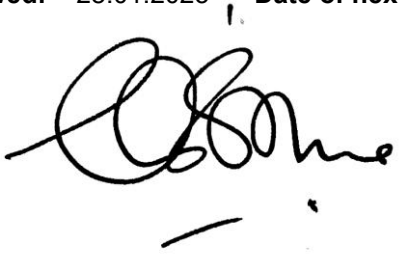
C. A. STONE
Medical & Legal Ltd

Information security policy

Aim: To ensure compliance with GDPR 2018 and the underlying principles of data protection.

Responsibility: C A Stone

Policy reviewed: 28.01.2025 **Date of next review**: 28.01.2028

Signed:  **Position**: Director

ICO Registration

Registration Number: ZA521139

Date Registered: 7 May 2019

Registration Expires: 7 May 2020 (renews automatically)

Data Controller: Christopher Anthony Stone

Registered Address:

C A Stone (Medical & Legal) Ltd

28 Alexandra Terrace

Exmouth

Devon

EX8 1BD

Companies House registration number: 07184587

Company correspondence address:

C A Stone (Medical & Legal) Ltd

PO Box 100

Sidmouth

EX10 1DJ

The company contracts secretarial services from Exeter Medical Ltd in respect of private cosmetic / surgical work. The company also employs a secretary in respect of medico-legal work who is trained in the principles of GDPR.

The following processes and procedures must be observed to ensure confidential data security.

Confidentiality within the Workplace

- The information on the computer system owned by CA Stone (Medical & Legal) Ltd ('the company') should only be seen by those who are authorised to see it.
- Screens provide a ready means for unauthorised persons to see confidential data. To guard against this, screens should be placed where they cannot easily be overlooked and their contents should be monitored by the user to ensure that confidential displays are kept to a minimum.
- The positioning should be such that the correct user can see the screen without difficulty but it is pointing away from members of the public. A time limit should be set on every computer that will invoke a screen saver. Both the clinical system and windows screen savers should be used with passwords needed to clear them.
- Only data that is stored on the company computer system will be included in the backup of data routine.

User ID's and passwords

- Extreme care should be taken to verify e-mail addresses.
- Individual usernames and passwords must be used at all times to access the computer system. Passwords must be kept secret and never disclosed to anyone. They should be unique and not easily identifiable (avoid names, date of birth etc). Do not keep a record of the username and password near the computer.
- The username and password are for the Director's exclusive use. They must not be shared or lent to anyone else.
- All medical reports or other sensitive material must be sent by email in an encrypted format.
- If logged onto a computer and intending to leave it for any time, the screensaver should be activated so that a password is needed to resume work.

Virus Protection

- Virus protection software (McAfee or Avast) is installed on all computers and should be checked for version control and updated monthly. If a virus is found it must be reported immediately to the company's IT consultants, Think IT.

Computer equipment owned by the company

- 2x HP desktop PCs, each password-protected

- Dell Inspiron laptop, password-protected
- Buffalo external hard drive, password-protected
- Scandisk encrypted flash drive
- Encrypted WD Passport external hard drive
- Encrypted Apple iPhone 13
- Sony alpha-7 digital camera

Data is backed-up to the WD external hard drive and securely to the Cloud via Livedrive.

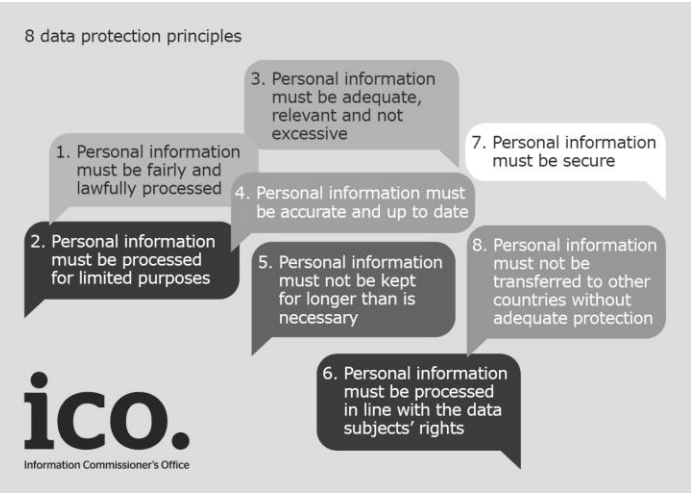
General Data Protection Regulations (GDPR) 2018

- The company Director, on behalf of the company, acquires personal data and determines the means and purpose of processing that data: a *Data Controller*.
- The company Director also manages, modifies, stores and analysis personal data on behalf of the company: a *Data Processor*.

Under GDPR regulations the company must:

- put in place compliance procedures
- ensure that any organisation with whom personal data is shared is GDPR compliant
- enter in to data governance agreements with instructing solicitors

The 8 Principles of data protection are summarised as follows:



Information held by CA Stone (Medical & Legal) Ltd

- Documents supplied by solicitors relating to personal injury and clinical negligence claims. These include (1) medical records; (2) clinical images; (3) personal contact information. Both hard copies and electronic files are stored.
- Medical reports compiled by the company.
- Patient images relating to medico-legal claims and cosmetic surgery.
- Email correspondence, stored on a password-protected email server.

Historical medico-legal records management

Hard copies of medical records relating to medico-legal claims are no longer stored within the secure premises of Crown Records Management, Exeter; the company has requested the destruction of all medical records held on behalf of the company and this process has now been completed.

Prospective medico-legal records management

The company is able to store records securely (locked and alarmed) on a temporary basis only at the company's correspondence address, pending production of the report. CA Stone (Medical & Legal) Ltd is unable to provide long term storage of paper records.

Where the bundle is provided in hard copy paper format it will be returned upon completion of the report to the instructing party at their cost, at standard courier 'signed for' rates. Alternatively, if specifically requested at the time of instruction, the hard copy records bundle will be confidentially destroyed upon completion of the report at the cost of the instructing party.

Clinical medical records management

Hard and electronic copies of medical records relating to patients treated by the company in its medical capacity are stored securely by Exeter Medical Ltd and Nuffield Health, Exeter. The company shall confirm GDPR compliance from both organisations for the storage and destruction of medical records held on behalf of the company.

The date controller will destroy / delete all claim records in the possession of the company (medical records, expert reports, invoices etc) in accordance with the following schedule, subject to the below[1]:

Date of last expert involvement:	Files will be deleted no later than:
2017	January 2025
2018	January 2026
2019	January 2027
2020	January 2028
2021	January 2029
2022	January 2030
2023	January 2031
2024	January 2032
2025	January 2033
2026	January 2034

[1] The data controller will archive all undeleted records at the time of winding up of the company. All files will be deleted no later than two years after that date.

The data controller will also arrange confidential destruction of hard copy records and deletion of electronic records files upon request by the instructing party.

The company has GDPR-compliant data security contracts in place with the following third parties:
Think IT
One Bright Spark
Thompson Jenner LLP Accountants

Privacy notices

Medico-legal website:
The Director of CA Stone (Medical & Legal) Ltd, Mr Christopher Stone, is the nominated data controller. Data is processed for the purposes of medico-legal expert witness reporting. CA Stone (Medical & Legal) Ltd will only process your information where it is necessary to support the legitimate interests of our business or those with whom we may have shared your information except where such interests are overridden by your interests or fundamental rights and freedoms which require the protection of personal data. Data shall only be shared with instructing solicitors and / or medico-legal agencies who are also GDPR-compliant.
Stored data shall include those details, including health records and images, necessary for the production of a medico-legal report. Data shall be stored in an encrypted format until a request for the data to be deleted has been received from the data subject or the instructing solicitor, or in accordance with Department of Health information retention schedules. Where possible all data shall be encrypted or otherwise anonymised at the time of electronic transfer. The data subject has the right to withdraw consent for storage of their personal information at any time or to lodge a complaint to the company or any relevant supervising authority.
CA Stone (Medical & Legal) Ltd will always respect your privacy and will only use your information for specified and lawful purposes as provided for under the General Data Protection Regulations (GDPR) 2018. We will use and handle your information responsibly and will take all appropriate organisational and technical measures to safeguard your information from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.
A copy of the company's information security policy is available upon request.

The privacy notices are posted on the following websites:

- www.medicalandlegal.co.uk

Individuals' rights

- Cosmetic surgery images: data will be deleted at the request of the data subject unless in so doing the company's ability to defend a clinical negligence claim becomes impaired

- Medico-legal records and images: data will be deleted at the request of the instructing solicitor

Subject access requests

- The company shall provide data subjects with the information held by the company free of charge within 30 days, subject to the conditions above.
- The company reserves the right to refuse requests for data that are manifestly unfounded, or to charge for the same.

Lawful basis for processing personal data

- The company operates a lawful practice in the provision of medico-legal reports and in the delivery of cosmetic and non-cosmetic surgical treatments.
- The company collects the minimum and relevant data necessary for it to exercise that lawful business.

Consent

- Consent under the terms of GDPR is defined as: '*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*.'
- Verbal consent for medical photography is sought from medico-legal clients at the time of examination.

Children

- The company provides medico-legal reports on behalf of children; however, the action is always brought by a Litigation Friend, who is an adult, parent or guardian.
- In such cases, the company applies GDPR principles to the Litigation Friend, from whom consent for data processing and storage is sought.

Data protection by design and data protection impact assessments

- The company shall be aware of situations where data processing is likely to result in high risk to individuals and shall undertake a DPIA where necessary.
- However, due to the narrow scope of the company's activity the potential for a DPIA to be required is currently assessed at being very low.
- Where a suspected or data breach occurs the company shall:
  (1) assess the impact and scope of the breach;
  (2) notify data subjects affected by the breach;
  (3) take immediate steps to prevent further breaches;
  (4) investigate the root cause of the breach;
  (5) make the necessary changes to strengthen its data security systems.