Oxford's Independent Business School

Data Protection Policy

1.1 The Board of Directors and management of Magna Carta College Ltd, located at 10 Innovation House, Pure Offices, John Smith Drive, Oxford OX4 2JY, are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Magna Carta College Ltd collects and processes in accordance with the General Data Protection Regulation (GDPR).

1.2 Compliance with the GDPR is described by this policy along with connected processes and procedures

1.3 The GDPR and this policy apply to all of Magna Carta College Ltd personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source

1.4 Magna Carta College Ltd has established objectives for data protection and privacy, which are in GDPR Objectives Record.

1.5 Margaret Faulkner, Data Protection Officer, is responsible for reviewing the register of processing annually in the light of any changes to Magna Carta College Ltd activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

1.6 This policy applies to all Employees/Staff and interested parties of Magna Carta College Ltd such as outsourced suppliers. Any breach of the GDPR will be dealt with under Magna Carta College Ltd disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

1.7 Partners and any third parties working with or for Magna Carta College Ltd, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Magna Carta College Ltd without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which Magna Carta College Ltd is committed, and which gives Magna Carta College Ltd the right to audit compliance with the agreement.

2. Responsibilities and roles under the General Data Protection Regulation

2.1 Magna Carta College Ltd is a data controller and data processor under the GDPR

2.2 The Directors and all those in managerial or supervisory roles throughout Magna Carta College Ltd are responsible for developing and encouraging good information handling practices within Magna Carta College Ltd

2.3 Margaret Faulkner is accountable to the Board of Directors of Magna Carta College Ltd for the management of personal data within Magna Carta College Ltd and for ensuring that compliance

10 Innovation House, John Smith Drive, Oxford, OX4 2JY, T: +44 (0) 1865 986787
Company Registration No: 08334025
VAT No: 206690021, ASIC Accreditation Number: AS88822/1117

with data protection legislation and good practice can be demonstrated. This accountability includes:

2.3.1 development and implementation of the GDPR as required by this policy; and
2.3.2 Security and risk management in relation to compliance with the policy.

2.4 Margaret Faulkner (DPO), whom the Board of Directors consider to be suitably qualified and experienced, has been appointed to take responsibility for Magna Carta College Ltd compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that Magna Carta College Ltd complies with the GDPR, as do all members of staff, in respect of data processing that takes place within their area of responsibility.

2.5 The DPO has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

2.6 Compliance with data protection legislation is the responsibility of all Employees/Staff of Magna Carta College Ltd who process personal data.

2.7 Magna Carta College Ltd ensures specific training and awareness requirements in relation to specific roles and Employees/Staff of Magna Carta College Ltd generally.

2.8 Employees/Staff of Magna Carta College Ltd are responsible for ensuring that any personal data about them and supplied by them to Magna Carta College Ltd is accurate and up-to-date.

3. Data protection principles

All processing of personal data will be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Magna Carta College Ltd policies and procedures are designed to ensure compliance with the principles.

4. Data subjects' rights

4.1 **Data subjects have the following rights regarding data processing, and the data that is recorded about them:**

4.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
4.1.2 To prevent processing likely to cause damage or distress.
4.1.3 To prevent processing for purposes of direct marketing.
4.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.
4.1.5 To not have significant decisions that will affect them taken solely by automated process.
4.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.
4.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
4.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

10 Innovation House, John Smith Drive, Oxford, OX4 2JY, T: +44 (0) 1865 986787
Company Registration No: 08334025
VAT No: 206690021, ASIC Accreditation Number: AS88822/1117

4.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

4.1.10 To object to any automated profiling that is occurring without consent.

4.2 Magna Carta College Ltd ensures that data subjects may exercise these rights:

4.2.1 Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how Magna Carta College Ltd will ensure that its response to the data access request complies with the requirements of the GDPR.

4.2.2 Data subjects have the right to complain to Magna Carta College Ltd related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

5. Consent

5.1 Magna Carta College Ltd understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

5.2 Magna Carta College Ltd understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

5.3 There must be consent to the Privacy Notice and consent cannot be inferred from non-response to a communication.

5.4 For sensitive data, explicit written consent, in the form of a signed and accepted copy of the privacy notice.

5.5 In most instances, consent to process personal and sensitive data is obtained routinely by Magna Carta College Ltd using standard consent documents e.g. when a new client signs a contract, or during induction for participants on programmes.

5.6 Where Magna Carta College Ltd provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit, which may be no lower than 13).

6. Security of data

6.1 All Employees/Staff are responsible for ensuring that any personal data that Magna Carta College Ltd holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Magna Carta College Ltd to receive that information and has entered into a confidentiality agreement.

10 Innovation House, John Smith Drive, Oxford, OX4 2JY, T: +44 (0) 1865 986787
Company Registration No: 08334025
VAT No: 206690021, ASIC Accreditation Number: AS88822/1117

6.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- **in a lockable room with controlled access; and/or**
- **in a locked drawer or filing cabinet; and/or**
- **if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or**
- **Stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media.**

6.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorise Employees/Staff of Magna Carta College Ltd. All Employees/Staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

6.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

6.5 Personal data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required before disposal.

6.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

7. Disclosure of data

7.1 Magna Carta College Ltd must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All [Employees/Staff] should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Magna Carta College Ltd business.

7.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO.

8. **Retention and disposal of data**

8.1 Magna Carta College Ltd shall not keep personal data in a form that permits identification of data subjects for a longer period than is necessary, in relation to the purpose for which the data was originally collected.

8.2 Magna Carta College Ltd may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

10 Innovation House, John Smith Drive, Oxford, OX4 2JY, T: +44 (0) 1865 986787
Company Registration No: 08334025
VAT No: 206690021, ASIC Accreditation Number: AS88822/1117

8.3 The retention period for each category of personal data will be set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations Magna Carta College Ltd has to retain the data.

8.4 Magna Carta College Ltd data retention and data disposal procedures will apply in all cases.

8.5 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

9. Data transfers

9.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects (as per ICO guidelines).
The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

9.1.1 An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.* *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

9.1.2 Privacy Shield

If Magna Carta College Ltd wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

10 Innovation House, John Smith Drive, Oxford, OX4 2JY, T: +44 (0) 1865 986787
Company Registration No: 08334025
VAT No: 206690021, ASIC Accreditation Number: AS88822/1117

Assessment of adequacy by the data controller

In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations
- The security measures that are to be taken as regards the data in the overseas location.

9.1.3 Binding corporate rules

Magna Carta College Ltd may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that Magna Carta College Ltd is seeking to rely upon.

9.1.4 Model contract clauses

Magna Carta College Ltd may adopt approved model contract clauses for the transfer of data outside of the EEA. If Magna Carta College Ltd adopts the model contract clauses approved by the relevant supervisory authority there is an automatic recognition of adequacy.

9.1.5 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

10 Innovation House, John Smith Drive, Oxford, OX4 2JY, T: +44 (0) 1865 986787
Company Registration No: 08334025
VAT No: 206690021, ASIC Accreditation Number: AS88822/1117

10. Information asset register/data inventory

10.1 Magna Carta College Ltd has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. Magna Carta College Ltd data inventory and data flow determines:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Organisation Name throughout the data flow;
- key systems and repositories;
- any data transfers and
- All retention and disposal requirements**.**

10.2 **Magna Carta College Ltd is aware of any risks associated with the processing of particular types of personal data.**

10.2.1 Magna Carta College Ltd assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by Magna Carta College Ltd, and in relation to processing undertaken by other organisations on behalf of Magna Carta College Ltd.

10.2.2 Magna Carta College Ltd shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

10.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Magna Carta College Ltd shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

10.2.4 Where, as a result of a DPIA, it is clear that Magna Carta College Ltd is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Magna Carta College Ltd may proceed must be escalated for review to the DPO.

10.2.5 The DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

10.2.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, in compliance with the GDPR.

10 Innovation House, John Smith Drive, Oxford, OX4 2JY, T: +44 (0) 1865 986787
Company Registration No: 08334025
VAT No: 206690021, ASIC Accreditation Number: AS88822/1117

A current version of this document is available to all members of staff.

This policy was approved by the [Board of Directors] on *[01.04.2018]* and is issued on a version controlled basis under the signature of the [Chief Executive Officer (CEO)].

Signature: **Date: 1st April 2018**

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	MSF	01/04/2018

10 Innovation House, John Smith Drive, Oxford, OX4 2JY, T: +44 (0) 1865 986787
Company Registration No: 08334025
VAT No: 206690021, ASIC Accreditation Number: AS88822/1117