE FARNBOROUGH

Data Protection Policy

TABLE OF CONTENTS

1. OVERVIEW

The College recognises the importance of data protection and is committed to protecting and safeguarding personal data.

The College collects, stores and processes personal data on a variety of stakeholders in order to carry out its activities and functions.

The College recognises that having controls around the collection, use, retention and destruction of personal data is important in order to comply with our obligations under Data Protection laws and in particular its obligations under Article 5 of the UK GDPR.

The College's Data Protection Officer is responsible for informing and advising the College and its staff on its data protection obligations and for monitoring compliance with those obligations and with the College's policies. If you have any questions about the content of this policy, or if you need further information, you should contact the Data Protection Officer via email at dpo@farnborough.ac.uk

2. ABOUT THIS POLICY

This Policy (and the other policies and documents referred to in it) sets out the basis on which the College will collect and use personal data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out rules on how the College handles uses, transfers and stores personal data.

It applies to all personal data stored electronically, in paper form, or otherwise.

3. DEFINITIONS

3.1. **Personal Data** – any information relating to an identified or identifiable living person (referred to as a data subject).

3.2. **Controller** – any entity (e.g. company, organisation or person) that determines the purposes for which, and the manner in which, any personal data is processed.

3.3. **Processor** – any entity (e.g. company, organisation or person) that processes personal data on behalf of a controller (e.g. the College).

3.4. **Special Categories of Personal Data** – personal data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, physical or mental health, sexual life or sexual orientation. Special Categories of personal data are subject to additional controls in comparison to ordinary personal data.

4. COLLEGE STAFF GENERAL OBLIGATIONS

4.1. All College staff must comply with this policy and associated staff procedures.

4.2. College staff must ensure that they keep confidential all personal data that they collect, store, use and come into contact with during the performance of their duties.

4.3. College staff must not release or disclose any personal data:

- outside the College; or
- inside the college to College staff not authorised to access the personal data,
- without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

4.4. College staff must take all steps to ensure there is no unauthorised access to personal data whether by other College staff who are not authorised to see such personal data or by people outside the College.

5. TRAINING

5.1. The College is committed to providing an appropriate level of training to its staff to help them understand their duties in relation to data protection and to ensure compliance.

6. DATA PROTECTION PRINCIPLES

6.1. When using personal data, Data Protection laws require that the College complies with the following principles which require personal data to be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- accurate and kept up to date, meaning that every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified as soon as possible;
- kept for no longer than is necessary for the purposes for which it is being processed; 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.

6.2. The College has a number of policies and procedures in place, including this policy and the documentation referred to within it, to ensure that the College can demonstrate its compliance.

7. LAWFUL USE OF PERSONAL DATA

7.1. In order to collect and/or use personal data lawfully the College needs to be able to show that its use meets one of a number of legal grounds:

- **Consent:** the individual has given clear consent for processing
- **Contract:** the processing is necessary for a contract with the individual
- **Legal obligation:** the processing is necessary for compliance with the law
- **Vital interests:** the processing is necessary to protect someone's life
- **Public task:** the processing is necessary to perform a task in the public interest
- **Legitimate interests:** the processing is necessary for legitimate business interests

7.2. In addition, when the College collects and/or uses special categories of personal data, the College has to show that one of a number of additional conditions is met:

- Explicit consent;
- Employment and social security obligations;

- Vital interests;
- Necessary for establishment or defence of legal claims;
- Substantial public interest; *and*
- Various scientific and medical issues.

7.3. The College's privacy notices outline the types of personal data (including sensitive personal data) that the College processes and the lawful basis for processing.

8. TRANSPARENT PROCESSING – PRIVACY NOTICES

8.1. Where the College collects personal data directly from individuals, the College will inform them about how the College uses their personal data in a privacy notice. These notices are available on the College website and are subject to regular review.

9. DATA QUALITY

9.1. Data Protection laws require that the College only collects and processes personal data to the extent that it is required for the specific purpose(s) notified to the individual in a privacy notice. The College is also required to ensure that the personal data the College holds is accurate and kept up to date.

9.2. The College will take reasonable steps to ensure that personal data is recorded accurately, is kept up to date and limited to that which is adequate, relevant and necessary in relation to the purpose for which it is collected and used.

9.3. The College will ensure that personal data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection laws.

10. DATA RETENTION

10.1. Data Protection laws require that the College does not keep personal data longer than is necessary for the purpose or purposes for which the College collected it.

10.2. The College has assessed the types of personal data that it holds and the purposes it uses it for and has set retention periods for the different types of personal data processed by the College and the reasons for those retention periods. These are set out in the Data Retention Schedule.

11. DATA SECURITY

The College takes information security very seriously and the College will use appropriate technical and organisational measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.

12. DATA BREACH

12.1. Personal data breach is defined very broadly and is effectively any failure to keep personal data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of personal data.

12.2. There are three main types of personal data breach, which are as follows:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, personal data e.g. hacking, accessing internal systems that a member of staff is not authorised to access, accessing personal data stored on a lost laptop, phone or other device, people gaining access to personal data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
- **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting personal data in error, loss of access to personal data stored on systems, inability to restore access to personal data from backup, or loss of an encryption key; and
- **Integrity breach** - where there is an unauthorised or accidental alteration of personal data.

12.3. In the event that a data breach occurs, the Data Protection Officer must be informed immediately so that appropriate action can be taken. Where applicable, the Information Commissioner's Office will be notified.

13. DATA PROCESSORS

13.1. When appointing a data processor, the College will ensure that appropriate contracts are in place.

13.2. Contracts with external organisations must provide the following obligations as a minimum:

- to only act on the written instructions of the controller;
- to not export personal data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or general) of the controller and under a written contract;
- to keep the personal data secure and assist the controller to do so;
- to assist with the notification of data breaches and DPIA;
- to assist with subject access/individuals' rights;
- to delete/return all personal data as requested at the end of the contract;
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the UK GDPR or other EU or member state data protection law.

13.3. In addition, the contract should set out:

- The subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of individuals; and
- the obligations and rights of the controller.

14. INDIVIDUALS' RIGHTS

14.1. Individuals are responsible for helping the College to keep their personal data up to date. Individuals should let the College know if the information they have provided to the College changes.

14.2. Subject Access Requests

- Individuals have the right under the UK GDPR to ask the College to confirm what personal data they hold in relation to them and to provide them with the data. Such requests should be made to the DPO.

14.3. Right of Erasure (Right to be Forgotten)

This is a limited right for individuals to request the erasure of personal data concerning them where:

- the use of the personal data is no longer necessary;
- their consent is withdrawn and there is no other legal ground for the processing;
- the individual objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data has been unlawfully processed; *and*
- the personal data has to be erased for compliance with a legal obligation.

14.4. Right of Data Portability

An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine-readable format where:

- the processing is based on consent or on a contract; *and*
- the processing is carried out by automated means.

This right isn't the same as subject access and is intended to give individuals a subset of their data.

14.5. The Right of Rectification and Restriction

Individuals are also given the right to request that any personal data is rectified if inaccurate and to have use of their personal data restricted to particular purposes in certain circumstances.

14.6. The College will use all personal data in accordance with the rights given to individuals under Data Protection laws.

15. MARKETING AND CONSENT

15.1. Where the College carries out marketing, Data Protection laws require that this is only done in a legally compliant manner; consent will be obtained where appropriate.

16. AUTOMATED DECISION MAKING AND PROFILING

16.1. Under Data Protection laws there are controls around profiling and automated decision making in relation to individuals.

- **Automated Decision Making** - happens where the College makes a decision about an individual solely by automated means without any human involvement and the decision has legal or other significant effects; *and*

- **Profiling** - happens where the College automatically uses personal data to evaluate certain things about an Individual.

16.2. Where the College uses automated decision making or profiling, the data subject will be informed in the appropriate privacy notice and has a right to object.

17. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

17.1. A DPIA is an assessment of issues affecting personal data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of personal data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; *and*
- outline the measures to address the risks.

17.2. A DPIA will be completed where the use of personal data is likely to result in a high risk to the rights and freedoms of individuals.

17.3. All DPIAs will be reviewed and approved by the Data Protection Officer.

18. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

18.1. The College may transfer personal data outside the European Economic Area to other countries on the basis that such countries are designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards.

18.2. We will inform data subjects of any envisaged international transfers in the relevant privacy notice.

18.3. College staff must not export any personal data outside the EEA without the approval of the Data Protection Officer.