Data Protection Policy

Author	Ingrid Hurtado	Contact	01619472720	Approved by	Clinical Governance Committee		
Created date	1st May 2018			Register Number		Version	V1.1
Policy Location	I:\Policies 2018			CQC Fundamental Standard	Good Governance		

Document Review history (This policy should be reviewed as scheduled once every year unless performance indicators, changes to legislation or the organisation necessitate it)		
Review Number	**Review Date**	**Reviewed by**

Purpose

Face and Eye needs to process certain information about natural living persons. These include patients, suppliers, business contacts, employees and any other natural persons that the organisation has a relationship with or holds personal information on.
This policy describes how this personal data must be processed and controlled to meet the company's data protection standards and to comply with the law.

This data protection policy ensures the company:

- Complies with the data protection laws and follows good practice and codes of conduct.
- Protects the rights of all natural living persons on which it controls and processes data.
- Is open about how the organisation controls and processes a natural living person's data.
- Protects itself from the risks of data breach and information leakage.
- Protect its proprietary information.

The Data Protection Law

1. The Data Protection Act (DPA)

DPA describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

- ✓ Be processed fairly and lawfully.
- ✓ Be obtained only for specific, lawful purposes.
- ✓ Be adequate, relevant and not excessive.
- ✓ Be accurate and kept up to date.
- ✓ Not to be held for any longer than necessary.
- ✓ Processed in accordance with the rights of data subjects.
- ✓ Be protected in appropriate ways.
- ✓ Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

2. Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR)

GDPR describes how organisations must collect, handle and store personal information. Article 5 of the GDPR requires that personal data shall be:

- ✓ Processed lawfully, fairly and in a transparent manner in relation to individuals.

- ✓ Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- ✓ Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- ✓ Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
- ✓ Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is to be processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- ✓ Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Individuals Rights

The GDPR provides the following rights for individuals:

1. The right to be informed.
2. The right of access.
3. The right to rectification.
4. The right to erasure.
5. The right to restrict processing.
6. The right to data portability.
7. The right to object.
8. Rights in relation to automated decision making and profiling.

Scope

This policy applies to:

- ✓ All directors of the company.
- ✓ All contracted staff and bank staff of Face and Eye.
- ✓ All contractors, suppliers and other people working on behalf of the company.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the DPA or GDPR.

This can include but aren't limited to:

- ✓ Any other information from which an individual's identity can be inferred.
- ✓ Genetic and histopathological information.
- ✓ Information concerning physical or mental health.
- ✓ Information regarding political, religious or philosophical beliefs.
- ✓ The company's proprietary Information.
- ✓ Any proprietary information belonging to third parties that the company is contractually obligated to protect.

Data Protection Risks

This policy helps to protect the company from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.
- Cybersecurity breach. For instance, we could suffer from phishing.
- Damage to business operations through the disclosure of proprietary information.

Responsibilities

Everyone who works for or with the company has some responsibility for ensuring data is controlled and processed in a compliant manner. Each member of the team that handles sensitive data must ensure that it is handled and processed in line with this policy and the eight data protection principles of the DPA.

Roles

- The management team at Face and Eye is ultimately responsible for ensuring that the company meets its legal obligations.
- The management team at Face and Eye, is responsible for:
    - Keeping the directors updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line within an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data the company holds about them ('subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- Eezy-IT is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Evaluating any third-party services that the company is considering using to store or process data. For instance, cloud computing services and cloud based back up service.
- Trend Micro Worry-Free Business Security:
    - Performing real time scanning to ensure security hardware and software is functioning properly.

General Staff Responsibilities

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- The company will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure by following the guidelines in the information security policies, and the company procedures.
- Passwords must be managed as stated in the Password Policy.
- Personal data should never be disclosed to unauthorised people, either within the company or externally.
- If employees suspect a breach or security event it should be reported to the information security department.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of following the Disposal Procedure.
- Employees should request help from their line manager or the data protection officer (J Fox) if they are unsure about any aspect of data protection.

Training

All staff will receive training on this policy, supporting policies and company procedures. New joiners will receive training as part of the induction process. Further training will be provided at least once a year or whenever there is a substantial change in the law or the company policy and procedure. A record of this training will be kept in each staff training file.

The Principles of Data Protection

Fair, lawful and transparent *conditions for processing*

The company will ensure any processing of personal data has a documented legal basis. All parties who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice or a fair processing notice.

Privacy Notices

To ensure fair, lawful and transparent processing, privacy notices and fair processing notices shall be issued to data subjects to make them aware of how the company intends to use and protect their data.

These notices:

- State the purposes of processing data.
- State the information that is to be held.
- State the legal basis for processing data.
- State the length of time that the data will be retained for.
- State the measures taken to protect all data held.
- State the third parties that can access this data.
- Provides the contact details of the DPO.
- Provides the contact details of the third parties' DPO.
- Inform the data subjects of their rights.

Accuracy

The company shall ensure that any personal data processed is accurate and up to date by following the Data Quality Assurance Procedure when collecting or processing data. Data subjects have a responsibility to take reasonable steps to ensure that any personal data the company holds is accurate and updated as required. For example, if their personal circumstances change, they should inform the company so that their records can be updated.

Adequacy and relevance

The company shall ensure that any personal data collected is used only for the purpose for which it was obtained. Personal data obtained for one purpose shall not be used for any unconnected purpose unless the individual concerned has provided consent or there is a legal obligation to do otherwise.

Data retention

The company will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with the company's data retention guidelines. The company's Information Asset Register contains the information on how long each asset should be retained for. This retention does not affect the subject's right to erasure. Assets should be disposed of by following the Disposals Procedure.

Data Security

The company shall keep sensitive data secure against loss, misuse or unauthorised disclosure. Where other organisations process personal data as a service on behalf of the company, through GDPR123 Face and Eye will ensure that all organisations provide the same level of data protection as the company. In order to maintain consistent information protection throughout the company, the Information Security Policy shall be implemented and enforced through the use of supporting policies and procedures, training and appropriate technologies.

Privacy by design and default

The company shall follow the principle of privacy by design and default. This is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan. When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Data protection impact assessments (DPIA)

Where processing personal information is likely to result in a risk to the rights and freedoms of the data subjects, a data protection impact assessment shall be carried out and the results shall be implemented and incorporated into the project. Records of all DPIAs shall be kept and the assessment shall be carried out according to the Data Protection Impact Assessment Procedure.

Storing data

All data controlled by the company must be kept in a secure manner. In cases where data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it. Printed data should be shredded when it is no longer needed according to the standards in the Disposals Procedure. Data stored on a computer should be protected as outlined in the Information Security Policy. Data stored on CDs or memory sticks must comply with the guidelines in the Removable Media Policy. Data should be regularly backed up in line with the company's continuity and disaster recovery plans. All servers containing sensitive data must be approved and protected by security software and strong firewalls.

Transferring data internationally

Face and Eye does not transfer data outside of the EU, therefore no electronic data would be transferred internationally (outside of the EU). If this becomes necessary, the company will ensure that data gets transferred in an appropriate and approved secure measure following the International Data Transfer Procedure.

Data Subject rights

Processing data in accordance with the individual's rights

The company shall abide by the data subject's rights laid out in both the DPA and GDPR. Any request from an individual shall be handled by the DPO and a response issued within a month.

Consent

Where the company uses consent as the legal basis for processing data, there must be a record of the data subject's active consent. Consent should be gathered in the manner outlined in the Consent Management Procedure. The data subject has the right to withdraw this consent at any time. This right does not affect any of the other rights.

In cases where sensitive personal data is processed, the data subject's explicit consent to this processing will be required, unless exceptional circumstances apply or there is a legal obligation to do this (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The right to be informed

Under GDPR data subjects have the right to be informed about how their data is processed. To comply with this right, the company provides the required information in its privacy notice.

The right of access

Under the Data Protection Act, data subjects are entitled, subject to certain exceptions, to request access to information held about them.

These requests shall be passed to the DPO to handle. When handling these requests, a response must be made to the data subject within one month. The requests must be recorded and monitored and the process from the Subject Access Request Procedure should be followed.

The right to data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. There will be no charge for data transfer requests.

Under GDPR data subjects can request that their personal data is transferred from one data controller to another.

These requests shall be passed to the DPO to handle. When handling these requests, a response must be made to the data subject within one month. The requests must be recorded and monitored and the process from the Data Portability Procedure should be followed.

The right to rectification

Under GDPR data subjects can request that personal information held on them is corrected.

These requests shall be passed to the DPO to handle. When handling these requests, a response must be made to the data subject within one month. The requests must be recorded and monitored and the process from the Subject Rectification Request Procedure should be followed.

The right to erasure

Under GDPR data subjects may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

These requests shall be passed to the DPO to handle. When handling these requests, a response must be made to the data subject within one month. The requests must be recorded and monitored and the process from the Subject Erasure Request Procedure should be followed.

The right to restrict processing

Under GDPR data subjects can request a restriction of processing on their personal data in instances where the data subject does not wish for their data to be erased but does not want the data processed.

These requests shall be passed to the DPO to handle. When handling these requests, a response must be made to the data subject within one month. The requests must be recorded and monitored and the process from the Restricting Processing Procedure should be followed.

The right to object

Under GDPR data subjects can object to processing if they suspect that their data is being processed illegally. Following an objection, the data controller is required to investigate the claim and communicate the results to the data subject.

These requests shall be passed to the DPO to handle. When handling these requests, a response must be made to the data subject within one month. The requests must be recorded and monitored and the process from the Objection Request Procedure should be followed.

Rights in relation to automated decision making and profiling

Under GDPR data subjects have the right to be informed if they are being subject to automated decision making and the possible consequences this automated decision making could have on them. To comply with this right, the company provides the required information in its privacy notice and collects and documents the appropriate consent as stated in the Gathering Consent Procedure.

Compliance

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Data audit and register

Regular data audits to manage and mitigate risks will form the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures.

This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures.

Consequences of failing to comply

Disciplinary Terms

Where an employee has been found to have violated the company policies or procedures the following actions may be taken:

- Written Warning – An official warning that any further infractions will lead to further action.
- Removal of privileges – The staff member will be forbidden from performing certain actions, accessing certain systems or using certain devices.
- Corrective action – The member of staff shall take actions so that no further infractions occur for example, training.
- Termination of employment – The member of staff shall no longer work for the company.
- Civil action – A claim of legal recompense may be made against the staff member.
- Legal action – The Company will pass details of the infraction to the authorities with the intention of pressing charges.

Contracted Third Parties

Where a contracted third party has been found to have violated the contractual obligations relating to data protection, the following actions may be taken:

- Written Warning – An official warning that any further infractions will lead to further action.
- Removal of privileges – The contracted third party will be forbidden from performing certain actions, accessing certain systems or using certain devices.
- Corrective action – The contracted third party shall take actions so that no further infractions occur for example, training.
- Security Audit – An audit of the contracted third party's systems to make sure that they still meet their obligations.
- Termination of contract – The contracted third party shall no longer be contracted to work for the company.
- Civil action – A claim of legal recompense may be made against the contracted third party.
- Legal action – The Company will pass details of the infraction to the authorities with the intention of pressing charges.

Equality Impact

As an employer and a provider of health care, Face and Eye aims to ensure that none are placed at a disadvantage as a result of its policies and procedures. This document has therefore been equality impact assessed in line with current legislation to ensure fairness and consistency for all those covered by it regardless of their individuality. This means all our services are accessible, appropriate and sensitive to the needs of the individual.