Harm Identification Table – Level of Harm

Risk of Harm	Low/Negligible	Medium	High	Extreme
Types of information	Publically available information	Name and gender	Contact details including UNE Employee number, email addresses of students or staff not already in the public domain.	Address information, Next of Kin/Emergency contact information, Health information, TFNs, Identity documents, passports, Medicare details, contact details of vulnerable people, contact information disclosing individuals who accessed a service or event which may expose them to public embarrassment or ridicule e.g. sexual health services.
Identity apparent or ascertainable	Yes but publically available or statistical information or not information has not been de-identified to the requisite standard.	Yes, but limited personal information	Yes	Yes detailed or relating to a vulnerable person or group.
How long has the information been accessible?	Investigation determined no breach due to information types.	Uncovered immediately or shortly after breach.	Access to information for a short term or access logs confirm limited exposure.	Long term or unknown
Health or sensitive information?	No	No	No	Yes or highly detailed information e.g. the information exposed individuals accessing mental health services, or treatment for sensitive health issues.
Source	Advertising material, paper files	Paper files, limited spreadsheet	Systems with limited access and information, spreadsheets with limited information, attendance lists	Major UNE system, USB with research data, hard copy sensitive information, health care database, and contact details related to a victim of domestic abuse, disclosure of attendance related to particular activity, which exposes sensitive information such as sexual orientation or trade union membership.
Individual context which may make harm more likely	No	No	Individuals with circumstances which may mean exposure is more harmful.	Yes e.g. domestic violence victims, individuals in witness protection, those involved in family court matters

Risk of Harm	Low/Negligible	Medium	High	Extreme
Severity and scale	Large scale but no personal information	Small scale limited personal details.	Medium scale breach. A few people with a medium amount of personal information or many individuals with low levels of personal information	Large-scale breach or small number with extensive sensitive details or belonging to a vulnerable population or a high-risk individual.
What could the information be used for/ potential harm	No impact	Insignificant - minimal impact on individual	Spam or unwanted marketing, nuisance emails, minor embarrassment, minor inconvenience, short term harm	Harm to individuals such as: • Financial fraud including unauthorised credit card transactions or credit fraud; • Identity theft causing financial loss or emotional and psychological harm; • Family violence; • Physical harm or intimidation; • loss of business or employment opportunities; • humiliation, damage to reputation or relationships; or • workplace or social bullying or marginalisation.
Is the personal information encrypted, anonymised, or otherwise not easily accessible?	Yes anonymised to a high standard.	Maybe or limited information	Encrypted or remote deletion possible or ability to determine no access has occurred.	Little to no protections or all access restrictions overcome.
Mitigation strategies	Not required	Mitigation reduced the effects on individuals to merely inconvenience.	Mitigation strategies were able to prevent or reverse any potential for high-level harm.	Mitigation was unsuccessful or ineffective.

Personal/Health/Sensitive Information Risk Categories =

Type of Information (Personal, Sensitive, Health)	Impacts a few individuals (less than 5)	Impacts small group	Affects all staff or whole student body	Entire UNE community/ general public
Highly sensitive/very high impact: Tax File Numbers, financial information, health information, Union membership, sensitive personal information e.g. sexual preferences	**High**	**Extreme**	**Extreme**	**Extreme**
Multiple fields of lower level sensitivity which can be used to create a detailed profile: For example name, D.O.B, contact information, unit and course enrolment, gender, home address.	**Medium**	**High**	**High**	**High**
Limited Personal Information: Name or student number (isolated personal information fields), internal identifiers	**Low**	**Low**	**Medium**	**Medium**
Publically available information	**Very Low**	**Very Low**	**Very Low**	**Very Low**

Harm Action Table Harm = Risk + Harm ratings

		Chance of Harm				
		Rare	**Unlikely**	**Possible or likely & probable harm which is Mitigated**	**Likely**	**Probable**
Level of Harm	**Extreme**	SIMT/Privacy Officer – Report to DG and SET within 6 months	SIMT/Privacy Officer – Report to DG and Set within 3 months	SIMT/ Privacy Officer – Report to DG and Set within 3 months	DBMT - Report to Set and Council within 1 month notifiy VC immediately	DBMT - Report to Set and Council within 1 month notifiy VC immediately
	High	SIMT/ Privacy Officer – Report to DG and Set within 6 months	SIMT/Privacy Officer – Report to DG and Set within 6 months	SIMT/Privacy Officer – Report to DG and Set within 3 months	SIMT/Privacy Officer – Report to DG and Set within 3 months	DBMT - Report to Set and Council within 1 month notifiy VC immediately
	Medium	Privacy Officer/IT Security	SIMT/Privacy Officer – Report to DG and Set within 6 months	SIMT/Privacy Officer – Report to DG and Set within 6 months	SIMT/Privacy Officer – Report to DG and Set within 3 months	SIMT/Privacy Officer – Report to DG and Set within 3 months
	Low/Negligible	Privacy Officer/IT Security	Privacy Officer/IT Security	Privacy Officer/ IT Security	SIMT/Privacy Officer Report to DG and Set within 6 months	SIMT/Privacy Officer Report to DG and Set within 6 months

Where breaches do not include technology the Privacy Officer in collaboration with expert colleagues (as required), will replace all mention of SIMT.

The phrase '**likely'** means the risk of serious harm to an individual is more probable than not (rather than possible). **Probable** means almost certain.

Assessment of harm is based upon:

- The nature, sensitivity and volume of personal information involved in the data breach;
- The circumstances of the data breach, including its cause and extent;
- The nature of the potential harm to the affected individuals

Internal notification or reporting is based on a combination of harm and the personal information risk rating and managed on an iterative basis for each data breach. Notification to external bodies such as the NSW Information and Privacy Commissioner and Office of the Australian Information Commission will occur when the secondary harm assessment remains high or extreme and is likely to occur for medium harm assessments. Secondary assessments should indicate when harm is mitigated.