

Data Protection Policy

(includes Disclosure Information Policy)

The correct functioning of software and hardware is critical to the delivery of services by Plastic Surgeon. This policy sets out practices and restrictions regarding the acceptable practices for securing Plastic Surgeon data.

Purpose

This policy applies to the securing of information, electronic and physical, required to conduct Plastic Surgeon business.

Secure Network Implementation

- (i) All routers, switches, wireless access points are password protected.
- (ii) Firewall changes are conducted by the Network Administrator and logged.
- (iii) All confidential data including customer databases and payment information are stored on the internal network (not the dmz) and protected by a firewall.
- (iv) The firewall is installed to protect the network and limit traffic to only which is required to conduct business. Regular updates are applied to the firewall to protect against viruses, malware, spam, and denial of service.
- (v) Web servers are located on a publicly reachable network by a firewall (DMZ).
- (vi) The Firewall is configured to translate (hide) internal IP addresses, using network address translation (NAT).
- (vii) Remote workers use an 3DES encrypted VPN tunnel to access systems.

Protection of Stored Data

- (i) All confidential data held on Plastic Surgeon production servers are accessed controlled via DACL permissions and strictly accessed on job role and need to know basis.
- (ii) Database backups are encrypted, password protected, and also open access is prevented via DACL (folder permission).
- (iii) Sensitive cardholder data is securely disposed of when no longer needed.
- (iv) All but the last four digits of the account number are masked when displaying cardholder data.
- (v) Any card data held within the systems is securely encrypted.
- (vi) SSL (Secure Socket Link) is used for transmission of sensitive cardholder data using version 3.0- and 128-bit encryption.
- (vii) No sensitive cardholder data is sent via email.

Development / Maintenance of secure systems and applications

- (i) Virus scanners are installed, and updates managed from an internal server.
- (ii) Changes to Plastic Surgeon bespoke computer system are formally authorised, planned, and logged before implementation.
- (iii) Production servers are service patched, and updates regularly applied.
- (iv) Vulnerability scans have been performed on internet-facing servers via Control Scan.

Access Control Methods

- (i) All users are required to authenticate using a unique username and password.
- (ii) Employees, IT administrators who connect remotely, use either software tunnel software or fixed IP addressing to gain access to systems.
- (iii) When an employee leaves the company their user account is revoked, and any security devices returned.
- (iv) Password policy is enforced, and complexity requirements are enabled.

- (v) All standard passwords are changed when a system is introduced to a production environment.
- (vi) Wireless technologies are protected with WPA keys.
- (vii) Production systems are hardened by removal of all unnecessary services and protocols. In particular Firewall server and Web Server.

Disclosure – Secure Handling, Use, Storage & Retention Policy

General Principles

The Plastic Surgeon Ltd complies fully with the Code of Practice, issued by Scottish Ministers, regarding the correct handling, holding, and destroying of Disclosure information provided by Disclosure Scotland under Part V of the Police Act 1997 (“the 1997 Act”), for the purposes of assessing applicants' suitability for employment purposes, voluntary positions, licensing, and other relevant purposes. It also complies fully with the General Data Protection Regulation and other relevant legislation pertaining to the safe handling, use, storage, retention, and disposal of Disclosure information.

Usage

We use Disclosure information only for the purpose for which it has been provided. The information provided by an individual for a position within The Plastic Surgeon Ltd is not used or disclosed in a manner incompatible with the purpose. We process personal data only with the express consent of the individual. We notify the individual of any non-obvious use of the data, including further disclosure to a third party, identifying the Data Controller, the purpose for the processing, and any further relevant information.

Handling

The Plastic Surgeon Ltd recognises that it is a criminal offence to disclose Disclosure information to any unauthorised person. We, therefore, only pass Disclosure information to those who are authorised to see it in the course of their duties.

Access and Storage

Disclosure information is kept electronically on an individual's personnel file. Access to Disclosure information is strictly controlled to authorised and named individuals, who are entitled to see such information in the course of their duties.

Retention

Disclosure information will be retained for the length of the applicants' service with The Plastic Surgeon Ltd. The same conditions relating to secure storage and access will apply during any such period.

Disposal

Once the retention period has elapsed, The Plastic Surgeon Ltd will not retain any image or photocopy or any other form of the Disclosure information. We will, however, keep a record of the date of issue of the Disclosure, the name of the subject, the Disclosure type, the position for which the Disclosure was requested, the unique reference number of the Disclosure and details of the recruitment decision taken.

Umbrella Bodies

Before acting as an Umbrella Body (i.e., a body which countersigns applications for Standard or Enhanced Disclosures on behalf of another organisation), The Plastic Surgeon Ltd will take all reasonable steps to ensure that the organisation on whose behalf we are acting will comply with the Code of Practice, and in full accordance with this policy. We will also take all reasonable steps to satisfy


ourselves that they will handle, use, store, retain and dispose of Disclosure information in full compliance with the Code of Practice, and in full accordance with this policy. We will also ensure that anybody or individual at whose request applications for Disclosures are countersigned, has such a written policy and, if necessary, will provide a model policy for that body or individual to use or adapt for this purpose.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Distribution

This policy is to be distributed to all staff.

Signed		Date	1 st May 2024
Name	Mike Aitken - Managing Director	Review	
Role	The Plastic Surgeon Ltd	Date	1 st May 2025