

## **CPP1.1 Information policy:**

### **6. Data and Document security: classification, disclosure and disposal**

#### **1. Introduction**

1.1 Passenger Focus deals with much sensitive information and it needs to ensure that all such information is treated in a secure manner. This protects both individuals and the nature of the work carried out, which is often of a sensitive nature itself. **This policy applies to both written and electronic information.**

1.2 The overall policy objective is to be open with information internally; the fact is however, that certain information cannot be generally available because if it was it may cause harm or embarrassment to individuals within or without Passenger Focus or damage to reputation. In extreme cases, certain views, forcibly expressed, may even be actionable if they became public knowledge – to protect our ability to express what we think, safeguards must be available where we need them. It is for this reason that this policy exists. All staff should ensure they understand it and apply it; they should speak to their manager at once if there are aspects of it they do not understand.

1.3 Although this policy applies primarily to staff, it should be noted that documents classified higher than OFFICIAL may often be sent to Board Members. In this respect, Members are not to be regarded as 'external' but 'internal' recipients.

1.4 The policy sets a framework to ensure information held is protected from loss, distortion or misuse. It also forms a strategic component of the IT security framework within Passenger Focus.

1.5 This policy (as of May 2014) also provides for the Minimum Mandatory Measures established by central government during 2008-09 to provide enhanced protection for personal data. The classification SENSITIVE: PERSONAL PROTECT has its roots in these measures, and intended or accidental breach may have severe consequences. This policy has been updated to reflect the new Government Security Classifications of April 2014.

#### **2. Document Classification**

2.1 All documents are covered by this guidance, regardless of their type (letter, memo, report, briefing, newsletter etc) or format (hard, electronic, Braille etc). It is the responsibility of the originator of the document to establish its classification or otherwise.

## **“Official” Documents**

2.2 Any document (email, Word, Excel or Powerpoint, or any document created by applications such as Cascade, Connect or CRM) created by Passenger Focus is an OFFICIAL document, even if it is not labelled as such. Either way, they may be assumed to be open to anyone to read internally, but may only be passed to anyone externally if one of the following conditions is satisfied:

- (a) It was created for that purpose. Letters, emails, reports and presentations are designed for external audiences. It is still important to check however that any underlying data or supplementary information is not, or perhaps should have been, classified as higher than OFFICIAL;
- (b) the information is routinely published via the website under our publication scheme;
- (c) the information is the subject of a request made under the Freedom of Information Act 2000 and there is no reason to apply an exemption;
- (d) the information is inter-governmental and passed to an organisation who treats it with similar care;
- (e) the information is the product of a Subject Access Request under the Data Protection Act 1998 and Passenger Focus has taken reasonable steps to verify the identity of the applicant;
- (f) the information is personal information as defined by the Data Protection Act 1998 and used for lawful processing by a third party;
- (g) the information is sensitive personal information as defined by the Data Protection Act 1998 and passed to a third party only with the explicit consent of the data subject;
- (h) the information has been authorised for release by the appropriate information asset owner.

2.3 It is not our policy to put OFFICIAL on all documents that have no higher classification but they remain classified as OFFICIAL nonetheless.

2.4 It is important to check the publication scheme carefully to determine what information may be provided under it, since there are exceptions to the scheme and exemptions under the Act. It is available on [Connect](#) and also on the website.

2.5 Any document without a classification mark should be assumed to be OFFICIAL.

## **“Sensitive” documents**

2.6 Any document which requires a level of classification above OFFICIAL – ie one that requires a **restricted** circulation list and one which we would **not** want to be released under the Freedom of Information Act 2000 must be classified as OFFICIAL SENSITIVE and, along with an appropriate descriptor, must be shown at the head of the document, and in the subject field of any email to which it is attached. **No such document (or any document attached to it) must ever be blind copied to any other recipient.**

2.7 The other public sector classifications are:

- Secret
- Top Secret

As it is unlikely that the work of Passenger Focus will attract either of these classifications their use is excluded from this policy.

### *Applying higher classifications*

2.8 Managers and staff handling the information are best placed to determine what classification should be applied in each scenario. When deciding upon the level of protective marking required the originator should consider the information value in terms of the likely damage that could result from the information being disclosed to someone without the proper authorisation. Choosing the correct classification is not always easy to determine. It is best practice to over classify rather than under classify as this can always be changed at a later date, without the risk of compromising the organisation

## **‘Sensitive’ Classification for internal use**

2.9 The main classification of documents which require a limited circulation is “SENSITIVE”. If this classification is used, however, it **MUST** be accompanied by a descriptor which enables the recipient(s) at a glance to tell why such a classification has been used. There are FOUR main types of descriptor:

<b><i>Classification and Descriptor</i></b>	<b><i>When to use it</i></b>
SENSITIVE – COMMERCIAL	When the information contained in the document (or any document attached to it) is commercially sensitive between the originator and the recipient(s). This might apply, for example, when a TOC provides advance notice of fares increases or the DfT provides details of a new franchise about to be let.
SENSITIVE – POLICY	When the information contained in the document (or any document attached to it) relates to a Board policy that has not been made public. This might apply, for example, when it is in the process of developing a policy position on a proposed major change within the industry, and does not want the policy made public until it so decides.

<p>SENSITIVE – MANAGEMENT / STAFF</p>	<p>When the information contained in the document (or any document attached to it) contains management information that may have an impact on staff. There are many examples of where this classification should be used. Management Team or RemCom agendas/minutes/KIPs should be thus classified, as most meetings discuss organisational matters with such an impact. This is not to say that certain matters perhaps initially covered by this classification will never be revealed to staff. But management must be able to discuss and evaluate options and proposals in the knowledge that their deliberations are secure until they collectively choose otherwise.</p> <p>For 121 communications between manager and staff member, see below.</p>
<p>SENSITIVE – PERSONAL PROTECT</p>	<p>Any information which <b>links</b> one or more identifiable living person with information about them whose release would put them at significant risk of harm or distress.</p> <p><b>In other words,</b></p> <p>Name / addresses (home or business or both) / postcode / email / telephone numbers / driving licence number / date of birth [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]</p> <p><b>Combined with:</b></p> <p>Sensitive personal data as defined by s2 of the Data protection Act, including records relating to the criminal justice system, and group membership, DNA or finger prints / bank, financial or credit card details / mother's maiden name / National Insurance number / Tax, benefit or pension records / health records / employment record / school attendance or records / material relating to social services including child protection and housing</p>

### **‘Confidential’ classification**

2.10 The use of confidential as a document classification has two main applications, internal and external. Generally, this classification applies when documents are transmitted between an originator and one recipient, although it is possible to copy other individuals in with discretion and judgement.

2.11 **Internally**, the classification most usually applies when the document (or any document attached to it) relates to the employment related affairs of an individual. These may include, but are not limited to:

- HR to member of staff: notification of changes to terms of employment (including pay, where a copy sent to payroll would be appropriate and reasonable)
- Line manager to member of staff: performance review record, note of 121 meeting, disciplinary matter (where a copy sent to HR would be appropriate and reasonable)

2.12 **Externally**, the classification may be applied to personal letters from the Chairman and Directors to senior industry / public executives where a more open airing of the issue would be prejudicial to the desired outcome and, therefore, may be said to be against the public interest.

### **3. Time Sensitive Information**

3.1 In certain circumstances it may be desirable to apply a protective marking, which is 'time sensitive'. This is, at the time of origination, the sensitivity of the information may merit the application of a protective marking. But at some time in the relatively near future the sensitivity will no longer apply, and therefore the protective marking effectively ceases to be needed or may be downgraded.

3.2 An example may be budgetary papers marked "SENSITIVE POLICY", prior to discussion and agreement, after which it is in the public domain and is no longer sensitive so the marking isn't required. If this is the case the marking should be altered to reflect the change.

### **4. Document and data security**

4.1 All documents classified higher than OFFICIAL must be kept in locked cabinets, with reasonable security precautions taken in respect of keys. When circulating or mailing such documents, they must be placed in an envelope and have a clearly visible classified label. Classified documents sent or forwarded by email should show the classification in the subject field.

4.2 Staff tasked with opening incoming mail should not open envelopes which have a label or mark classified higher than OFFICIAL. These should be treated as 'addressee only'. Where staff are given access to another individuals email inbox, they should not open any incoming email classified higher than OFFICIAL unless they have been given specific, and written, permission to do so.

4.3 Responsibilities under 4.1 or 4.2 above are consistent with the staff handbook Part 1, Section 4 (Conduct) 1.3 (Disclosure and use of information) and breaches of this policy will be treated accordingly.

4.4 Documents, including books and publications, which are classified as OFFICIAL or not protectively marked may be left on desks, walls and notice boards.

4.5 The correct destruction of all information is vital to the classification process. All information classified higher than OFFICIAL must be disposed of by secure waste.

4.6 No document classified higher than OFFICIAL or similar data should ever be stored on a laptop/desktop hard drive or smartphone or unencrypted memory stick; they must be stored on a secure area of Connect. Responsibilities under this paragraph are consistent with the staff handbook Part 1, Section 4 (Conduct) 1.3 (Disclosure and use of information) and breaches of this policy will be treated accordingly.

4.7 Any **SENSITIVE – PERSONAL PROTECT** data transmitted to a third party (for example payroll and pension providers) must only be done with assurances that the third party has procedures in place to deal with such data on terms consistent with this policy and, if transmitted electronically, the means of the transmission is beyond doubt secure.

## 5. Disclosure

5.1 As a general rule, recipients of documents classified higher than OFFICIAL and/or data are responsible for ensuring their security, as above, provided they were received securely.

5.2 Staff who come across documents classified higher than OFFICIAL clearly not intended for them should pass them at once to either the originator or intended recipient (whichever is most practicable) immediately and without reading them.

5.3 The responsibility of any member of staff, having come across, received, or been passed, a document classified higher than OFFICIAL or SIMILAR data, to return it to the originator or intended recipient immediately, without reading it, is consistent with the staff handbook Part 1, Section 4 (Conduct) 1.3 (Disclosure and use of information) and breaches of this guidance will be treated accordingly.

5.4 The responsibility of any member of staff, having come across, received, or been passed, a document classified higher than OFFICIAL or data, not to in turn pass it onto, copy, forward or make it available to any other person, is consistent with the staff handbook Part 1, Section 4 (Conduct) 1.3 (Disclosure and use of information) and breaches of this guidance will be treated accordingly.

## 6. Specific Accountabilities

6.1 The Policy is owned by the **Senior Information Risk Owner** (SIRO) who has accountability for its implementation, compliance and monitoring. The SIRO is directly accountable to the Chief Executive / Accounting Officer and Audit & Risk Assurance Committee in this respect.

6.2 **Directors, team leaders** and **information asset owners** should note that special attention should be given to managing security aspects of any temporary staff, consultants and contractors for whom they are responsible.

6.3 **All employees** have a duty of care with respect to sharing of information and a duty to Passenger Focus to ensure sensitive information is adequately protected. To ensure we meet our legal and compliance responsibilities in this regard, employees are accountable for adequately protecting information processed during the course of their employment, in accordance with the procedures established within this policy.

REQUIRES BOARD APPROVAL

*[Approved by the Board meeting in Manchester May 2014]*