Varsity

Section 1 - Data Protection Statement

Introduction

For ease of understanding, and also for the purpose of full transparency this document is applicable to all activities within the group of organisations that effectively form "Varsity" (or otherwise for the sake of simplicity referred to as "The Company" in the remainder of this document).

These are:

1. **Varsity Publications Ltd** – a not for profit Limited Company registered in England & Wales whose registration number is 561235. The company is registered for VAT – the registration number is GB 213 9420 86. Varsity is registered with the specific SIC code 58130 - Publishing of newspapers.

The principal activities of Varsity Publications Ltd are those of a media organisation – in brief, the company produces:

- A print newspaper published during Cambridge University term-time.
- A news media website which publishes throughout the year.
- An annual academic Wallplanner/Yearplanner.
- An annual Guide to Careers.
- An annual anthology of poetry, prose and artwork/illustrations called "The Mays" featuring new, previously unpublished work from the students of Oxford University and the University of Cambridge.

2. **The Varsity Society** (more commonly referred to as "VarSoc") – an official student society registered with the proctors at the University of Cambridge whose activities are subject to University rules, supervision and oversight; it is an official student society registered with the proctors at the University of Cambridge. The Society's membership is made up principally of resident junior members of the University of Cambridge. The principal function of The Varsity Society is to provide its membership with educational and social activities and opportunities related to the Company's activities.

3. **The Varsity Trust** – A charity registered in England & Wales whose registration number is 1012847. The principal activities of the Varsity Trust are furthering the education of students in journalism; principally by the provision of funds in the form of scholarships, bursaries or grants to eligible students.

Separate accounting procedures are in place for each organisation above in accordance with the applicable laws of England & Wales, along with applicable rules set out by the University of Cambridge. Separate bank accounts are in place for each organisation.

Dr Mike Franklin has been appointed the Company's data protection officer. This appointment has been made as Dr Franklin holds senior official positions across all three organisations – these being: the Chairman and a majority shareholder of Varsity Publications Ltd, the Chairman and a Trustee of the Varsity Trust and the Senior Treasurer of The Varsity Society.

The types of data we collect and use

A review and audit was conducted with input from Mark Curtis, Business Manager, Mike Franklin, Varsity Chairman and Michael Derringer, Varsity director & IT Contractor.

Varsity Publications Ltd

Varsity holds personal information regarding the shareholders of the company. This is a legal obligation.

Varsity holds personal information regarding the directors of the company. This is a legal obligation.

Varsity collects the personal information of web site users through its Server Logs in the form of user IP addresses. This is a legal obligation.

Varsity collects personal information regarding its users for the purposes of Website security and diagnostics. Data retained is deemed to be proportionate and Varsity only keeps data for 60 days before deletion.

Varsity collects information from its clients and suppliers for invoicing and accounting purposes in the form of client/supplier purchase history and contact details. This is a legal obligation.

Varsity collects information regarding current and prospective clients in the form of a customer contact database (name, email address, address, industry sector, publications that they have booked into or showed an interest in and sector of activity – for example “Retail”, “Graduate Recruitment” etc.) Varsity does not currently share this information with any third parties. No bulk emailing sales systems are utilised or third party CRM management is utilised. There is a legitimate interest in the information being held as it essential to the operation of the company – however clients on this list are immediately deleted upon request.

Varsity operate a free equipment loan scheme for its students and personal data is collected in order to operate this scheme effectively. This data is not retained for a period longer 12 months.

The Editors of Varsity will collect personal data from prospective and current student contributors, for example through signing up students at Freshers’ Fairs or other similar events, for the purposes of commissioning articles and general administrative use in running the publication. Those signing up for such lists have the option for their information to be deleted upon request.

Note: It is important to note the key data collected here other than the individuals name is their email address. University Information Services (UIS allocated email addresses (more commonly referred to as “CRS IDs”) have a pre-determined “lifespan” and last for only as long as the student or member is deemed a student resident in the University of Cambridge. However, all email addresses and any other data (other than name) should be deleted once a student is no longer a resident member of the University of Cambridge.

This note may also be applicable, in whole or in part to other sections of this report.

The Editors of Varsity will collect additional personal data from key student members for the purposes of allowing secure card access to the Varsity offices at the University of Cambridge.

Student (and indeed staff) cards are issued and administered by the University of Cambridge and are therefore not under the control of Varsity. However, it is necessary for Varsity to collect personal data on a termly basis (card numbers and "Mifare" numbers) in order to pass this on to the University so designated team members are able to access the building. Redundant data should be deleted on a termly basis by the Editors.

When students or members of the public are in correspondence with members of the Varsity team, it is done through allocated varsity email addresses, specific to each role e.g.: editor@varsity.co.uk, music@vsarsity.co.uk) – these emails are allocated on a termly basis to those undertaking those role in publication. These communications to such @varsity.co.uk addresses are then effectively forwarded on to the relative team members own email address allocated by the University of Cambridge. Varsity does not retain such incoming email traffic on its own servers for any period longer than is necessary to complete the forwarding process.

Varsity will hold personal data in the form of copyright release forms and similar release documents from the contributors to the newspaper. This is a legal requirement. As the licence period granted is in perpetuity, records held are kept permanently.

Varsity will retain personal data from those individuals who complain to the newspaper. Data held in the regard will not normally be held for longer than a period of seven years in order to protect the company in the event of any legal proceedings.

The other forms of communication by means of which members of the public may communicate or otherwise interact with Varsity include Facebook, Twitter and Instagram – Varsity believes that appropriate data protection measures are in place from these providers.

Internally, Varsity uses the Slack software communication system for private interaction internally – Varsity believes that appropriate data protection measures are in place from this provider. Regardless, access to Slack is principally only available to those holding a current @Varsity.co.uk email address, and therefore access to this facility is only enabled for as long as it is the individual has a defined role on the editorial team.

Varsity will from time to time retain personal information in order to publish lists of the names of former editors and notable contributors. This archiving activity is regarded as being in the public interest.

It should be noted again that all other personal data collected is deemed to fall under the two sections further on in the report marked "Exemptions" and "The Journalistic Exemption".

The Varsity Trust

The Varsity Trust collects personal information from those who apply for funding. Data from unsuccessful applicants will not be held for a period longer than 12 months. Data from successful applicants should be retained for a period of seven years in the event of any queries on enquiry from the Charity Commission of England & Wales or the Trust's own auditors.

Varsity will from time retain data in order to publish lists of the names of former Trust recipients. This archiving activity is regarded as being in the public interest though in this case the option of a Trust recipient to have their name removed in future publications is available upon request.

The Mays

The Mays will hold personal data in the form of copyright release forms from the contributors to the publications. This is a legal requirement. However, as the licence granted is only for a period of five years. Any records held after that date will be destroyed.

The Mays will hold and publish a list of current/former editors and contributors – these are exempt as this archiving activity is regarded as being in the public interest

The Mays has an online shop, where members of the public may purchase copies of the publication. Transactions for purchases are conducted through the PayPal system and so will fall in part under PayPal's own data governance. At present The Mays holds the personal information regarding those purchasing the books that is necessary to fulfil these orders and deal with any complaints etc, for example non-delivery. Any personal information is removed after a period of 12-24 months.

The Mays collects information from its clients (typically donating Colleges of Oxford University and the University of Cambridge) and suppliers for invoicing and accounting purposes in the form of client/supplier purchase history and contact details. This is a legal obligation.

The Mays collects information regarding current and prospective clients in the form of a customer contact. The Mays does currently does not share this information with any third parties. No bulk emailing sales systems are utilised or third party CRM management is utilised. There is a legitimate interest in the information being held as it essential to the operation of the company.

Varsoc

Currently no central record or database consists of past Varsoc members (Varsity contributors) currently exists. In January 2018 the Varsity Board resolved to establish such an alumni list with information including name, address, College, current email address, years worked on the publications, roles held etc. The list once established will be used to assist the Chairman with a long term project of writing a new history of Varsity (to update the previously published "From our Cambridge Correspondent" by Mark Weatherall published in 1995); this would be exempt as it would be classed under historical research purposes and more broadly can be classed as "employee data". However, this database would also be used by the Varsoc President in order to send invitations to the Varsity annual dinner, garden party etc and also possibly in the future in order to contact alumni who may be interested in taking up a paid subscription to the newspaper and other fundraising activities. Therefore the option to opt out of receiving further communication and the option to have their data deleted (for these latter purposes) is available.

Varsoc does collect personal data from its membership wishing to purchase branded promotional wear during their time on the paper. This will not be held for a period any longer than 12 months.

Varsoc does collect personal data from its membership for the purpose of administering the Varsity annual dinner and other such events. This should not be held for a period any longer than 12 months.

Varsoc does collect personal data from its membership and may pass this data on to a third party voting system for the purposes of operating and administrating the election of a student President.

Exemptions

It is important to note that Varsity operates principally as a media organisation, and established appropriate exemptions under the GDPR are considered be applicable with regard to these activities. This section of the document has been adopted from published advice from the law firm Taylor Wessing in October 2017.

It should be noted that they are still awaiting appropriate further legislation and clarification, this section will be updated once this is in place.

There are exemptions under the GDPR allowing controllers and processors to derogate from the specific personal data processing provisions they are to be found in Articles 85-91 of the GDPR. They include certain processing relevant to:

- Freedom of expression and information
- Public access to official documents
- National identification numbers
- Employee data
- Scientific and historical research purposes or statistical purposes
- Archiving in the public interest
- Obligations of secrecy
- Churches and religious associations.

In these areas there is potential for disparity between different EU Member States, as each will have the ability to introduce supplemental laws or derogations relevant to these special situations as well as derogations on issues such as national security, public security, the protection of judicial independence and proceedings and the enforcement of civil law matters, subject to these national measures being necessary and proportionate.

The Journalistic Exemption

Of key relevance to media organisations is the exemption relating to freedom of expression and information under Article 85, which states: “Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression”. Recital 153 of the GDPR includes that “In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.”

The journalistic purposes derogation, where relevant, applies to most of the provisions of the GDPR (including the principles, the rights of data subjects and transfers of personal data to countries

outside of the EU) meaning that the processing subject to it will generally not have to be compliant with those parts of the rules.

National Governments will be required to put legislative measures in place to implement this exemption, which shall be enforced by local regulatory authorities. In the UK, this will be the Information Commissioner's Office (the 'ICO').

In the UK, the DPA currently contains the special purposes exemption under section 32 (the 'journalistic exemption') which exempts data controllers from complying with most of the provisions of the DPA and states:

1. Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if —

a. the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,

b. the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and

c. the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.

Although section 32 of the DPA is likely to be repealed, the UK Government, via the Department for Digital, Culture Media & Sport, published on 7 August 2017 a statement of intent entitled "A New Data Protection Bill: Our Planned Reforms" confirming that a new provision, but one broadly replicating the existing section 32 (which it states strikes "the right balance") will be enacted in its place when the GDPR comes into force. The main difference will be to amend provisions relating to the ICO's enforcement powers to strengthen its ability to enforce the re-enacted journalistic exemption effectively. On 14 September 2017 the Government published the Data Protection Bill which is intended to replace and repeal the DPA and to deal with various matters reserved to EU Member States by the GDPR, including Article 85.

Part 5 of Schedule 2 of the Bill states, at paragraph 24 (which follows section 32 of the DPA) , that:

1. In this paragraph, "the special purposes" means one or more of the following—

a. the purposes of journalism;

b. academic purposes;

c. artistic purposes;

d. literary purposes.

2. The listed GDPR provisions do not apply to personal data that is being processed only for the special purposes to the extent that:

a. the personal data is being processed with a view to the publication by a person of journalistic, academic, artistic or literary material,

b. the controller reasonably believes that publication of the material would be in the public interest; and

c. the controller reasonably believes that the application of any one or more of the listed GDPR provisions would be incompatible with the special purposes.

3. In determining whether publication would be in the public interest the controller must take into account the special importance of the public interest in the freedom of expression and information.

4. In determining whether it is reasonable to believe that publication would be in the public interest, the controller must have regard to any of the codes of practice or guidelines listed in sub-paragraph (5) that is relevant to the publication in question.

5. The codes of practice and guidelines are:

a. BBC Editorial Guidelines;

b. Ofcom Broadcasting Code;

c. IPSO Editors' Code of Practice.

11. With reference to sections 32(4) and 32(5) of the DPA, section 166 of the Bill deals with staying special purposes proceedings and states:

1. In any special purposes proceedings before a court or tribunal, if the controller or processor claims, or it appears to the court or tribunal, that any personal data to which the proceedings relate:

a. is being processed only for the special purposes,

b. is being processed with a view to the publication by any person of journalistic, academic, literary or artistic material, and

c. has not previously been published by the controller, the court or tribunal must stay the proceedings.

2. In considering, for the purposes of subsection (1)(c), whether material has previously been published, publication in the immediately preceding 24 hours is to be ignored.

3. Under subsection (1), the court or tribunal must stay the proceedings until either of the following conditions is met—

a. a determination of the Commissioner under section 164 with respect to the personal data or the processing takes effect;

b. where the proceedings were stayed on the making of a claim, the claim is withdrawn.

The following decisions in the English civil courts on the interpretation of section 32 give an indication of how things will likely continue after the GDPR comes into force in England.

Steinmetz v Global Witness [2014] EWHC 1186 (Ch) – The ICO (having been referred this issue by the English High Court) decided that section 32 applied broadly to anyone engaged in public interest

reporting, not just conventional media organisations, and that journalism is widely defined as imparting information, opinions and ideas for general public consumption. This allowed Global Witness (a not for profit NGO which raises public awareness and campaigns on alleged corruption relating to natural resources) to defend the claims being brought against it under the DPA. Further, the ICO stated that its role was not to decide if there was a public interest, but whether the data controller's belief that there was one was reasonable.

Stunt v Associated Newspapers [2017] EWHC 695 (QB) – The English High Court held that section 32(4) of the DPA, which effectively stays a civil data protection claim brought against a data controller in respect of unpublished data held for the purposes of journalism was not incompatible with EU law. The court ordered that the relevant parts of the data protection claims brought against the defendant publisher (for alleged failure to comply with subject access, erasure and cease processing requests) be stayed under section 32(4).

Along with these cases, other indications of how the ICO might deal with section 32 issues if empowered by a new, similar provision pursuant to Article 85 of the GDPR, come from the ICO's guidance entitled "Data protection and journalism: a guide for the media". This recommends, for example, that media organisations have clear policies on what content requires editorial approval, provide awareness training to staff on data protection, create an inbuilt public interest check at key stages of a story (e.g. when using covert methods or giving a final decision to publish) and keep an audit trail for high-profile or intrusive stories.

Section 2 – Data Protection Policy

Introduction

This Policy sets out the obligations of Varsity ("the Company") including its associated institutions – laid out in Section 1 regarding data protection and the rights of customers, business contacts ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. **The Data Protection Principles**

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;
b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against Data Protection Policy accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. **Lawful, Fair, and Transparent Data Processing**

The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. **Processed for Specified, Explicit and Legitimate Purposes**

4.1 The Company collects and processes the personal data set out in Part 21 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties.
4.2 The Company only processes personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible after collection where it is obtained from a third party.

5. **Adequate, Relevant and Limited Data Processing**

The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. **Accuracy of Data and Keeping Data Up to Date**

The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and annual intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. **Timely Processing**

The Company shall not keep personal data for any longer than necessary. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

8. **Secure Processing**

The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy.

9. **Accountability**

9.1 The Company's data protection officer is Dr Mike Franklin chaiman@varsity.cam.ac.uk
9.2 The Company has conducted an audit and review of all of its activities with regard to data processing. These are detailed in the first section of this report.

10. **Privacy Impact Assessments**

The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Company's data protection officer and shall address the following areas of importance:

10.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
10.2 Details of the legitimate interests being pursued by the Company;
10.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
10.4 An assessment of the risks posed to individual data subjects; and
10.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. **The Rights of Data Subjects**

The Regulation sets out the following rights applicable to data subjects:
a) The right to be informed;

b) The right of access;
c) The right to rectification;
d) The right to erasure (also known as the 'right to be forgotten');
e) The right to restrict processing;
f) The right to data portability;
g) The right to object;
h) Rights with respect to profiling.

12. **Keeping Data Subjects Informed**

12.1 The Company shall ensure that the following information is provided to every data subject when personal data is collected:
12.2 Details of the Company including, but not limited to, the identity of its Data Protection Officer;
a) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
b) Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
c) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
d) Where the personal data is to be transferred to one or more third parties, details of those parties;
e) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers);
f) Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);
g) Details of the data subject's rights under the Regulation;
h) Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;
i) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);
j) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
12.3 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:
12.3.1 Where the personal data is obtained from the data subject directly, at the time of collection;
12.3.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):
a) If the personal data is used to communicate with the data subject, at the time of the first communication; or
b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or
c) In any event, not more than one month after the time at which the Company obtains the personal data.

13. **Data Subject Access**

13.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of

the need for the extension).
13.2 All subject access requests received must be forwarded to Dr M Franklin, the Company's data protection officer chairman@varsity.cam.ac.uk
13.3 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. **Rectification of Personal Data**

14.1 If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).
14.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. **Erasure of Personal Data**

15.1 Data subjects may request that the Company erases the personal data it holds about them in the following circumstances:
a) It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;
b) The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
c) The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object);
d) The personal data has been processed unlawfully;
e) The personal data needs to be erased in order for the Company to comply
15.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).
15.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. **Restriction of Personal Data Processing**

16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.
16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. **Data Portability**

17.1 The Company processes personal data using manual process.
17.2 Where data subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).
17.3 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following formats:
a) Adobe PDF or established Microsoft Office formats
17.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.
17.5 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

18. **Objections to Personal Data Processing**

18.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling).
18.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.
18.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.
18.4 Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. **Profiling**

In the event the Company uses personal data for profiling purposes, the following shall apply:
a) Clear information explaining the profiling will be provided, including its significance and the likely consequences;
b) Appropriate mathematical or statistical procedures will be used;
c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and
d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 21 and 22 of this Policy for more details on data security).

20. **Personal Data**

This is covered in Section 1 – "The types of data we collect and use"

21. **Data Protection Measures**

The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:
a) All emails containing personal data should ensure appropriate data protection measures are put in place; however, practically it is the University Information Service (UIS) at the University of Cambridge that provides the bulk of our users with an email platform (Hermes)
b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely.
c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
d) Personal data contained in the body of an email, whether sent or received, should be stored securely. All temporary files associated therewith should also be deleted;
e) In the unlikely event where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
f) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient (or sent using an established postage service or other courier including the University Messenger Service)
g) No personal data may be shared informally and if an employee, agent, subcontractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Varsity Data Protection Officer.
h) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored in the Varsity office which is secured via an authorised card access system.
i) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the Varsity Data Protection Officer or the Varsity Business Manager.
j) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;
k) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user should lock the computer and screen before leaving it;
l) Staff must take when data should be stored on mobile device (including, but not limited to, laptops, tablets and smartphones) and ensure the device is secure (password protected) and that any is not held on these devices for any longer than is absolutely necessary.
m) No personal data should be transferred to any device personally belonging to any employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);
n) All personal data stored electronically shall be backed up daily with backups stored onsite or at the UIS.
o) All electronic copies of personal data should be stored securely.
p) All passwords used to protect personal data should be changed regularly.
q) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, save for appropriate sharing between Mike Franklin, Varsity Chairman, Michael Derringer Varsity Director and IT Contractor and Mark Curtis the Varsity Business Manager which are deemed necessary for the smooth operation of the Company.

22. **Organisational Measures**

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:
a) All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, Data Protection Policy and shall be provided with a copy of this Policy through its' publication on the shared Varsity server to which all those working in the office have access;
b) Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
c) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately advised;
d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
f) The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
g) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;
h) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation;
i) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

23. **Transferring Personal Data to a Country Outside the EEA**

24.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.
24.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between
public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
c) The transfer is made with the informed consent of the relevant data subject(s);

d) The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
e) The transfer is necessary for important public interest reasons;
f) The transfer is necessary for the conduct of legal claims;
g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

25. **Data Breach Notification**

25.1 All personal data breaches must be reported immediately to the Company's data protection officer.
25.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
25.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
25.4 Data breach notifications shall include the following information:
a) The categories and approximate number of data subjects concerned;
b) The categories and approximate number of personal data records concerned;
c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
d) The likely consequences of the breach;
e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

26. **Implementation of Policy**

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Mike Franklin
Position: Varsity Chairman
Date: 19th May 2018
Due for Review by: 29th March 2019
Signature: