RISK AND CONTROL MATRIX

The General Data Protection Regulation, Article 5, sets out six principles which outlines the main data protection responsibilities for organisations. This risk/control matrix identifies which processing activity is most at risk from non-compliance from which principle and what control measures are used to ensure compliance and demonstrate accountability. Each risk has been scored for the likelihood of it happening (1 being unlikely and 5 being highly likely). The impact to the university should a breach of the principles occur has also been scored (where 1 is the lowest score and 5 the highest). When the likelihood and the impact scores are multiplied this gives an overall risk score, >15 presents a high risk to the university, between 9- 15 is considered a medium risk and <9 a low risk.

The six principles are:

Article 5 –

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
(b) Collected for a specific, 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 considered to be incompatible with the initial purpose;
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
(d) Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
(e) Kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the personal data are 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 appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals;
(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Processing activity	Principle where significant risk may present	Likelihood	Impact	Risk score (Likelihood x impact)	Control measures to reduce or remove risk
Student personal data collected and processed for the purpose of processing applications and providing higher education	(a) Processed lawfully, fairly and in a transparent manner in relation to individuals	5	5	25	student enrolment and data collection points have links to privacy statements which are available on line
	(e) Kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the personal data are 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 appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals	5	2	10	The university's master retention schedule provides guidance to staff regarding data retention periods
	(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	5	5	25	The university has provided staff with data protection training. In addition it has data protection and IT usage policies in place ensuring staff understand their responsibilities. The university IT department provide IT protection and backup systems.
Student special category data necessary to comply	(f) Processed in a manner that ensures appropriate security of the personal data, including protection against	1	5	5	The university has provided staff with data protection training. In addition it has data protection and IT usage policies in place

with equality legislation	unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.				ensuring staff understand their responsibilities. The university IT department provide IT protection and backup systems.
Processing student personal data for the purpose of providing additional services i.e. accommodation	(a) Processed lawfully, fairly and in a transparent manner in relation to individuals	2	3	6	At the point of collection for this data there are links to accommodation specific privacy notices available on line. Staff have completed data protection training
	(e) Kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the personal data are 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 appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals	5	2	10	The university's master retention schedule provides guidance to staff regarding data retention periods
Processing student personal and special category data for the purpose of providing educational support, counselling and wellbeing services	(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	1	5	5	The data has restricted access and only available to necessary staff. The university has provided staff with data protection training. In addition it has data protection and IT usage policies in place ensuring staff understand their responsibilities. The university IT department provide IT protection and backup systems.
Staff personal data processed for recruitment and	(a) Processed lawfully, fairly and in a transparent manner in relation to individuals	1	5	5	Access is restricted to necessary staff only. Staff have received data protection training and at

employment purposes					the point of collection for the data links are provided to privacy notices.
	(d) Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay	5	2	10	H.R. circulate a form to all staff on an annual basis to allow staff to update their personal data.
Staff special category data necessary to comply with equality legislation	(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	1	5	5	The data has restricted access and only available to necessary staff. The university has provided staff with data protection training. In addition it has data protection and IT usage policies in place ensuring staff understand their responsibilities. The university IT department provide IT protection and backup systems
Processing personal data for the purposes of conducting research	(a) Processed lawfully, fairly and in a transparent manner in relation to individuals	3	5	15	Access is restricted to necessary staff only. Staff have received data protection training and at the point of collection for the data links are provided to privacy notices. The university has available to staff research ethics policy.
	(b) Collected for a specific, 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 considered to be incompatible with the initial purpose	2	2	4	Staff have received data protection training. In addition to data protection policies the university also has research ethics policies and a research approval process
Processing personal data for procurement of	(a) Processed lawfully, fairly and in a transparent manner in relation to individuals	2	2	4	Access is restricted to necessary staff only. Staff have received data protection training and at

services and products require for normal business operations					the point of collection for the data links are provided to privacy notices.
Processing personal data for marketing purposes	(a) Processed lawfully, fairly and in a transparent manner in relation to individuals	5	5	25	Access is restricted to necessary staff only. Staff have received data protection training and at the point of collection for the data links are provided to privacy notices. The university has cookie consent acceptance flags on its webpages where cookies are used.
	(b) Collected for a specific, 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 considered to be incompatible with the initial purpose	5	5	25	The university has introduced an updated consent form and briefed staff working in these areas accordingly.
	(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	5	5	25	The data has restricted access and only available to necessary staff. The university has provided staff with data protection training. In addition it has data protection and IT usage policies in place ensuring staff understand their responsibilities. The university IT department provide IT
Processing personal data for commercial operations carried out by the university	(a) Processed lawfully, fairly and in a transparent manner in relation to individuals	2	2	4	Access is restricted to necessary staff only. Staff have received data protection training and at the point of collection for the data links are provided to privacy notices.

Use of CCTV equipment for security, safety and crime prevention/detection	(a) Processed lawfully, fairly and in a transparent manner in relation to individuals	2	4	8	Access is restricted to necessary staff only. Staff have received data protection training. Appropriate signage is displayed in the areas covered by CCTV
Processing personal data for the purpose of maintaining Alumni relations	(a) Processed lawfully, fairly and in a transparent manner in relation to individuals	4	5	20	Access is restricted to necessary staff only. Staff have received data protection training and at the point of collection for the data links are provided to privacy notices.
	(b) Collected for a specific, 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 considered to be incompatible with the initial purpose	5	5	25	Staff have received data protection training. In addition to data protection policies. Privacy notices available on the university web page and unsubscribe options are offered in all communications.