DATA PROTECTION POLICY

The Organisation needs to collect and use certain types of information about staff, clients and other individuals who come into contact with the company in order to operate. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

This personal information must be dealt with properly, however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this is within the EU General Data Protection Regulation and the Data Protection Act 2018.

We regard the lawful and correct treatment of personal information as very important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. We ensure that our Organisation treats personal information lawfully and correctly.

Most businesses hold personal data on their customers, employees and partners. The explosion in the use of the Internet, electronic communication and computerisation of business data has led to an increase in the importance of privacy. Breaches of computerised data security have prompted the introduction of legislation on a national and European level.

These include:

- Human Rights Act 1998
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 2018
- Computer Misuse Act 1990
- European Union General Data Protection Regulation 2016 (EU GDPR)

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the “rights and freedoms” of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

The top management of FCS Laser Mail are strongly committed to the rights of individuals whose data they collect and process and will comply with UK and EU laws related to personal information in- line with the EU General Data Protection Regulation (GDPR).

The top management of FCS Laser Mail ensures that it meet its requirements under EU GDPR for the management of personal information, that the objectives of FCS Laser Mail and obligations under the law are met, and ensures that controls are in place that reflect the level of risk that FCS Laser Mail is willing to accept. In addition, steps are taken to ensure that FCS Laser Mail is able to meet all the regulatory, statutory and contractual obligations that are applicable, including the protection of the interests of individuals and all other relevant stakeholders.

As a data processor, FCS Laser Mail and its Clients (Data controllers) comply with the requirements of GDPR as follows:

- Process personal information only where this is strictly necessary for legitimate organisational purposes
- Collect only the minimum personal information required for these purposes and not process excessive amounts of personal information
- Provide clear information to individuals about how their personal information will be used and who will be using the information
- Only process relevant and adequate personal information
- Process personal information fairly and lawfully
- Keep all personal information secure
- Maintain an inventory record of the type of personal information that is processed
- Ensure they keep personal information accurate and up to date
- Retain personal information only for as long as is necessary for legal or regulatory reasons or for legitimate organisational purposes
- Respect individuals' rights in relation to their personal information as defined in the GDPR
- Only apply exemptions permitted by data protection legislation
- Identify staff with specific responsibility and accountability for the ongoing maintenance and support of the requirements of the GDPR.

In addition, a separate data controller/processor agreement is in place between FCS and its client.

FCS Laser Mail has notified the Information Commissioner that it is a data controller and/or processor and that it processes personal data.

The policy applies to all Employees and Processors of FCS Laser Mail such as outsourced suppliers. Any breach of the GDPR will be considered as a breach of the disciplinary policy and could also be considered a criminal offence, potentially resulting in prosecution.

All third parties working with or for FCS Laser Mail, and who have or may have access to personal information, will be expected to comply with this policy. All third parties who require access to personal data will be required to sign a Third Party Security agreement. This agreement will ensure that the third party has the same legal obligations as FCS Laser Mail. This will also include an agreement that FCS Laser Mail can audit compliance with the agreement and forms part of our Certification to ISO27001.

GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

The location, for the purposes of GDPR, of any data controller located in the EU will be the place where the controller makes the key decisions related to the data processing purpose. This is likely to be FCS Laser Mail HQ.

Any data controller that is not located within the EU, will be required to have to appoint a representative in a location that is under the jurisdiction that applies to the data that is being used in order to act on behalf of the controller and engage with the appropriate supervisory authorities for that location.

Company Responsibilities

FCS Laser Mail is a data processor as defined under the GDPR.
Senior Management and all those in managerial or supervisory roles throughout FCS Laser Mail are responsible for developing and encouraging good information handling practices within the organisation; responsibilities are set out in individual job descriptions.

The IMS Management Representative is responsible for the management of personal information within FCS Laser Mail and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes the development and implementation of security and risk management to ensure compliance. The IMS Management Representative is responsible for ensuring that FCS Laser Mail complies with the GDPR in relation to all aspects of data processing and has direct responsibility for policy and procedures, including Subject Access Requests. This is also the person to whom all staff will go to seek guidance regarding GDPR compliance.

It should be noted that compliance with GDPR requirements remains the responsibility of all staff who process or control personal information for FCS Laser Mail. All members of staff employed by FCS Laser Mail are also responsible for ensuring that any personal data that is about them that is supplied by them to FCS Laser Mail is accurate and up-to-date.

IMS5 - Staff Training and Awareness policy defines specifically what training is required for all staff, including specific roles.

Risk Assessment in relation to GDPR

FCS Laser Mail needs to ensure that it is aware of any risks associated with the processing of all types of personal information. A Risk Assessment procedure is in place as per our ISO27001 Certification and a Risk register is maintained. A full information security risk management process is in place and results and observations are subject to an internal Management Review process along with six monthly external audits.

Principles of Data Protection

Any processing of personal data must be conducted in accordance with the following data protection principles of the Regulation, and FCS Laser Mail's policies and procedures will ensure compliance.

Personal data must be processed lawfully, fairly and transparently. The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' 'rights and freedoms.
Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must as a minimum include:

- The identity and the contact details of the controller and, if any, of the controller's representative
- The contact details of the Data Protection Officer, where applicable
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- The period for which the personal data will be stored
- The existence of the rights to request access, rectification, erasure or to object to the processing
- The categories of personal data concerned
- The recipients or categories of recipients of the personal data, where applicable

Personal data can only be collected for specified, explicit and legitimate purposes. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of FCS Laser Mail's GDPR registration.

Personal data must be adequate, relevant and limited to what is necessary for processing. A data Processor/Controller agreement is in place which sets out both parties' obligations in regards to obtaining, storing and processing data as part of the EU GDPR regulations.

The IMS Management System representative will ensure that all processes are reviewed annually by internal audit or external experts to ensure that collection continues to be adequate, relevant and not excessive. FCS Laser Mail is audited externally via SGS UK limited every six months in relation to our ongoing certification to ISO27001.

Other Considerations

Personal data must be accurate and kept up to date.
Data that is kept for a long time must be reviewed and updated as necessary. Any data that is considered to be inaccurate or likely to be inaccurate must be removed.

All individuals are responsible for ensuring that any data held by FCS Laser Mail is accurate and up-to-date. Any data submitted by an individual to a company, such as via a registration form, will be considered to be accurate at the time of receipt.

Employees or other individuals should notify FCS Laser Mail of any changes in personal information to ensure personal information is kept up to date. It is the responsibility of FCS Laser Mail to ensure that any notification of changes to personal information is implemented.

Data Security falls under our comprehensive Certification to ISO27001 for which we are externally audited by SGS UK Limited every six months.

Personal Data Considerations

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Where personal data is retained beyond the processing date, it will be encrypted in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in the Data Retention Policy.

Personal data must be processed in a manner that ensures its security.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Security controls will be subject to audit and review.

FCS Laser Mail's compliance with this principle is contained in its Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001:2013 and the Security Policy set out in the ISMS Manual.

Personal data shall not be transferred to a country or territory outside the European Union Member States unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

The transfer of personal data outside of the EU Member States is prohibited unless one or more of the specified safeguards or exceptions apply.

Safeguards

An assessment of the adequacy by the data controller taking into account the following factors:

- The nature of the information being transferred
- The country or territory of the origin, and final destination, of the information
- How the information will be used and for how long
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations
- The security measures that are to be taken as regards the data in the overseas location.

Accountability

The GDPR states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR. As a result, controllers are required to keep all necessary documentation of all processing operations, and implement appropriate security measures.

Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about the mechanics of automated decision-taking process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by automated process
- To sue for compensation if they suffer damage by any contravention of the GDPR
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data
- To request the ICO to assess whether any provision of the GDPR has been contravened
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller
- The right to object to any automated profiling without consent.

Data subjects may make data access requests as described in the Subject Access Requests procedure. This procedure also describes how FCS Laser Mail will ensure that its response to the data access request complies with the requirements of the Regulation.

Complaints

A Data Subject has the right to complain to at any time to FCS Laser Mail if they have concerns about how their information is used. If they wish to lodge a complaint this should be directed to the Data Controller, in the event that FCS Laser Mail is processing data on behalf of its clients.

A Data subject also has the option to complain directly to the Information Commissioners Office.

Consent

FCS Laser Mail understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

In addition, FCS Laser Mail understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Consent to process personal and sensitive data is obtained routinely by FCS Laser Mail using standard consent documents. This may be through a contract of employment or during induction.

Data Security

All FCS Laser Mail Staff that are responsible for any personal data which FCS Laser Mail holds must keep it securely and ensure that it is not disclosed under any conditions to any third party unless that third party has been specifically authorised by FCS Laser Mail to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- In a lockable room with controlled access; and/or
- In a locked drawer or filing cabinet; and/or
- If computerised, it must be password protected in line with the Access Control Policy
- Stored on encrypted removable media in line with the ICP4- Cryptography Policy.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Staff of FCS Laser Mail. A Secure workstation policy is in place.

Regarding physical controls, a clear desk policy is in place along with a fully secure magnetic fob access control system around the entire building premises.

Personal data may only be deleted or disposed of in line with the Data Retention policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by the Data Retention policy. Because of the increased risk all Staff must be specifically authorised to process data off-site as detailed in our Mobile and Teleworking Policy.

Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held FCS Laser Mail in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by FCS Laser Mail, and information obtained from third-party organisations about that person. Subject Access Requests are dealt with as described in the Subject Access Request Procedure.

Disclosure of data

FCS Laser Mail must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. All staff sign a confidentiality agreement upon starting their employment with FCS.

GDPR permits a number of exemptions where certain disclosure without consent is permitted, as long as the information is requested for one or more of the following purposes:

- To safeguard national security
- Prevention or detection of crime including the apprehension or prosecution of offenders
- Assessment or collection of tax duty
- Discharge of regulatory functions (includes health, safety and welfare of persons at work)
- To prevent serious harm to a third party
- To protect the vital interests of the individual, this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the IMS Representative.

Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a member of staff has left FCS Laser Mail, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. FCS Laser Mail's data retention and data disposal procedures will apply in all cases.

Disposal of records

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the Data Retention policy.

E-mail and Internet privacy

The inappropriate use of e-mail and the Internet by employees, e.g. using the Internet for non-work purposes, can have significant consequences for our Organisation. This can be in terms of:

- Embarrassment/damage to the Organisation's reputation
- Loss of productivity
- Increased risk of liability and legal action, e.g. for sexist or racist e-mails
- Increased virus risk

To avoid inappropriate usage, we have introduced security electronic safeguards. Firewall checks manages e-mail attachments. The Organisation has installed filtering software that searches e-mails for specific words or phrases, normally obscene or discriminatory, and monitors which websites our employees are accessing as well as filtering which types of websites our employees can access.

Acceptable use of E-mail and the Internet

Please see the E-mail and Internet Acceptable Usage Policy.
In addition, the Organisation's employees will be kept fully informed about overall information security procedures and the importance of their role within these procedures. Similarly, manual filing systems are held in secure locations and only authorised employees can access them.

Responsibilities and review

The IT Manager has overall responsibility for the administration and implementation of the Organisation's Data Protection Policy.

Each Department Manager will assume authority for the compliance of the employees within their department.

This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018 and the GDPR.

The Data Protection Policy will, under normal circumstances, be managed and reviewed annually. The reviews to the Policy will be subject to scrutiny and, from time to time, updates and re-issues will be circulated.

However, the Policy will be reviewed sooner in the event of any one or more of the following:

- Weakness in the Policy is highlighted
- Weaknesses in hardware and software controls are identified
- In case of new threat(s) or changed risks
- Changes in legislative requirements

Changes in Government, company or other directives and requirements.

Version	Date	Description	Approved by
A	10.08.18	Initial version	Steve Beeching