DATA PROTECTION POLICY

(a) The policy

The Data Protection Act 1998 (the "Act"), which came into force in the United Kingdom on 1st March 2000, governs the use of an individual's personal details. The Company has adopted the principles of the Act as the basis for its "best practice" data protection policy set out below.

The Company regards the lawful and correct treatment of personal information as being of utmost importance. Accordingly, it is the Company's policy to comply with data protection legislation at all times, and to take extra steps to adopt "best practice" data protection procedures in relation to all of its activities. All employees of the Company are expected to comply with the policy. Failure to do so could result in disciplinary action.

(B) What is data protection?

The Act governs the collection, holding and all uses of personal data.

(C) What is personal data?

Personal data is all information concerning or relating to any living individual. This includes personal data held in electronic records and also, for the first time, in manual records (e.g. paper files, microfilm and other media). This applies to personal data held not only by the Company, but also to personal data held or processed on its behalf by third parties.

(D) The "Data Protection Principles"

The Act contains eight "Data Protection Principles", which require that personal data shall be:

- "Processed" (which means doing absolutely anything to the data, including its acquisition, holding, use, transfer, destruction etc) in a manner, which is "fair and lawful". Processing will generally be "fair and lawful" only where the individual to whom the data relates has given their consent to that type of processing, or where the processing is necessary for the performance of a contract, or else where the processing is necessary for the purposes of a legitimate interest of the Company;

- Obtained only for specified and lawful purposes, and shall not be processed in a way which is incompatible with that purpose or those purposes;

- Adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

- Accurate and kept up to date;

- Kept for no longer than necessary for the purposes for which it was collected;
- Processed in accordance with the rights of individuals under the Act;
- The subject of technical and organisational measures to prevent unauthorised or unlawful processing of personal data, and against accidental loss, destruction or damage to that personal data; and
- Not transferred outside the EEA, except in certain circumstances.

(E) What does the Act mean in practice?

The key requirements of the Act, and therefore of the Company's data protection policy, are as follows:

I. Personal data relating to any individual should never be used for a purpose to which that individual has not consented.

II. Personal data should never be disclosed to anybody who does not reasonably require the information for the purpose for which it was collected.

For example, the personal data of a customer should never be disclosed outside the Company unless the individual has specifically consented or guidance has been sought from the Data Protection Co-ordinator who is Michael Fay or his/her successor from time to time. Equally, no personal information should be disclosed to another member of the Company's staff if the reasons for that person requesting the information appear unclear or doubtful.

III. Personal data should be adequate and not excessive for the purposes for which it is processed, and it should be kept accurate and up to date.

Information held should be the minimum required for efficient operation. Requests from customers or other individuals to update personal records should be actioned immediately and cross-referred to any other databases or files containing personal data about them.

IV. Personal data should be kept for the minimum time necessary and destroyed appropriately.

All personal data should be the subject of formally agreed and documented retention periods. Check with the Data Protection Co-ordinator if you are in doubt.

V. Personal data should at all times be kept secure from unauthorised access, loss or destruction.

Not only should information held on computer be protected by sufficient security measures, but also manual records containing the personal data of any individual should be kept locked away with access strictly controlled.

VI. Personal data should not be transferred outside the EEA.

Essentially, personal data should not be transferred outside the EEA (including, for example, by such methods as e-mail and through the Intranet) unless:

- The individual to whom the data relates has given their informed consent to the transfer;
- It is being transferred to an FCS Laser Mail company which has chosen to implement a group data protection policy; or
- Appropriate contracts are in place with the non-EEA recipient (whether a member of FCS Laser Mail or not) to ensure that there will be adequate protection for the personal data.
- The reason for transfer falls within the exemptions allowed under the Act.

Always check with the Data Protection Co-ordinator.

VII. The rights of individuals established under data protection legislation must be observed.

VIII. Requests for access to or rectification of personal data by any individual should immediately be forwarded to the Data Protection Co-ordinator.

The Company should allocate responsibility for managing data protection issues to a nominated individual (the "Data Protection Co-ordinator"). All queries should be addressed in writing to the Data Protection Co-ordinator. No information should be provided to individuals without written confirmation and advice from the Data Protection Co-ordinator.

IX. Staff should familiarise themselves with their responsibilities in respect of handling personal data, see also point (G).

X. Where personal data is transferred to any party outside FCS Laser Mail, there should always be a contract in place between FCS Laser Mail and that other party to ensure that they comply with their data protection obligations.

Consult the Data Protection Co-ordinator when in doubt.

XI. Care should be taken when disposing of any personal data which, if it were to come into the wrong hands, could potentially cause embarrassment, distress or damage to the individual which it concerns.

Material containing such personal data should, when it is being discarded, be shredded or otherwise disposed of in a secure manner.

XII. The Data Protection Co-ordinator will maintain details of current personal data processing activities.

Staff undertaking new personal data processing activities are required to inform the Data Protection Co-ordinator.

IN ANY SITUATION WHERE YOU ARE IN DOUBT ABOUT ANY USE OR DISCLOSURE OF INFORMATION CONCERNING ANY INDIVIDUAL, GUIDANCE SHOULD BE SOUGHT FROM THE DATA PROTECTION CO-ORDINATOR WITHOUT DELAY.

(F) Employee information

I. The Company and/or any Group Company "processes" employee information for example, name and address, which is held for the purposes of staff administration. Processing includes obtaining, holding, editing, destroying and disclosing employee information to any Group Company and/or any third parties (for example, insurers, pension scheme trustees, banks and other employers following a business transfer or merger).

II. The Company may transfer employee information to any Group Company and/or any third parties (for example, insurers, pension scheme trustees, banks and other employers following a business transfer or merger) located inside and outside of the European Economic Area.

III. You will provide your employee information to the Company and consent to the processing of employee information (either inside or outside of the EEA) for the purposes of staff administration.

IV. The Company and/or any Group Company may monitor and/or record your use of office equipment, for example, e-mail, internet, telephones and mobile telephones for the purposes of compliance with Company procedures and policies, maintenance, security and regulatory requirements or as permitted by law.

V. If your circumstances change at any time you should inform the Data Protection Co-ordinator as soon as possible in order to ensure that all employee information remains accurate.

(G) Guidance notes on the management and use of all lists of contacts

I. The following is a guide to the management of lists of contacts held in either electronic or manual format.

II. Contact details should usually contain only business title, a business address, phone and fax number and e-mail address. If private address etc details are recorded, note on the list that these details are not to be released or used for communicating with the individual (unless the contact has given express permission for this to be allowed, or permission is clearly implied).

III. All contact details should be accurate and up to date. Review lists regularly to ensure that they are correct. Delete / shred all information about contacts where contact is not, or it is envisaged that contact will not, be maintained.

IV. Opinions and personal comments about an individual on the list should be avoided.

Do not divulge contact details to others in FCS Laser Mail unless there is a legitimate business need.