

This Agreement is dated 19 April 2023

PARTIES

- (1) **UNIVERSITY OF WARWICK** incorporated and registered in England and Wales with Royal Charter Number RC000678 whose registered address is the University of Warwick, Coventry, CV4 8UW (“**Warwick**”); and
- (2) **WARWICK STUDENTS’ UNION LIMITED** incorporated and registered in England and Wales with registered number 7297865 whose registered address is at SU HQ, Gibbet Hill Road, Coventry CV4 7AL (“**the SU**”).

BACKGROUND

- (A) Warwick is sharing Personal Data with the SU and receiving Personal Data from the SU.
- (B) Each Party will use the Personal Data for its own purposes as separate Data Controllers.

AGREED TERMS

1. DATA PROTECTION

- 1.1 Each Party agrees to comply with its obligations as set out in Schedule 1 (Data Protection) of this Agreement.

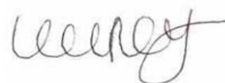
This Agreement has been entered into on the date stated at the beginning of it.

Signed for an on behalf of Warwick:



Matthew Collins, Senior Legal Counsel

Signed for an on behalf of the SU:



Tracy Murphy Chief Executive - interim

SCHEDULE 1

DATA PROTECTION

1. DEFINITIONS

In this Schedule 1 the following definitions shall apply:

"Controller", "Processor", "Data Subject" "Personal Data" and "Sensitive Personal Data/Special Category Data "	shall have the meaning given to those terms in the applicable Data Protection Laws;
"Data Protection Authorities"	means the UK Information Commissioner's Office;
"Data Protection Laws"	means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 2018 and, the General Data Protection Regulation ("UK GDPR") Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5.2016 as retained in the law of England and Wales, and all legislation enacted in the UK in respect of the protection of personal data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) including any relevant replacement/subsequent European and/or UK legislation together with all codes of practice and other guidance on the foregoing issued by any relevant Data Protection Authority, all as amended from time to time;
"Data Processing Particulars"	means, in relation to any Processing under this Agreement: (a) the subject matter and duration of the Processing; (b) the nature and purpose of the Processing; (c) the type of Personal Data being Processed; and (d) the categories of Data Subjects; as set out in Appendix 1 (<i>Data Processing Particulars</i>).
"Data Subject Request"	means an actual or purported request or notice or complaint from or on behalf of a Data Subject exercising his rights under the Data Protection Laws in relation to Personal Data including without limitation: the right of access by the Data Subject, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability and the right to object;
"Regulator"	means the UK Information Commissioner's Office, or any successor or replacement body from time to time; also means the relevant local governmental or other official regulator(s) responsible for

enforcement of the Data Protection Legislation from time to time in relation to Warwick

- "Regulator Correspondence"** means any correspondence or communication (whether written or verbal) from the Regulator in relation to the Processing of Personal Data;
- "Losses"** means all losses, fines, penalties, liabilities, damages, costs, charges, claims, amounts paid in settlement and expenses (including legal fees (on a solicitor/client basis), disbursements, costs of investigation (including forensic investigation), litigation, settlement (including ex gratia payments), judgment, interest and penalties), other professional charges and expenses, disbursements, cost of breach notification including notifications to the data subject, cost of complaints handling (including providing data subjects with credit reference checks, setting up contact centres (e.g. call centres) and making ex gratia payments), all whether arising in contract, tort (including negligence), breach of statutory duty or otherwise;
- "Permitted Recipients"** means the third parties to whom each Party is permitted to disclose the Personal Data, as set out in more detail in Appendix 1 (*Data Processing Particulars*);
- "Personal Data"** means any personal data (as defined in the Data Protection Laws) Processed by either Party in connection with this Agreement, and for the purposes of this Agreement includes Sensitive Personal Data/Special Category Data (as such Personal Data is more particularly described in Appendix 1 (*Data Processing Particulars*));
- "Personal Data Breach"** has the meaning set out in the Data Protection Laws and includes any actual or suspected, threatened or 'near miss ' personal data breach in relation to the Personal Data and, for the avoidance of doubt, includes a breach of paragraph 2.2.2(e);
- "Processing"** means any use of or processing applied to any Personal Data and includes "process" or "processing" as defined in applicable Data Protection Legislation. For the avoidance of doubt, this includes, without limitation, collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying Personal Data;
- "Third Country"** means a country, territory or jurisdiction outside of the United Kingdom which is not deemed to provide adequate protection in accordance with Article 45(1) of the UK GDPR (as applicable); and
- "Security Measures"** means the requirements regarding the security of Personal Data, as set out in the Data Protection Laws and the measures set out in Articles 28 and 32 of the UK GDPR as applicable and as set out in the Data Processing Particulars.

2. DATA PROTECTION

2.1 Nature of the Processing

2.1.1 The Parties acknowledge that the factual arrangements between them dictate the role of each Party in respect of the Data Protection Laws. Notwithstanding the foregoing, each Party agrees that the nature of the Processing under this Agreement will be as follows:

- (a) the Parties shall each Process the Personal Data;
- (b) each Party shall act as a Controller in respect of the Processing of the Personal Data on its own behalf and in particular each shall be a Controller of the Personal Data acting individually and in common, as follows:
 - (i) Warwick shall be a Controller where it is Processing Personal Data in relation to its purposes as set out in Appendix 1 (*Data Processing Particulars*) and
 - (ii) the SU shall be a Controller where it is Processing Personal Data in relation to its purposes as set out in Appendix 1 (*Data Processing Particulars*).
- (c) Notwithstanding Paragraph 2.1.1(b), if either Party is deemed to be a joint Controller with the other in relation to the Personal Data, the Parties agree that they shall be jointly responsible for the compliance obligations imposed on a Controller by the Data Protection Laws, and the Parties shall cooperate to do all necessary things to enable performance of such compliance obligations.

2.1.2 Each of the Parties acknowledges and agrees that Appendix 1 (*Data Processing Particulars*) to this Agreement is an accurate description of the Data Processing Particulars.

2.2 Data Controller Obligations for each Party

2.2.1 Each Party shall in relation to the Processing of the Personal Data comply with its respective obligations under the Data Protection Laws.

2.2.2 Without limiting the generality of the obligation set out in Paragraph 2.2.1, in particular, each Party shall:

- (a) where required to do so make due notification to the Regulator;
- (b) ensure it is not subject to any prohibition or restriction which would:
 - (i) prevent or restrict it from disclosing or transferring the Personal Data to the other Party as required under this Agreement;
 - (ii) prevent or restrict it from granting the other Party access to the Personal Data as required under this Agreement; or
 - (iii) prevent or restrict either Party from Processing the Personal Data, as envisaged under this Agreement;
- (c) ensure that all privacy notices have been provided (and/or, as applicable, consents obtained) and are sufficient in scope to enable each Party to Process the Personal Data as required in order to

obtain the benefit of its rights and to fulfil its obligations under this Agreement in accordance with the Data Protection Laws (for the avoidance of doubt neither party warrants to the other that any use of the Personal Data outside the scope of this Agreement shall be compliant with the Data Protection Laws).

- (d) ensure that all Personal Data disclosed or transferred to, or accessed by, the other Party is accurate and up-to-date, as well as adequate, relevant and not excessive to enable either Party to Process the Personal Data as envisaged under this Agreement;
- (e) ensure that appropriate technical and organisational security measures are in place sufficient to comply with
 - (i) at least the obligations imposed on the Controller by the Security Measures; and
 - (ii) the obligations set out in the Data Processing Particulars;and where reasonably requested provide to the other party evidence of its compliance with such requirements promptly, and in any event immediately on request;
- (f) notify the other Party immediately on receipt of any Data Subject Request or Regulator Correspondence which relates directly or indirectly to the Processing of Personal Data under, or in connection with, this Agreement and together with such notice, provide a copy of such Data Subject Request or Regulator Correspondence to the other Party and reasonable details of the circumstances giving rise to it. In addition to providing the notice referred to in this Paragraph 2.2.2(f), each Party shall provide the other Party with all co-operation and assistance required by the other Party in relation to any such Data Subject Request or Regulator Correspondence;
- (g) provide a contact point for enquiries to Data Subjects and subject to any obligations of confidentiality will make available, upon request, a summary of this Schedule 1 to Data Subjects;
- (h) notify the other Party immediately upon receipt of a Data Subject Request or Regulator Correspondence. Upon notification, the Parties shall determine who shall have sole conduct of the response to any such data subject request or ICO Correspondence, with the other Party providing reasonable co-operation and assistance;
- (i) use reasonable endeavours to notify the other Party if it is obliged to make a disclosure of any of the Personal Data under any statutory requirement, such notification to be made in advance of such disclosure or immediately thereafter unless prohibited by law;
- (j) notify the other Party in writing by following the procedure set out in Appendix 2 (*Notification Procedure*) immediately upon becoming aware of any actual or suspected Personal Data Breach in relation to the Personal Data received from the other Party and shall, within such timescale to be agreed by the Parties
 - (i) implement any measures necessary to restore the security of compromised Personal Data; and

- (ii) support the other Party to make any required notifications to the Regulator and/or other relevant regulatory body and affected Data Subjects;
- (k) not do anything which shall damage the reputation of the other Party or that Party's relationship with the Data Subjects;
- (l) not transfer any Personal Data it is processing to a Third Country;
- (m) hold the information contained in the Personal Data confidentially and under at least the conditions of confidence as such Party holds Personal Data Processed by it other than the Personal Data; and
- (n) not disclose the Personal Data to a third party (including a sub-contractor) in any circumstances without the other Party's prior written consent, save in relation to:
 - (i) disclosures to Permitted Recipients; and
 - (ii) unless that Party is prohibited by law or regulation from notifying the other Party of that disclosure, in which case it shall do so as soon as practicable thereafter (where permitted by law or regulation);
- (o) arrange for the prompt and safe return and/or secure permanent of all Personal Data, together with all copies in its possession or control within 30 days and, where requested by the other Party certify that such destruction has taken place.

3. **INDEMNITY**

3.1 The Parties shall indemnify each other on an after tax basis against any:

3.1.1 monetary penalties or fines; and

3.1.2 losses, damage, costs, charges, expenses and liabilities (including reasonable legal fees and disbursements);

in each case incurred or suffered by it or arising out of or in connection with any breach by the other party of this Schedule 1.

3.2 Notwithstanding any other provision of this Agreement limiting either Party's liability, but subject always to there being no liability limit on either Party for death or personal injury caused by negligence or for fraud or fraudulent misrepresentation, each Party's liability under this indemnity shall be limited to five hundred thousand pounds (£500,000) per event or series of related events.

APPENDIX 1

DATA PROTECTION PARTICULARS

The purposes for which Warwick is Data Controller
Its public functions namely research and education including its incidental functions e.g. as an employer, land owner, etc..
The purposes for which the SU is Data Controller
Its functions as a students' union including its functions as an employer.
The subject matter and duration of the Processing
<p>Although Warwick and the SU are separate legal entities, they work together to support the efficient delivery of services and support to students, staff and the wider community. As such the relationship between Warwick and the SU requires the sharing of Personal Data.</p> <p>Each category of personal data listed below will have its own duration for processing however this data sharing agreement will be reviewed on an annual basis in line with the academic year.</p>
The nature and purpose of the Processing
<ul style="list-style-type: none">• Data migration/sharing;• Recording and storing;• Organising, adapting and altering;• Retrieving, consulting, processing;• Erasing and destroying.
The type of Personal Data being Processed
<ol style="list-style-type: none">1. <u>Student membership data</u> Background: Specific datasets are shared by Warwick with the SU after enrolment for the purpose of enabling the SU to administer student membership. Legal bases for sharing: Explicit consent of the students is collected when they go through the enrolment process each academic year. Method for sharing: The data is read directly from SITS — it is pulled through a direct connection on a daily basis. Type of personal data: Full name, Student ID, date of birth, Warwick email address, home and term time address, course details, fee status, equality and diversity data2. <u>Staff ID cards</u> Background: The SU operates on Warwick property and as such the SU provides Warwick with SU staff details if the staff member requires a staff card. The below information is then passed from the SU to Warwick so that it can produce staff ID cards. Legal bases for sharing: necessary for the performance of a contract/Consent Method for sharing: Email Type of personal data: Full name, email, DOB, start date and end date3. <u>Staff Car parking permits</u> Background: SU operates on Warwick property and as such if SU staff wish to park in one of the car parks they need to register on the Warwick staff car parking portal to receive staff car parking rates. SU collect all details for the

access and provide it to the Warwick so they can add permissions for SU staff to register.

Legal bases for sharing: Necessary for the performance of a contract/Consent

Method for sharing: Email

Type of personal data: Full name, Email address

4. **Warwick infrastructure services to SU**

Background: SU staff data is shared with Warwick to provide specific services such as, but not limited to, records backup, monitoring and security logging and access to the Warwick wifi

Legal Basis for Sharing: Necessary for the performance of a contract

Method of sharing: electronic transfer

Types of personal data: all data held by the SU

5. **CCTV**

Background: Both Parties operate their own CCTV systems. Footage may be shared for the purposes of undertaking an investigation, assisting with a criminal investigation, or for the wellbeing and safeguarding of a member of the University community.

Legal bases for sharing: Legal obligation / Legitimate interests /necessary for the performance of a contract/ vital interests

Method for sharing: Viewing footage and if useful footage is burnt to CD.

Type of personal data: CCTV footage

6. **Security incident reports**

Background: Warwick's Community Safety team operates a system called iTrak. Incident reports are inputted into the iTrak system which, once submitted, generates an email, detailing the information in the report. If the incident involves the SU (e.g. naming the SU's staff, takes place on the SU's premises or involves an SU club or society) an email will also be sent to the most appropriate staff member at the SU to deal with the incident.

Legal bases for sharing: Legal obligation / Legitimate interests /necessary for the performance of a contract/ vital interests/task in the public interest

Method for sharing: Email

Type of personal data: Anything written within the report — ranging from full name or initials of all involved in incident including witnesses and staff who helped to manage incident e.g. RCT/Community Safety, student/staff ID number, description of incident, medical / health data, address and contact details

7. **Sports club membership passes**

Background: Students purchase club membership with the SU. As part of that, they are required to also purchase a club pass to enable them to access Warwick facilities. The SU share that data with Warwick (Warwick Sport) for the purposes of administrating Club Sports passes so that they can have access to Warwick sporting facilities.

Legal bases for sharing: Necessary for the performance of a contract, legitimate interest

Method for sharing: Gladstone (Warwick system) to MSL (the SU system) query

Type of personal data: Full name, student University ID number, type of club membership purchased, name of club(s) joined, equality and Diversity data

8. **Sports club coaches**

Background: Clubs and societies may have third party coaches who are third party contractors of the SU. The SU will share with Warwick (Warwick Sport) for the purposes of enabling the coaches to have access to Warwick sporting facilities to provide coaching.

Legal bases for sharing: Necessary for the performance of a contract

Method for sharing: Excel spreadsheet contained within email

Type of personal data: Full name, contact number, date of birth, club they are a coach for, photo

9. Student discipline committee members

Background: Warwick may convene a disciplinary committee to investigate any major disciplinary offence under Regulation 23 — Student Disciplinary Offences. Documentation (which contains personal data) is shared with two Sabbatical officers at the SU who sit on the panel of the Disciplinary Committee. If the outcome is appealed and an appeal granted, an appeal panel is convened consisting of two different Sabbatical officers from those involved in the first panel.

Legal bases for sharing: Necessary for the performance of a contract / public task

Method for sharing: Files.Warwick

Type of personal data: Full name(s) and Student University ID number of student(s) and others involved in the disciplinary; Medical / health data, relevant to the disciplinary and / or disclosed by the individual student for the purposes of the disciplinary; Contact details of student(s) and others involved in the disciplinary/complaint; Nature and details of the incident that has given rise to the disciplinary/complaint including any supporting documentation, investigation reports, interviews, statements, CCTV footage or other relevant documents or evidence; Outcome of disciplinary investigation and appeal

10. Disciplinary investigation and complaints

Background: Warwick and the SU may need to conduct parallel investigations, or determine who should take the lead in investigating when both parties have received complaints, if the SU requests it is escalated to Warwick, or if the reporter/respondent is a student and works for Warwick. Recommendations/outcomes of Warwick investigations may include sanctions and recommendations for the SU to consider, which effect the students SU membership. In any of these scenarios, information will need to be shared between the parties. This is primarily for the benefit of the students involved (reporters as well as respondents) so that they are not put through the same/similar processes twice, and/or to ensure the most appropriate body is dealing with the investigation. As such, both parties may hold information pertinent to an investigation which may need to be passed over to the other party to uphold and enforce policies and procedures of both organisations and take any necessary further actions. Where the Student Discipline Committee has made recommendation(s) to the SU, the recommendation(s) and rationale to support them where appropriate will be shared with the SU.

Legal bases for sharing: Explicit consent, necessary for the performance of a contract, public task, legitimate interests, necessary for reasons of substantial public interest.

Method for sharing: Verbal and email

Type of personal data: Full name(s) and University ID(s) of student(s) and others involved in the disciplinary/complaint; contact details of student(s) and others involved in the disciplinary/complaint; nature and details of the incident that has given rise to the disciplinary/complaint including any supporting documentation, investigation reports, interviews, statements, CCTV footage or other relevant documents or evidence; Outcome of the disciplinary investigation/complaint and rationale to support this where appropriate; Minutes (redacted if required) from Disciplinary Committee hearings; recommendations made to SU about the student(s)

11. Disciplinary outcomes that effect SU membership

Background: Where there is a PWD or TWD sanction then the Governance Team will inform the SU. This will be communicated to the student concerned in the outcome letter. Each term Warwick will update the SU on the names of students who, in relation to disciplinary activity, have completed their sanctions and are again eligible for membership of clubs and societies.

Legal bases for sharing: Necessary for the performance of a contract, legitimate interests.

Method: Email

Type of personal data: Full name(s) and University ID(s) of student(s), date from and to of the temporary withdrawal as a disciplinary sanction, date of the permanent withdrawal as a disciplinary sanction

12. External speakers

Background: Club and Societies host events with external speakers. They submit an external speaker's form: External Speaker Events - the information within which is submitted to a single shared resource account. A risk assessment may be conducted and if the event is deemed high risk - both organisations will conduct and share their own risk assessments.

Legal bases for sharing: Legal obligation, Legitimate interests.

Method for sharing: Sitebuilder form electronic submission to email resource accounts.

Type of personal data: (a) Organiser details: Full name, Status — student or staff, Society or department, Details regarding event — time, date, location (on or off campus), title of event, expected number of attendees, how and where has the event been advertised, who will be able to attend, press invited, short description of content. (b) Guest speaker details: Full name and any stage names, Organisation, Details of what will be discussed at event, Details if the speaker has been invited to speak at other HE/FE institutions and/or Warwick in the past?, subject of the speech, language of the speech, Any past controversy surrounding the speaker or topic, Materials to be distributed, Link to speaker's website/written material, Link to research conducted by Warwick and SU into speakers, Special requirements for speakers, Details of people accompanying the speaker, Sponsor of event (c) Risk assessment by SU and Warwick: all of the data noted above plus anything available on the internet or social media that indicates where they may have spoken before, what if any issues arose, any controversy and then arrangements for the event to mitigate any risks identified.

13. Contractors

Background: There is a landlord tenant relationship between Warwick and SU. As such any work SU require to be carried out is coordinated through Warwick estates department. The estates department will book contractors who will be provided with SU contact details to liaise with them directly. Alternatively, SU may seek their own contractors and pass these details to the Warwick estates department.

Legal bases for sharing: Necessary for the performance of a contract

Method for sharing: Email

Type of personal data: Contractors contact details, SU staff contact details

14. Conference clients

Background: A client of Warwick Conference may request to book SU facilities. Warwick Conference will provide a quote to the client but then will pass over the client's contact details to SU so that the client can speak directly to SU about the finer details. All data could apply to client (organiser), speakers/trainers and delegates/guests

Legal bases for sharing: Necessary for the performance of a contract

Method for sharing: Email/booking form

Type of personal data: Full name and email address, telephone number, dietary requirements, disability access, gender, age

15. Health and safety accident reporting

Background: Warwick operate an online reporting system, recording any accident that might have occurred on Warwick premises. This is because a duty of care is owed to all students, staff and visitors. SU might be aware of an accident and therefore will notify Warwick by completing the online reporting form. Students involved in SU clubs or societies may also

complete the online reporting form and the system will generate an email to inform the SU of any incidents relevant to them.

Legal bases for sharing: Legal obligation

Method for sharing: Online reporting form via SHE software which creates an email notification.

Type of personal data: Reporter's full name, department and contact details, Incident details and action taken (including first aid), Affected persons full name, department, age range and contact details, Names and contact details of witnesses, Any attached documentation

16. Health and safety committee

Background: Warwick Director of Health and Safety attends SU Health and Safety committee meetings and has access to SU health and safety committee papers which will contain pseudonymised data regarding accidents.

Legal bases for sharing: Legal obligation / legitimate interests

Method for sharing: Email

Type of personal data: Summary of accidents/incidents — no names but details are given so potential to identify.

17. Wellbeing

Background: SU and Warwick may need to share information to support any matters relating to safety and wellbeing to ensure a safe and secure environment for all students, staff and visitors. Information arising from a safeguarding, welfare, complaint or disciplinary matter might be shared between the two parties to ensure that internal policies and procedures for risk, safety and welfare can be followed.

Legal bases for sharing: Vital interests, legal obligation, legitimate interests, Necessary for reasons of substantial public interest.

Method for sharing: Verbal conversations between SU and any of the following: Wellbeing & Student Support Services, Community Safety, Residential Community Team, Complaints Team, Disciplinary, Human Resources and the Executive team.

Type of personal data: Some or all of the below information may be shared: Full name, University ID number, Details of incident which led to Whether the student is known to be engaged with Wellbeing & Student Support Services.

18. HEAR Report

Background: The Higher Education Achievement Report (HEAR) is an electronic document detailing undergraduate students' achievements whilst at university, including volunteering, prizes awarded, positions of responsibility, module marks and the degree classification awarded. SU share achievement data with Warwick to populate student HEAR reports.

Legal bases for sharing: Consent, legitimate interests.

Method for sharing: Excel spreadsheet

Type of personal data: Full name, University ID number, Details of achievements obtained via SU — e.g. trustee, officer or exec positions

19. Major incidents

Background: Warwick has a Major Incident Plan and Major Incident Team who are concerned with supporting the University's response to a major incident. The purpose of the Major Incident Plan and Team is to: minimise loss, damage and harm, either to staff, students, visitors or members of the public; to minimise damage and loss to the University's estate and infrastructure; to communicate effectively both internally and externally; and to mitigate any potential reputational damage that may follow a major incident. The Chief Executive of SU is a member of the Major Incident Team (Silver) and as such personal data may be shared between the two organisations during a major incident.

Legal bases for sharing: Legal obligation, Legitimate interests, Vital interests.

Method for sharing: Verbal / Email / Committee papers

Type of personal data: Hard to specify as would depend on the incident but could range from names, contact details, circumstances affecting individuals in relation to the incident.

20. Development and alumni engagement

Background: The Development and Alumni Engagement department requests data about student's positions of responsibility and participation in sports (Captains and Colours) to understanding how best to engage with these students after they graduate.

Legal bases for sharing: Consent, legitimate interests.

Method for sharing: Email/spreadsheet

Type of personal data: Full name; University ID number; Details of achievements obtained via SU — e.g. trustee, officer or exec positions, sports clubs and societies

The categories of Data Subjects

- 1. Student personal data** – all students who enrolled through Warwick enrolment process and actively explicitly consented to the sharing of their personal data with the SU.
- 2. Staff personal data** — SU staff data which needs to be shared with Warwick to provide specific services/access.
- 3. CCTV footage and Community Safety**— potentially any individual captured on either Warwick or SU CCTV systems — this could include students, staff of both organisations and any external visitors.
- 4. Sports Clubs memberships and facility access** — any students who are members of sports clubs or their coaches (external third parties) who require Warwick sports facility access.
- 5. Disciplinary and complaints** — any student who engages with the disciplinary process.
- 6. External Speakers** — any student who submits the external speaker form on behalf of a club or society and the details of any external speakers.
- 7. Contractors** - external contractors engaged to do work on behalf on SU but within Warwick facilities or SU staff.
- 8. Conference Clients** — internal Warwick staff client or external clients — i.e. external businesses/members of the public.
- 9. Health and safety**— students, staff and members of the public.
- 10. Wellbeing** — any student or third party.
- 11. HEAR Report** — any student who engages with SU.
- 12. Major incident team** - students, staff and members of the public
- 13. Development and Alumni Engagement** – graduates

APPENDIX 2

NOTIFICATION PROCEDURE TO THE CONTROLLER IN THE EVENT OF A DATA BREACH OR SECURITY INCIDENT

1. The SU must contact the Data Protection Officer at Warwick at:

DPO@warwick.ac.uk

or by completing the data breach report form on Warwick's website.

2. Warwick must contact the Data Protection Officer at the SU at:

dataprotection@warwicksu.com

3. Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
4. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
5. Describe the likely consequences of the personal data breach;
6. Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects; and
7. Where it is not possible to provide all the information at the same time, the information should be provided in phases as and when it becomes available, without undue further delay.