Family Support Information Security Classification

It is presumed that the majority of information assets owned, or used, by Family Support are freely available to all staff, volunteers, service users, Directors, contractors and visitors unless there is a justifiable reason to limit access to them.

Where there is a justifiable legal or business reason to limit access to information, Family Support uses two security markings:

- INTERNAL

  Examples of information assets classed as INTERNAL include unpublished business sensitive information such as financial accounts, contract details, and information security procedures. Board and Committee papers and minutes, and press releases which are subject to a publication embargo. Information marked INTERNAL is only for staff, Family Support Directors and those volunteers or contractors who need the information for their volunteering or contractual duties. It may only be made public if authorisation is given by senior management.

- CONFIDENTIAL

  Examples of CONFIDENTIAL information include service user case files, records that include address and telephone number, personal information about staff, contractors, or volunteers, information sent to us by other agencies which is marked Confidential, Restricted or Sensitive, commercial information to which access needs to be highly restricted. Assets marked CONFIDENTIAL are only made available to specified staff, Directors and contractors.

It is the responsibility of the person creating the Information asset to determine the appropriate security marking for their assets and those who have rights to access them. Requests to access information assets will be considered on a case-by-case basis by information asset owners.

Any information received by Family Support that has a security marking already in place will be treated as INTERNAL as a minimum. Final classification will be made by the appropriate information asset owner.

Protectively marking (labelling) documents

Every information asset (for instance documents and emails) will require a classification. All unmarked information assets may be assumed to be UNCLASSIFIED and therefore PUBLIC documents, suitable for anybody to access, unless it is clear from the content that the information should have been marked. Protective marking must be applied as follows:

UNCLASSIFIED – no protective marking required

INTERNAL – must have:

- The word INTERNAL in either the header or footer of every page if it is a document
- The authors name should be in the header or footer of every page if it is a document
- The word INTERNAL in the name of the file
- Every page must be numbered in the format 1 of x

CONFIDENTIAL – must have:

- The word CONFIDENTIAL in either the header or footer of every page if it is a document
- The authors name should be in the header or footer of every page if it is a document
- The word CONFIDENTIAL in the name of the file
- Every page must be numbered in the format 1 of x
- The word CONFIDENTIAL in the subject of an email

Handling of data

Information that is marked CONFIDENTIAL or INTERNAL should be handled in accordance with the following guidance unless Family Support business procedures permit otherwise:

Activity	How to handle information marked 'internal'	How to handle information marked 'confidential' (*these are in addition to the internal actions*)
Labelling	All documents should be marked with their security classification: **'internal'** or **'confidential'**, as well as author, date and page numbers in the 1 of x format.	
Storing	**Physical papers** Inside locked cabinets. All shared cabinets should be assigned an owner.	**Physical papers** Be aware of who has access.eg control who holds keys.
	Electronic documents Store on Family Support protected systems.	**Electronic documents** Password protect or restrict access to file folders to specified users.
	Voice messages and verbal communications Do not disclose in voicemail messages - request callback instead. Avoid discussing information in a place where you can be overheard.	
Destroying	**Paper documents and DVDs** Must be placed in confidential waste bins. Where the special bins are not available, use an approved shredder.	
Sending	**Fax** Call ahead, use a cover sheet, and ask recipient to acknowledge safe receipt.	**Fax** Do not use fax.

Activity	How to handle information marked 'internal'	How to handle information marked 'confidential' (*these are in addition to the internal actions*)
	Postal dispatch Suitable for normal postal service. A return address should be visible on the outside of the envelope Ensure the envelope is sealed and cannot come unstuck	**Postal dispatch** Send by Signed-For post (or normal courier if it is a package) For information where you need to track safe receipt and where the impact of unauthorised access would be very high, consider using Special Delivery or a secure courier. To protect the information from being seen by a recipient's post-room staff, double-envelope it and mark the inner envelope as Addressee only – Confidential.
	Electronic channels or equipment Can be sent by normal email service within Family Support network Include **'internal'** in subject line of email. Information should not be emailed to a non-Family Support email address except as permitted by Family Support business procedures. Only Family Support approved devices (eg encrypted memory sticks, tablets, or laptops) may	**Electronic channels or equipment** Keep the detail to the minimum necessary State **'confidential'** in the subject line of email When sending to non-Family Support email addresses: - Password protect attachments and confirm password by telephone - Do not put confidential information in the body of the email – use initials or file references to indicate who it's about (put confidential details in an attachment) - Use secure email if it is available to you.

Activity	How to handle information marked 'internal'	How to handle information marked 'confidential' (*these are in addition to the internal actions*)
	be used to take information out of Family Support premises.	
Removing **Paper files from Family Support premises**	**Physical papers** Get permission, (either on a case-by-case basis or as a regular practice) or discuss with your line manager. Carry in an opaque folder and do not look at in a public place. Do not leave unattended.	**Physical papers** Keep a record if the item is removed from the office and check it in on return. Place item(s) in a sealed envelope or folder which is marked with the return address so it can be returned if it's lost.
Disclosing	**Digital and non-digital information** When sharing with another organisation, a signed confidentiality agreement or third party information exchange agreement must be in place, or the sharing must be in accordance with an agreed procedure. See **Send** for secure procedures when sending the information externally via different channels.	**Digital and non-digital information** Must be in accordance with an agreed procedure, practice standards, or a legal requirement. Check that you are adhering to any relevant information sharing or disclosure agreements before providing the information. See **Send** for secure procedures when sending the information externally.

Activity	How to handle information marked 'internal'	How to handle information marked 'confidential' (*these are in addition to the internal actions*)
	A contract must be in place before information is disclosed to suppliers (data processors)	A contract must be in place before information is disclosed to suppliers (data processors)