GDPR Compliance Statement

Introduction

The EU General Data Protection Regulation ("GDPR") comes into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. Founded on the fundamentals of privacy by design and a risk-based approach, the GDPR has been designed to meet the requirements of the digital age. The new Regulation aims to standardise data protection laws and processing across the EU, affording individuals stronger, more consistent rights to access and control their personal information.

Our Commitment

Basingstoke College of Technology ('we' or 'us' or 'our' or 'BCoT') are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We recognise the requirement and importance of updating and expanding our data protection program to meet the demands of the GDPR and the UK's Data Protection Bill.

BCoT are dedicated to safeguarding the personal information under our remit and to developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation plans for the GDPR have been summarised in this statement and includes the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

How BCoT are Preparing for the GDPR

Basingstoke College of Technology already has a consistent level of data protection and security across our organisation, however it is our aim to be fully compliant with the GDPR by 25th May 2018. Our preparation includes: -

- **Information Audit** - carrying out a college-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

- **Policies & Procedures** – revising and, where applicable, implementing new data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: -
  - **Data Protection** – our main policy and procedure document for data protection has been rewritten to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.
  - **Data Retention & Erasure** – we are updating our retention policy and schedule to ensure that we meet the 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We are reviewing our erasure procedures to meet the new 'Right to Erasure' obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
  - **Data Breaches** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possibility. Our procedures are robust and have been disseminated to all employees, who are aware of the reporting lines and steps to follow.
  - **International Data Transfers & Third-Party Disclosures** – currently all of our data is stored on servers within the EU, but where BCoT stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a review of the countries where our data may be sent to ensure sufficient and comparable data protection laws; standard data sharing agreements for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.

- **Subject Access Request (SAR)** – we are revising our SAR procedures to accommodate the revised 1-month timeframe for providing the requested information and for making this provision free of charge. Our new procedures will detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and will ensure that communications with data subjects are compliant, consistent and adequate.

- **Legal Basis for Processing** - we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we are also maintaining records of our processing activities, ensuring that our obligations under Article 30 of the GDPR are met.

- **Privacy Notice** – we are revising our Privacy Notice to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

- **Obtaining Consent** - we are revising our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

- **Direct Marketing** - we have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions, a clear notice and method for opting out, and providing unsubscribe features on all subsequent marketing materials.

- **Data Protection Impact Assessments (DPIA)** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

- **Processor Agreements** – where we use any third-party to process personal information on our behalf (i.e. Recruitment, Server Hosting, Marketing), we ensure that the contracts meet the GDPR obligations to keep the data secure and won't be used for marketing purposes. We limit the information we share to only what is necessary. We will also include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.

- **Special Categories Data** - where we obtain and process any special category information, we do so in compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we will provide easy to access information via induction and on our website of an individual's right to access any personal information that Basingstoke College of Technology processes about them and to request information about: -

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store the personal data for

- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

Information Security & Technical and Organisational Measures

Basingstoke College of Technology takes the privacy and security of individuals and their personal information very seriously and are taking every reasonable measure and precaution to protect and secure the personal data that we process. We have dedicated information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including: -

- Ensuring staff are aware of their responsibilities, and only have access to the data that they need and is appropriate for their role
- Using secure, encrypted communication technologies such as SSL
- Ensuring external access to our networks is restricted using firewalls and that antivirus and antimalware software is used
- Ensuring that our software is as up-to-date as possible, with the most recent security patches applied
- Conducting penetration testing through a third party and acting on any recommendations
- Maintaining good backups so that data can be restored if needed
- Having a password policy that requires a good level of complexity and is changed frequently
- Password protecting files containing personal data that are sent externally
- Restricting access (both physically through, for example, locked doors or filing cabinets, and electronically through appropriate permissions to files, folders and systems)
- Using, where possible, anonymisation and pseudonymisation methods to limit the scope of personal data within datasets

GDPR Roles and Employees

Basingstoke College of Technology have designated Greg Devereux-Cooke as our Data Protection Officer (DPO) to develop and implement our roadmap for complying with the new data protection Regulation. The DPO is responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

We utilise a GDPR checklist designed by the ICO to assess each business activity, function and process and to ensure that we have a company-wide approach to meeting the new standards and requirements.

Basingstoke College of Technology understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. We have planned awareness raising activities leading up to 25th May 2018, and will have implemented an employee training program which will be provided to all employees, and forms part of our induction and annual training program.

If you have any questions about our preparation for the GDPR please contact the DPO, email: gdpr@bcot.ac.uk