Appendix 3 **Incident Assessment**

	Incidents at this level are reportable to line management		Incidents at this level should follow the Critical Incident Process and be notified to the Risk Manager who will evaluate impact on the Strategic Risk Register		
Incident Source	**Low**	**Moderate**	**High**	**Severe**	**Extreme**
ICT Operations	Incident leading to brief downtime of essential systems	Loss of essential systems 0.5-1 day	Loss of essential systems 1-3 working days	Loss of essential systems 3-5 working days	Loss of essential systems 5> working days
ICT Security *(refer also to Management of Information Security Policy; Information Security Incident Reporting Procedure*)	Password 'sharing', Unattended, unlocked PCs	Unauthorised access to restricted systems / data, Loss of portable media (e.g. USB flash drives)	Unauthorised access to / compromise of very sensitive data or inappropriate use leading to compromise Loss of portable media containing sensitive information	Theft of systems / data / hardware	Malicious software (Malware) attacks e.g. viruses, spyware, key-logger programs etc. leading to major compromise of system integrity
Information Governance	Accidental release or loss	Accidental release or loss	Disclosure or loss of sensitive	Malicious disclosure or	Unauthorised disclosure

and Security *(refer also to DP Breach Procedure, role of IMLOs; Information Security Incident Reporting Procedure)*	of personal data (e.g. names addresses, correspondence)	of sensitive personal data	or personal data	accidental loss of highly sensitive information with potential to cause harm	leading to harm to individuals
Facilities Security	Loss of id badge	Attempt by unauthorised person(s) to access facilities	Unauthorised access to restricted areas	Theft of assets	Major theft / fraud or misappropriation of assets
Facilities Operations	Brief compromise of facilities availability (e.g false fire alarm)	Loss of power supply or key facilities through fire / flood <1 day	Loss of power supply or key facilities 1-3 days	Loss of power supply or key facilities 3-5 days	Loss of key facilities 5>days
Violence / Abuse *(refer also to H&S incident reporting procedure)*	Swearing / shouting	Aggressive or intimidating language or gestures	Threatening behaviour directed to employees or members of the public during the performance of Council business	Harm (physical or psychological) to employee(s) / members of the public	Death or serious injury
Health and Safety	For Health and Safety related incidents generally, refer to Health, Safety and Wellbeing Team, YourHR and associated procedures.				

Notes:

Assessment of Impacts

To rate incidents as ‘severe’ or ‘extreme’, the impact, or potential impact must meet one or more of the following criteria:

- Does the incident have the potential to cause harm to an individual or communities?
- Does the incident have the potential to significantly and negatively impact the Council’s reputation?
- Is the Council at risk of prosecution?
- Will the Council be unable to carry on normal operations for a defined or undefined period?
- Will the Council be unable to provide essential services?

Near Misses Reporting Protocol

‘Near Miss’ is a term which refers to incidents which have been prevented or avoided, usually as a result of intervention following the emergence of a danger or threat. Although the impact of a near miss is necessarily lower than that of an actual incident, the intelligence gleaned from near misses can also influence the management of risk. Near misses will generally be identified in the areas of Health and Safety, and security around information, facilities and ICT. It is important that all employees becoming aware of a near miss report the matter to their line manager. Managers should determine whether the scale of the near miss is such that it needs to be reported as a Critical Incident so that lessons may be learned and appropriate system improvements made. It is also the case that records of incidents and near misses, even where they have not followed the Critical Incident process, will be analysed in order to identify trends and patterns which may be then be reported to senior management through performance dashboards.