



Privacy Policy

Contents

Document Control	3
1. Purpose of this document	3
2. Publication details	3
3. Document history	3
4. Document approval	3
5. Associated Documents & Legislation	4
Overview	5
1. Scope of this Policy	5
2. Statement of Intent	5
3. Key Responsibilities	5
a) The Board of Directors	5
b) Managers, Supervisors and Team Leaders	6
c) All Staff and Contractors	6
d) Named Responsible Staff	6
What data do we collect?	7
How do we collect your data?	7
How will we use your data?	8
How do we store your data?	9
Marketing	9
What are your data protection rights?	9
Cookies	11
1. How do we use cookies?	11
2. What types of cookies do we use?	11
3. How to manage cookies	11
Privacy policies of other websites	11
Changes to our privacy policy	11
How to contact the appropriate authority	11
Data Breach Plan	12
1. Overview	12
2. Initial Actions	12
3. Investigation Process	13
4. Reporting Process	13
5. Remedial Actions	14
Consultation and Review	15
1. Consultation	15
2. Review	15
3. Authorisation to Publish	15

Document Control

1. Purpose of this document

This document details how Eaton General Services Limited, trading as Eaton Medical Services (the company) uses personal data that is collected from individuals, whether customers or otherwise.

This policy applies to all individuals involved in company operations, regardless of their terms of engagement, and the company's service users where applicable.

2. Publication details



Document Version:	1.0
Document Status:	Published
Initial Author(s):	Innes Eaton
Publication Date:	28/05/25
Next Review Date:	27/05/26
Directorate:	Training & Compliance
Responsible Manager(s):	Compliance Manager

3. Document history

Date	Version	Author/Reviewer	Amendment/Review Details
28/05/25	1.0	Innes Eaton	Amended for first publication
28/05/25	0.1	Innes Eaton	First draft: submitted for proof reading

4. Document approval

The following responsible managers have reviewed this document and approved it for publication:

Name	Job Title	Signatures
Innes Eaton	Managing Director	
Charlotte Eaton	Training & Compliance Director	

5. Associated Documents & Legislation

Internal	External
Clinical Operations Policy	Data Protection Act 2018
Compliance Policy	General Data Protection Regulations (GDPR)
Information Governance Policy	Freedom of Information Act 2000
Recruitment Policy	The Information Commissioner's Office (ICO)
Reporting Policy	The Care Quality Commission (CQC)
Safeguarding Policy	
Whistleblowing Policy	

Overview

1. Scope of this Policy

This policy applies to all individuals engaged in activities associated with Eaton Medical Services. It includes any contractors who undertake any activity for or on behalf of the company, any service users of the company, and covers all aspects of company activity.

This policy will cover all areas of data protection legislation applicable to the activities reasonably expected to be undertaken by the company, including:

- Data collection
- Data use and marketing
- Data storage
- Data destruction
- Cookie policy
- Data protection rights
- Details of the company's Data Protection Officer

2. Statement of Intent

By the methods described within this and the Information Governance policy, Eaton Medical Services intends to:

- Clearly state how data from individuals can be collected
- Clearly state how these data can be used, particularly in regard to marketing activities
- Clearly state how these data can be stored and for how long
- Clearly state how and when these data will be destroyed
- Clearly state how we use cookies and how an individual can manage these
- Clearly state the rights of an individual with regards to data that we hold
- Clearly state the actions to be taken by the company in the event of a data breach
- Give contact details of the company's Data Protection Officer as appointed under our registration with the Information Commissioners Office.
- Consult with staff members at regular intervals on the content of this and other related policies, both directly and through trade union representatives
- To regularly review, amend and update this and other related possibilities, taking into account the results of staff consultation wherever possible.

3. Key Responsibilities

a) The Board of Directors

The board of directors have full accountability for ensuring that the company complies with its legal obligations in regard to data protection; the shareholding of the individual director shall determine the level of personal accountability.

The subject of data protection falls fully within the remit of the training and compliance directorate: The Training & Compliance Director (where appointed) shall therefore assume full responsibility from the Managing Director for creation, implementation and review of data protection policy. Any aspect of these responsibilities may be delegated to a suitable manager and/or the appointed Data Protection Officer; however, accountability remains with the responsible director.

The responsible director must also ensure that regular compliance audits are undertaken, and that a robust incident reporting and 'whistleblowing' process exists: The results, recommendations and remedial actions of which should be collated and disseminated to all interested parties as soon as possible. A 'Freedom to Speak Up Guardian' shall be appointed by the responsible director, details of whom shall be made available to all staff and contractors. The same responsibilities also apply to implementing the recommendations of external bodies within a suitable timeframe.

b) Managers, Supervisors and Team Leaders

All managers, supervisors and team leaders within the company are responsible for ensuring that data protection policy is adhered to as closely as possible in all local activities.

All managers, supervisors and team leaders are responsible for ensuring that staff, contractors and service users are aware of their responsibilities under this policy, and supporting them in achieving these. Where necessary, managers, supervisors and team leaders shall act as a liaison between staff and the board of directors.

c) All Staff and Contractors

All staff and contractors working for or on behalf of the company, regardless of the employment terms by which they are bound, are responsible for ensuring that they are aware of their responsibilities under this policy, their contract of employment (where applicable), the law, and any other policy, protocol or guidelines applicable to the task undertaken.

All staff and contractors must adhere at all times to this policy, seeking guidance from an appropriate director, manager, supervisor or team leader if they have any queries or concerns.

d) Named Responsible Staff

Directors with specific data protection accountability:

Name	Job Title	Contact Details
Innes Eaton	Managing Director	Mobile: 07903 726728 innes@eaton-medical.co.uk
Charlotte Eaton	Training & Compliance Director	Mobile: 07756 615893 charlotte@eaton-medical.co.uk

Managers with specific data protection responsibilities:

Name & Job Title	Responsibilities	Contact Details
(Vacant) Compliance Manager	Policy & monitoring compliance	Covered by: Training & Compliance Director

Other key contacts within the company:

Name & Job Title	Responsibilities	Contact Details
Charlotte Eaton Data Protection Officer	Initial incident reporting and general enquiries	Mobile: 07756 615893 (Office Hrs) charlotte@eaton-medical.co.uk
Duty Manager	Escalation of incidents or for OOH incident reporting	Duty Phone: 07535 382223 (H24) dm@eatongeneralservices.co.uk
Duty Director	Escalation of serious untoward incidents (SUIs)	Duty Phone: 07535 382223 (H24) directors@eatongeneralservices.co.uk

What data do we collect?

The company may collect the following data from all individuals:

- Name
- Address
- Telephone number(s)
- E-mail address

Where a sale occurs, the company may collect the following additional data:

- Payment details

Where the individual wishes to work for the company, the company may collect the following additional data:

- Sex
- Date of birth
- Photographic identification such as driving licence, passport, or other suitable document
- Relevant occupational health history
- National insurance number
- Information about tax, national insurance, student loan and pension status
- Next of kin details
- Bank details
- Employment history
- Educational history
- Details of referees and their responses

Where a booking for medical cover is made, the company may collect the following data:

- Contact details for the event organiser(s)
- Contact details for the nominated point of contact
- Contact details for the relevant accounts department
- Details of the event, some of which may not be public knowledge
- Details of any risk assessment and/or resilience planning

Where a clinical consultation takes place, the company may collect any data that would assist in the triage, diagnosis, treatment and/or onward referral of the patient.

How do we collect your data?

You directly provide the company with most of the data that we collect. We collect and process data when you:

- Enquire about, or purchase/book, any of our products or services
- Voluntarily complete a customer survey or provide feedback on any of our message boards or via email
- Use or view our website via your browser's cookies
- Apply for employment with the company
- Present as a patient to any of our medical team

The company may also receive your data indirectly from the following sources:

- When another organisation enquires about, or purchases/books any of our products or services on your behalf
- Referees providing data on request, as part of the application process
- From friends/relatives in the event of a medical emergency, when you are not able to provide the data yourself

How will we use your data?

The company collects your data so that we can:

- Quote, process your booking, and/or manage your account
- Prepare an event medical plan, including any required risk assessment
- Take payment for products or services
- To provide suitable medical treatment and/or onward referral if you present as a patient

In the case of recruitment:

- To satisfy our due diligence requirements during the process
- To ensure that you are paid correctly for any work undertaken on behalf of the company where applicable

The company will not share data with external organisations for the purposes of marketing. Data may be shared with external organisations for the following purposes:

- As required to ensure seamless onward referral in the case of a medical episode requiring such
- The event organiser(s) and/or HSE, where an incident you are involved in is required to be reported
- As required for the purposes of fulfilling employment, regardless of the terms
- To prevent fraudulent transactions by sharing of data with credit reference agencies
- During the process of a credit application, in order for the relevant company to begin processing your application
- For the prevention of crime

As such, the company may only share your data with the following organisations:

- External healthcare providers, including (but not limited to):
 - The NHS Ambulance Service
 - Local hospitals
 - The 111 or Out of Hours service
 - Your registered GP
- External interested parties
 - The event organiser(s)
 - HSE
- Credit referencing agencies, via:
 - Stripe Inc
 - PayPal Europe
 - Zettle
 - Square
 - GoCardless
 - PayltMonthly Ltd
- Credit providers
 - PayltMonthly Ltd
 - PayPal Europe
- Legal authorities
 - The police
 - HMRC
- Other organisations as required for the purposes of fulfilling employment
 - Your nominated bank
 - NEST Pension Scheme
 - GetScheduled
 - Salus3 Cloud
- Other organisations as required for the delivery of our services
 - Salus3 Cloud
 - Bookeo
 - Xero Accounting Software
 - RAMSapp

How do we store your data?

The company securely stores your electronic data online through one or more of the following software packages, as applicable:

- Bookeo
- Salus3 Cloud
- Xero Accounting Software
- GetScheduled
- Google Forms
- Dropbox for Business
- RAMSapp

All of the above packages are password protected with access limited to those with the need to access the data for legitimate reasons. Payment card information is collected automatically during the checkout process and is not visible to any users.

The company securely stores written data that cannot be destroyed in one of our secure storage facilities. These are kept locked with keys only available to those with the need to access the data for legitimate reasons.

The company will keep your data for the time periods listed below. Once this time period has expired, we will delete electronic data from all applicable software packages and/or securely shred and dispose of any written data.

- | | |
|-----------------------------|--|
| • Event/administrative data | 1 year after completion of the event |
| • Clinical data | 8 years after completion of treatment by us* |
| • Employee data | 6 years after termination of employment |

*Clinical data shared by us to external healthcare providers may be stored for longer periods if required.

Marketing

The company will not use your data for marketing purposes, nor will we share your data with any organisation for the purposes of marketing.

What are your data protection rights?

The company would like to make sure you are fully aware of all of your data protection rights. Every user is entitled to the following:

- **The right to access** – You have the right to request Our Company for copies of your personal data. We may charge you a small fee for this service.
- **The right to rectification** – You have the right to request that Our Company correct any information you believe is inaccurate. You also have the right to request Our Company to complete the information you believe is incomplete.
- **The right to erasure** – You have the right to request that Our Company erase your personal data, under certain conditions.
- **The right to restrict processing** – You have the right to request that Our Company restrict the processing of your personal data, under certain conditions.
- **The right to object to processing** – You have the right to object to Our Company's processing of your personal data, under certain conditions.
- **The right to data portability** – You have the right to request that Our Company transfer the data that we have collected to another organization, or directly to you, under certain conditions.

If you make a request, we have one month to respond to you. If you would like to exercise any of these rights, please contact us by one of the following means:



- Email: data@eatongeneralservices.co.uk
- Post: Eaton General Services LTD t/a Eaton Medical Services
Unit 10, Field Side Farm
Quainton
Aylesbury
Buckinghamshire
HP22 4DQ

Cookies

Cookies are text files placed on your computer to collect standard Internet log information and visitor behaviour information. When you visit our websites, we may collect information from you automatically through cookies or similar technology

For further information, visit www.allaboutcookies.org.

1. How do we use cookies?

Our Company uses cookies in a range of ways to improve your experience on our website, including:

- Keeping you signed in
- Understanding how you use our website
- Preventing repeated pop-up boxes when you have already visited our site

2. What types of cookies do we use?

There are a number of different types of cookies, however, our website uses:

- Functionality – Our Company uses these cookies so that we recognise you on our website and remember your previously selected preferences. These could include what language you prefer and location you are in. A mix of first-party and third-party cookies are used.
- Advertising – Our Company uses these cookies to collect information about your visit to our website, the content you viewed, the links you followed and information about your browser, device, and your IP address.

3. How to manage cookies

You can set your browser not to accept cookies, and the above website tells you how to remove cookies from your browser. However, in a few cases, some of our website features may not function as a result.

Privacy policies of other websites

The Eaton Medical Services website contains links to other websites. Our privacy policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.

Changes to our privacy policy

Our Company keeps its privacy policy under regular review and places any updates on our web page. This privacy policy was last updated on 28th May 2025.

How to contact the appropriate authority

Should you wish to report a complaint or if you feel that the company has not addressed your concern in a satisfactory manner, you may contact the Information Commissioner's Office.

Data Breach Plan

1. Overview

In the event of a confirmed or suspected data breach, or a near-miss incident, the Data Protection Officer (DPO) shall be immediately notified and shall take charge of the organisation's response. The DPO shall additionally have the full support of the Board of Directors.

A data breach shall be defined as any situation in which data (as defined in this policy) is accessed by anyone not authorised to do so by the owner of that data. A near-miss incident shall be defined as any situation in which data is able to be accessed by unauthorised users, although no breach actually occurs.

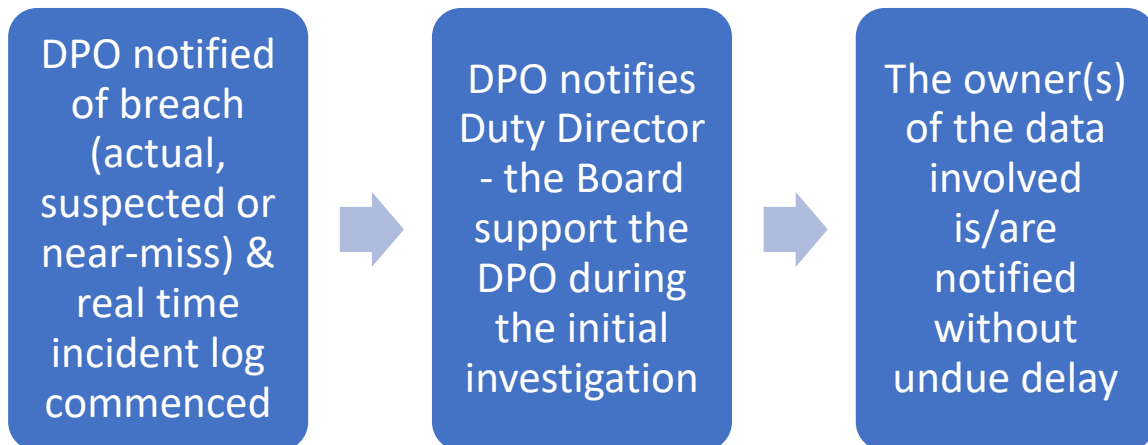
The Data Protection Officer shall decide whether any data breach constitutes a reportable incident as defined by the Information Commissioner's Office (ICO) and take action to ensure that the company's legal obligations in this respect are met in a timely manner.

The company shall commit to a regular audit schedule designed to test both the resilience of its data protection measures and the efficacy of any data breach plans in place.

Further information on this subject can be found in the relevant sections of the company's Information Governance and Reporting Policies.

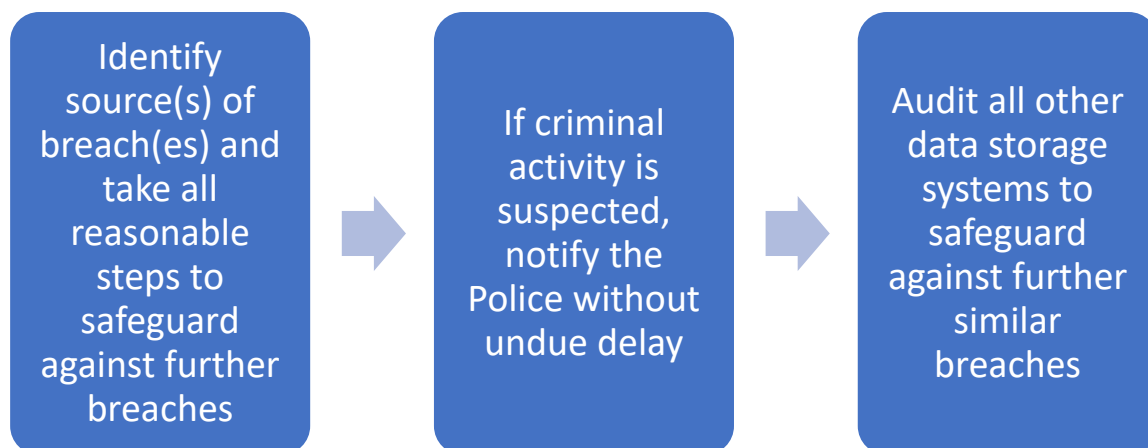
2. Initial Actions

Anyone may make an initial incident report by telephone to the company's Data Protection Officer via the contact details given in this document. The DPO is solely responsible for initiating the company's initial response. In the event that the DPO is not immediately contactable, the Duty Director may assume this role in the interim.



3. Investigation Process

The investigation shall start as soon as practical, taking into account the nature of the report – note that if the ICO need to be informed, this must be done within 72 hours of the initial report. The DPO is solely responsible for overseeing the investigation process and shall be supported by the Board of Directors in doing so. The owner(s) of any data involved must be kept up to date with the progress of the incident, insofar as is reasonably practical.



4. Reporting Process

The reporting process is further covered in the company's Reporting Policy. The ICO may impose a time limit on the publishing of the final report and the Board of Directors shall ensure that this is complied with and that all interested parties are kept informed of the progress and any unexpected delays.





5. Remedial Actions

Any remedial actions recommended in the final report shall be instigated as soon as possible. It shall be the responsibility of the Training & Compliance Director to ensure that these actions have been implemented in a timely manner and are being adhered to.

Consultation and Review

1. Consultation

All staff and contractors affected by this policy document are invited to send suggestions for future amendments to the Managing Director of Eaton General Services Limited by email in the first instance.

Where substantial amendments to this policy are planned, opportunities for direct staff and contractor consultation shall be provided.

2. Review

This policy document remains the responsibility of the Training & Compliance Directorate.

This policy document shall be reviewed at least annually, or whenever there are significant changes required: the RAG system shall be used to decide the timescale in which changes must be applied.

Green: Spelling or grammatical errors, small changes to policy wording where the meaning of such is not significantly changed. These changes shall be completed at the next scheduled document review. Where five or more 'green' changes exist for this policy document, the changes shall be considered in line with 'amber' guidance below.

Amber: Significant alterations to the policy document wording or structure, whether or not the meaning of such is changed, that do not negatively affect safe working practices in the interim. 'Amber' changes shall be referred to the Training & Compliance Director for a decision as to when the document shall be reviewed and updated: in any case, this shall not exceed three months.

Red: Significant alterations to the policy document wording or structure where safe working practices may be affected in the interim. This includes changes in policy following a SUI as an example. 'Red' changes must be referred to the Training & Compliance Director, and the document must be reviewed and updated as soon as possible: in all cases, this shall not exceed seven days. Where appropriate, an interim bulletin shall be issued until such time as the document can be updated.

This document is next scheduled for review on 28/05/26.

3. Authorisation to Publish

Authority to publish this version (v1.0) of the document was given by the Board of Directors on 28/05/25.