Information Breach – When to Report to the ICO			
Criteria	**Severity**		
Type of breach	Data is lost and cannot be recovered Loss of encrypted media/digital devices	Verbal unauthorised disclosure Email, fax or paper document sent to incorrect recipients Unauthorised copying and removal Information lost in transit	Cyber incident Data is lost and unrecoverable for a major system e.g. Athena Written unauthorised disclosure Loss of unencrypted media/digital devices Unauthorised access
Type of data	Personal data Subject matter or nature of the event already in the public domain. Name Address	Special category personal data Race Ethnic Origin Religion Politics Trade union membership Intel Safeguarding	Highly sensitive special category personal data and criminal offence & conviction data. Medical data Identity documents Financial data Biometric data Arrest data Offence data A combination of several types of data CHIS Witness protection Intel Handling code 4-5
Volume of data	One file	Few files Several files that contain very little personal data	Several files One or few file(s) that contain highly sensitive material. E.g. PVP, sex offenders etc.
Ease of identification of individuals	Individuals cannot be identified by the data. Anonymised data	If the data was matched with other data sets the individual could be identified. Pseudonymised data	Individuals can be identified from the data.

Data Protection Reform

General Data Protection Regulation (GDPR)

Data Protection Act 2018

Information Breach – When to Report to the ICO			
Criteria	**Severity**		
Consequences on the individual	Little to no risk to an individuals' rights and freedoms	Medium risk to the rights and freedoms of the individual.	High risk to the rights and freedoms of the individual. Fraud Physical harm Psychological distress Damage to reputation Large financial losses Discrimination
Number of affected individuals	one	Few One individual who could be considered vulnerable.	Many One individual who is vulnerable
Characteristics of the individual	Professionals e.g. emergency services, solicitors, social workers etc.	Members of the public who are not considered as vulnerable	Vulnerable children & adults
Is it a trusted recipient?	The information has gone to a trusted recipient who deals with the type of data often. We have a working relationship with the individuals/organisation on a regular basis.	The information has gone to a trusted recipient but they do not deal with the type of data. We have a working relationship with the individuals/organisation on an ad hoc basis.	The information has not gone to a trusted recipient. We do not have a working relationship with the individuals/organisation.
Can the breach be mitigated?	The breach can be mitigated fairly easily.	The breach can be mitigated but there is residual risk still left.	The breach cannot be mitigated. The breach can be mitigated but the original risk to the individual without mitigation is high.

Data Protection Reform

General Data Protection Regulation (GDPR)

Data Protection Act 2018

Information Breach – When to Report to the Individual			
Criteria	**Severity**		
Nature & content of the personal data concerned	Personal data Subject matter or nature of the event already in the public domain. Name Address	Special category personal data Race Ethnic Origin Religion Politics Trade union membership	Special category and criminal conviction data Financial information Location data Internet log files Web browsing history Email data Itemised call lists
Consequences of the breach	Little to no risk to an individuals' rights and freedoms	Medium risk to the rights and freedoms of the individual.	High risk to the rights and freedoms of the individual. Identity theft Fraud Physical harm Psychological distress Humiliation Damage to reputation
Circumstances of the breach	Data is lost but not in possession of an unauthorised third party	Data is likely to be in possession of an unauthorised third party	Data is in possession of an unauthorised third party