Appendix A – Security Classification [ISO/IEC27001:2013 8.2.1]

NHS Shetland has adopted the NHSS Green, Amber, Red classification of information:

eHealth Guidance	NHS Shetland Examples	Equivalent UK Government Security Classification
GREEN: Unclassified information This is information which is unlikely to cause distress to individuals, breach confidence, or cause any financial or other harm to the organisation if lost or disclosed to unintended recipients. This can include information which mentions only a person's name (e.g. routine appointment confirmation letter) **as long as it does not contain anything that is judged to describe a person's physical or mental state.**	Most NHS Shetland corporate documents fall within this category, including: • Names, posts of employees • Most management correspondence and minutes • Work contact details	**OFFICIAL**
AMBER: Protected information In most boards the largest proportion of patient information can be said to require extra protection because it is defined as 'special category data' by the Data Protection Act. In particular: • Any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost • Any information which if lost or disclosed to unintended recipients would lead to a low risk to a person's safety (e .g. loss of an address but no evidence to suggest direct harm would result). • Any information if lost that would be likely to negatively affect the efficiency of that service (e.g. cancellation of appointments).	• Patient medical details or the performance or health of individual colleagues • Commercially sensitive procurement information during the tendering process • Home contact details • Sensitive management discussion	**OFFICIAL**

eHealth Guidance	NHS Shetland Examples	Equivalent UK Government Security Classification
RED: Highly sensitive information Most boards also hold some information which is highly sensitive. In particular: • Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way). • Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person's sexual health. • Information that affects the privacy or could cause distress to more than one individual (e.g. several family members or several linked persons contained in a file). Information relating to vulnerable persons' health (e.g. child protection cases). • Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment). • Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc.	• Highly sensitive patient medical information or staff equality & diversity information identifying individuals, particularly sexual orientation • Serious allegations against individual staff • Banking or credit card details of individuals	***OFFICIAL – SENSITIVE PERSONAL**

* When communicating with UK or Scottish Government agencies, local authorities or the Police, Red data must be labelled as:

OFFICIAL – SENSITIVE PERSONAL. [ISO/IEC27001:2013 8.22]