Appendix 1 - Scottish Government Mobile Data Standard (CEL 25, 2012)

Email Handling Guidelines

The following classification scheme for information has been derived from the Mobile Data Protection Standard (CEL 25,2012) first issued in 2008, which has now been revised and takes into account the rapid adoption by Boards of new types of device, such as tablets, smart phones and digital pens, for a variety of purposes.

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. 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.

Note: The sensitivity level and impact can also vary depending on the volumes (e.g. a corporate document with just one name of an employee may be unclassified whereas a document with hundreds of names may push it into the amber category below).

Control for protecting 'Unclassified' (Green) Information sent by email

Action	Technical/Non Technical security requirements
Sending By Public Network (inc. Email)	Limited on a need to know basis

AMBER: Protected Information

In NHS Fife the largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined 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 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).

Control for protecting 'Protected' (Amber) Information Sent by Email

Action	Technical/Non Technical security requirements
Sending By Public Network (inc. Email)	Allowed; only to be sent by secured

	methods and to secure recipients as per the GP/E6 Email policy.

RED: Highly Sensitive Information

NHS Fife holds information which is highly sensitive. Particularly:

- 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 individuals (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.

Control for protecting 'Highly Sensitive' (Red) Information Sent by Email

Action	**Technical/Non Technical security requirements**
Sending By Public Network (inc. Email)	Allowed; only to be sent by secured methods and to secure recipients as per the GP/E6 Email policy.