



DATA PROTECTION POLICY

1. Introduction

The General Data Protection Regulation (EU) 2016/679 ("GDPR") and the Data Protection Act 2018 govern how East Coast Vets processes personal data.

This policy sets out how East Coast Vets collects, uses, stores, shares, and protects personal data relating to individuals, including clients, employees, suppliers, contractors, and other third parties with whom the organisation interacts.

East Coast Vets is committed to complying with all applicable Data Protection Legislation and to ensuring that personal data is processed lawfully, fairly, transparently, and securely.

2. Purpose

East Coast Vets ("the Practice") is committed to protecting the privacy and security of personal data and complying with the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the Data Protection Act 2018, and all applicable Irish Data Protection Legislation.

This policy establishes the principles and procedures that all employees, contractors, and third parties acting on behalf of the Practice must follow when processing personal data. In order to operate effectively, East Coast Vets processes personal data relating to individuals, organisations, and companies with whom it engages. Such processing shall be carried out in accordance with Data Protection Legislation and internal governance requirements.

3. Scope

This policy applies to:

- All employees, directors, contractors, temporary staff, volunteers and other workers affiliated with third parties.
- All personal data processed by the Practice in electronic or paper format.
- All systems, devices, applications, and services used to process personal data.

4. Responsibilities

The Data Protection Lead/Privacy Officer is responsible for overseeing compliance with Data Protection Legislation and the implementation of this policy.

All employees, contractors, and third parties acting on behalf of East Coast Vets shall process personal data in accordance with this policy and associated procedures.

Employees shall report any data protection concerns, incidents, or breaches to the Data Protection Lead/Privacy Officer without delay.

5. Policy

Definitions

To aid the understanding of this document and the provisions of Data Protection Legislation, the following definitions are provided.

Personal Data

Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified directly or indirectly, in particular reference to an identifier such as name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.

Examples of personal data processed includes (but is not limited to):

- Name, address, email address, gender, age;
- Pay and bank details, including credit card details;
- Pension details;
- Qualifications
- Job performance

Processing

Any operation or set of operations performed on personal data or sets of personal data, such as:

Collection, recording, organising, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, transfer, and deletion.

Data Processor

Means any person, other than an employee of East Coast Vets, who processes personal data on behalf of the data controller, e.g. an organisation contracted to provide a payroll service.

Data Subject

An individual whose personal data is processed by the Practice.

Special Category Data

Personal data revealing racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, health data, sexual life/orientation, genetic or biometric data, or other categories defined by GDPR.

Data Controller

Refers to East Coast Vets and their practices.

Profiling

Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

Third Party

Means a person, agency, organisation, or public authority; other than the data subject, controllers, or processor and who, under the direct instruction of the controller or processor, are authorised to process personal data.

Consent

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to the individual.

Personal Data Breach

Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Protection Principles

GDPR requires that personal data is processed in accordance with the following principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

East Coast Vets shall ensure compliance with these principles and shall be able to demonstrate such compliance where required.

Meeting the Principles

East Coast Vets shall ensure that all processing of personal data is supported by a lawful basis under Article 6 GDPR and, where applicable, Article 9 GDPR.

Individuals shall be provided with clear and transparent information regarding how their personal data is processed through appropriate Privacy Notices.

Personal data shall be:

- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date where required
- Retained only for as long as necessary in accordance with the Retention Policy
- Processed securely using appropriate technical and organisational measures

6. Categories of Personal Data Processed

The Practice may process:

Client Data

- Names
- Addresses
- Telephone numbers
- Email addresses
- Payment and billing information
- Insurance details

Animal Records

- Ownership details
- Medical histories
- Treatment records
- Vaccination records
- Laboratory reports

Employee Data

- Contact information
- Payroll information
- Tax records
- Performance and employment records

Supplier Data

- Contact details
- Financial and contractual information

Website Data

- Website enquiries
- Cookie information
- Analytics data where applicable

7. Lawful Bases for Processing

The Practice processes personal data under one or more of the following lawful bases:

- Performance of a contract.
- Compliance with legal obligations.
- Legitimate interests.
- Consent.
- Protection of vital interests.

Where consent is relied upon, it shall be freely given, specific, informed, and capable of withdrawal.

Personal data shall not be processed (including disclosure) unless at least one of the conditions in Article 6 of the GDPR is met and in the case of the processing of special categories of personal data at least one of the conditions in Article 9 of the Regulation must also be met.

One of the conditions to process personal data is consent, which must be freely given. The GDPR recognises that employers will rarely be able to rely on consent as a lawful basis due to the clear imbalance between the individual and the employer, as it's unlikely that consent can be freely given in all circumstances of a specific situation.

The majority of the remaining conditions require the processing to be 'necessary', therefore the processing must be a targeted and proportionate way of achieving the purpose. It would not be necessary if the purpose could be reasonably achieved by a less intrusive way.

East Coast Vets must determine a lawful basis before they begin processing; therefore, employees must seek the **Data Protection Lead/Privacy Officer's** advice when determining the relevant condition to process personal data, as consideration will have to be given to associated data protection provisions. There will also be a requirement to update the **Record of Processing Activities Log** held by the Data Protection Lead/Privacy Officer.

Appendix A provides the Article 6 and 9 conditions.

8. Data Subject Rights

The Regulation grants several rights to individuals. Not all of them are absolute and can be subject to exemption. They are, the right:

- Right to be informed.
- Right of access.
- Right to rectification.
- Right to erasure.
- Right to restrict processing.
- Right to data portability.
- Right to object.
- Rights relating to automated decision-making including profiling.

All requests received (verbally, electronically, or in writing) should be forwarded immediately to the **Data Protection Department**.

Requests shall be handled promptly and within statutory deadlines.

Individuals have the right to lodge a complaint with the Data Protection Commission (DPC) where they believe their personal data has been processed in breach of Data Protection Legislation.

Right to be Informed – Privacy Notice

The right to be informed encompasses an obligation to provide individuals, including employees, information about how East Coast Vets will use their personal data, including the lawful basis of processing. This is provided to individuals in a form of a Privacy Notice.

The right applies whether East Coast Vets collect the personal data directly from the individual or another source.

A Privacy Notice must:

- Be concise, transparent, intelligible and easily accessible;
- Be written in clear plain language;

- Include the right to withdraw consent if the processing was based on consent;
- Include all the information within either Article 13 or 14 of the Regulation.

East Coast Vets' Privacy Notice is published on their website.

Employee Data and Privacy Notice

East Coast Vets reserve the right to collect, store and process data about its employees insofar as it is relevant in the employment context and it's retained according to the Retention Policy. This includes the processing of special categories of personal data. The processing is for the purposes of the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer property, well-being of staff, and for the purposes of rights and benefits related to employment and for the purpose of the termination of the employment relationship.

The Staff Privacy Notice is provided to new starters and available on PAWpad and Bright HR.

The **Data Protection Department (Data Protection Lead/Privacy Officer and CIO)** will review the Privacy Notices regularly.

The **Data Protection Department's** advice must be sought where a decision is going to be made based solely on automated processing, including profiling, as this is prohibited by the GDPR in certain circumstances and appropriate safeguards need to be put in place. This includes the requirement to notify the individual of such processing, so they can exercise their right to obtain meaningful human intervention (someone who has authority to change the decision), express their views, obtain an explanation of the decision reached and contest the decision.

Where data is being processed by East Coast Vets and the identity of the individual has been confirmed, East Coast Vets shall respond to the rights request, on behalf of practices and provide the data subject with a response.

The Data Protection Lead/Privacy Officer

The **Data Protection Lead** oversees compliance with Data Protection Legislation, specifically:

- Inform and advise East Coast Vets employees who carry out processing, of their obligations pursuant to Data Protection Legislation;
- Monitor compliance with Data Protection Legislation and other policies in relation to data protection, including the assignment of responsibilities, awareness raising, and training of staff involved in processing activities, and the related audits;
- Provide advice where requested with regards to Data Protection Impact Assessments (DPIA) and monitor its performance;
- Act as the contact point for the Data Protection Commission (DPC) on issues to processing, including the prior consultation on DPIA's, and to consult, where appropriate with regards to any other matter;
- Cooperate with the DPC.

Record of Processing Activities Log (RoPA)

It is a legal requirement that East Coast Vets maintain a register of all the personal data they process.

The **Data Protection Lead/Privacy Officer** maintains the log for East Coast Vets which includes, but is not limited to, the legal basis for processing personal information, the processing purpose, who it is shared with, retention and categories of personal data.

All processing of personal data must be recorded on the log and be provided to the DPC on request.

Data Processors

To ensure compliance with the requirements of Data Protection Legislation in respect of processing carried out on behalf of East Coast Vets, by another body (data processor), East Coast Vets will only use processors providing sufficient guarantees, in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of Data Protection Legislation, including for the security of processing.

The processing by a processor shall be governed by a contract, which is detailed in **Data Processing Agreement**. This contract stipulates the requirements set out in Article 28 of the GDPR, including, but not limited to:

- The subject-matter and duration of the processing;
- The nature and purposes of processing;
- The type of personal data and categories of data subjects, taking into account the specific task and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject;
- Ensuring that they and their staff who have access to personal data, are aware of this policy and are aware of their duties and responsibilities under Data Protection Legislation;
- Allow data protection audits by East Coast Vets of data held on its behalf (if requested); and
- Confirm that they will abide by the requirements of Data Protection Legislation.

Upon completion of processing, the processor shall, at the choice of East Coast Vets, return or securely delete personal data unless retention is required by law.

Practices should seek advice from the **Data Protection Department** at East Coast Vets prior to any engagement with a data processor to ensure contractual arrangements meet Data Protection Legislation requirements.

Data Protection by Design

The GDPR makes privacy by design a legal requirement, under the term 'data protection by

design and by default’.

East Coast Vets will ensure that the data it collects and uses is proportionate and necessary for the intended purpose. Processes, procedures and systems will enable the data to be accessed only by those that require access and deleted in accordance with the Retention Policy.

East Coast Vets will demonstrate transparency in accordance with Data Protection Legislation and look at creating and improving security features on an ongoing basis.

The undertaking of a Data Protection Impact Assessment (DPIA) will assist East Coast Vets comply with this requirement.

Data Protection Impact Assessment

A DPIA is required in situations where data processing is likely to result in high risk to data subjects.

The DPIA enables East Coast Vets to identify and rectify problems at an early stage, demonstrate compliance with data protection obligations, meet individual’s expectations of privacy and help avoid reputation damage which might otherwise occur.

The **Data Protection Impact Assessment template** allows:

- The nature, scope, context and purposes of processing to be described;
- The necessity, proportionality and compliance measures to be assessed;
- Risks to individuals to be identified and assessed; and
- Additional measures to mitigate risks to be identified.

East Coast Vets’ DPIA’s are performed by the Data Protection Lead/Privacy Officer. Data processors or the CIO can be requested to assist with the completion.

Where a Data Protection Impact Assessment (DPIA) identifies a high residual risk that cannot be mitigated, East Coast Vets shall consult the Data Protection Commission prior to commencing the processing activity.

8A. Subject Access Requests (SAR) Procedure

8A.1 Right of Access (Subject Access Requests)

Under Article 15 of the GDPR, individuals (data subjects) have the right to obtain confirmation as to whether East Coast Vets processes personal data relating to them and, where that is the case, to access that personal data and receive a copy.

A Subject Access Request (SAR) may be made verbally, in writing, by email, or via any communication channel used by the Practice.

8A.2 Receipt and Escalation of SARs

All staff must recognise and promptly forward any potential SAR to the Data Protection Lead/Privacy Officer without delay.

The date of receipt is the date the request is first received by any member of staff, not when it is escalated internally.

The Data Protection Lead/Privacy Officer will:

- Log the request in the SAR register
- Verify the identity of the requester
- Confirm the scope of the request where necessary
- Coordinate the search and retrieval of relevant data

Staff must not attempt to respond to SARs informally or provide partial data outside of this procedure.

8A.3 Identity Verification

Before disclosing any personal data, East Coast Vets will take reasonable steps to verify the identity of the requester.

Where necessary, additional information may be requested to confirm identity, particularly where:

- Sensitive personal data is involved
- The request is made remotely
- There is reasonable doubt as to identity

8A.4 Time Limits

SARs will be responded to **without undue delay and within one calendar month** of receipt.

This period may be extended by up to two additional months where requests are complex or numerous. Where an extension is required, the individual will be informed within one month of receipt, together with the reasons for the delay.

8A.5 Scope of Information Provided

Where a valid SAR is made, East Coast Vets will provide the data subject with:

- Confirmation of whether personal data is being processed
- A copy of the personal data held
- Purposes of processing
- Categories of personal data concerned
- Categories of recipients
- Retention periods or criteria used to determine retention
- The source of the data (where not obtained directly from the individual)
- Information on data subject rights
- Details of international transfers and safeguards (if applicable)
- Details of any automated decision-making or profiling (if applicable)

8A.6 Exemptions and Restrictions

The Practice may withhold or redact personal data where permitted under GDPR and applicable Irish Data Protection Law, including where:

- Disclosure would adversely affect the rights and freedoms of others
- Third-party personal data cannot be reasonably separated or anonymised
- Legal professional privilege applies
- Disclosure would prejudice ongoing investigations or legal claims

Where exemptions are applied, the data subject will be informed where appropriate.

8A.7 Format of Response

Information will be provided in a commonly used electronic format unless otherwise requested by the data subject.

Where SARs are submitted electronically, responses will be provided by secure electronic means unless otherwise agreed.

8A.8 Fees

SARs will generally be provided free of charge.

A reasonable fee may be charged, or the request refused, where the request is manifestly unfounded, excessive, or repetitive.

8A.9 Record Keeping

The Data Protection Lead/Privacy Officer will maintain a SAR register including:

- Date of receipt
- Identity verification steps
- Scope and actions taken
- Response date
- Exemptions applied (if any)
- Correspondence with the data subject

All SAR documentation will be retained in accordance with the Practice Retention Schedule.

8A.10 Staff Responsibilities

All employees must:

- Recognise SARs regardless of wording used by the requester
- Escalate requests immediately to the Data Protection Lead/Privacy Officer
- Preserve relevant data once a SAR is received (no deletion or alteration)
- Maintain confidentiality throughout the process

Failure to properly escalate or mishandling a SAR may result in disciplinary action.

9. Security Measures

The Practice shall implement appropriate security measures including:

- Strong password requirements.
- Multi-factor authentication where available.
- Role-based access controls.
- Device encryption.
- Secure backups.
- Anti-malware protection.
- Regular software updates and patching.
- Secure disposal of confidential records.
- Physical security controls for premises and records.

Access to personal data shall be restricted to authorised personnel only.

Data Protection Legislation requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All employees have a responsibility to take appropriate technical and organisational security measures to safeguard personal information.

In particular, an employee should, as a minimum, ensure that:

- Paper files and other records or documents containing personal/special category data are kept in a secure environment, by locking them away in a securely locked cupboard/cabinet;
- Personal data is disposed of in confidential waste bins or shredded;
- Personal data held on computers and computer systems are protected by the use of a secure password;
- Computer networks that hold personal data will be protected with appropriate levels of physical and logical security to prevent unauthorised parties having access to that data;
- Individual passwords should be such that they are not easily compromised;
- Passwords are applied to sensitive documents when sending via email;

Employees should not remove information from a place of work unless it is absolutely necessary to do so. If it is necessary, assurances should be implemented to ensure it is adequately protected from unauthorised use or disclosure. Laptops, other devices and any hard copies of personal data should not be left unattended in any public place. Care should also be taken when observing the information in hard copy or on screen, that such data is not viewed by anyone who is not legitimately privy to that information.

Any loss of personal data must be reported in accordance with the **Notification of Breach Procedure**.

If an employee acquires personal data in error, by any means, they shall report and manage it in accordance with that procedure also.

Personal Data Breach

All employees at East Coast Vets have a responsibility to report any potential, suspected or actual personal data breaches immediately to the **Data Protection Department** at East Coast Vets, in order that all necessary and appropriate action can be taken.

A personal data breach is a security incident and may arise from (but not limited to):

- Loss or theft of data or information;
- A deliberate attack on systems;
- The unauthorised or unlawful use of personal data by a member of staff;
- Misuse of information or equipment;

- Inappropriate disclosure;

- Accidental loss or equipment failure.

If it is determined that the incident is indeed a breach of personal data and results in a risk to the rights and freedoms of an individual, the **Data Protection Department** at East Coast Vets will notify the DPC within 72 hours of becoming aware of it.

If it is determined that the breach will likely result in a high risk to an individual, e.g. identify fraud, the individual must be informed without undue delay. If the risk is deemed to be serious by the DPC it could result in a fine of up to 4% of global turnover or €20,000,000.

Further information about what to do in the event of a personal data breach can be found in Notification of Breach Procedure.

10. Confidentiality

All staff must maintain confidentiality regarding personal data obtained through their employment.

Employees must not disclose personal data to unauthorised persons and must comply with all confidentiality obligations.

East Coast Vets will ensure that personal data is treated as confidential and access to personal data will be on a role requirement basis.

Employees during the course of employment may have access to, gain knowledge or be entrusted with personal information or other confidential information. Employees are not to inappropriately disclose to any person or make any use of such information, in any form whatsoever, at any time, whether during or after the end of employment with East Coast Vets.

However, employees need to be able to draw a distinction between ensuring personal data is treated confidentially, and the requirements of whistleblowing, which provides avenues for staff to raise concerns as to malpractice or wrong doings.

Disclosures

Release of information must be, and will be, in accordance with the provisions of Data Protection Legislation. East Coast Vets have a duty to share certain data to agencies such as Office of the Revenue Commissioners (Revenue). This will be carried out strictly in accordance with statutory requirements.

11. Data Retention

Personal data shall be retained only for as long as necessary to fulfil legal, regulatory, operational, and professional obligations.

The Practice shall maintain a documented Retention Schedule specifying retention periods for each category of records.

At the end of the retention period, data shall be securely deleted, anonymised, or destroyed.

12. Data Sharing

Personal data may be shared with:

- Veterinary laboratories.
- Referral veterinary practices.
- Insurance providers.
- Payment service providers.
- IT and software providers.
- Professional advisers.
- Regulatory or law enforcement authorities where legally required.

Appropriate Data Processing Agreements shall be maintained where required.

Information shall not be disclosed unless Article 6, and if special category personal data, Article 9 are satisfied.

There are occasions where East Coast Vets are required to share information. In all cases where information is shared East Coast Vets will have identified the lawful basis for disclosure or having obtained the data subject's consent to share.

Where East Coast Vets share without asking for the data subject's consent, they must have a legal duty or power to share information with other statutory bodies from statute or from common law.

13. International Transfers

Where personal data is transferred outside the European Economic Area (EEA), the Practice shall ensure appropriate safeguards are in place in accordance with GDPR requirements.

Data Protection Legislation imposes restrictions on the transfer of personal data outside the European Union to third countries or organisations.

Personal data may only be transferred outside the EU in compliance with the conditions for transfer set out within the GDPR.

No employee is to transfer East Coast Vets practice data outside of the EU, without consulting the Data Protection Lead/Privacy Officer.

14. Training and Awareness

All staff shall receive appropriate data protection training.

Training shall be provided:

- Upon induction.
- Periodically thereafter.
- Following significant legislative or operational changes.

All employees across East Coast Vets are required to complete the **Understanding GDPR** module and **Cyber Security Best Practices** module upon induction and then annually via the BrightHR E-Learning platform). Employees must familiarise themselves with and digest the content of the GDPR Awareness document, all policies, procedures and guidance notes published on PAWpad/Bright HR

East Coast Vets will continually review and update training materials to ensure appropriate role related training is given.

15. Consequences of Non-Compliance

All employees are under an obligation to ensure that they have regard to the six principles relating to the processing of personal data and this policy when collecting, access, using and disposing of personal data. Failure to observe the principles and this policy may result in an employee incurring personal criminal liability, or disciplinary action.

The DPC has powers, including the ability to fine organisations, to ensure that the principles of the GDPR as well as the rights of the individuals concerned are upheld according to the wording and the intention of the Regulation.

If an employee at East Coast Vets is in any doubt about what they may or may not do with personal information, they should initially seek advice from their immediate manager, or contact the **Data Protection Department**.

16. Appendix A – Lawfulness of Processing

Article 6 states that processing shall be lawful only if at least one of the following applies:

- 6 (1) (a) – the data subject has given **consent** to the processing of his or her personal data for one or more specific purpose;
- 6 (1) (b) – processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- 6 (1) (c) – processing is necessary for compliance with a **legal obligation** to which the controller is subject;
- 6 (1) (d) – processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
- 6 (1) (e) – processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;
- 6 (1) (f) – processing is necessary for the purposes of the **legitimate interest** pursued by the controller or by a third party.

Article 9 states that processing of personal data revealing **special categories** of information is prohibited unless one of the following applies:

- 9 (2) (a) – the data subject has given **explicit consent** to the processing of the personal data for one or more specified purposes;
- 9 (2) (b) – processing is necessary for the purposes of carrying out the **obligations** and exercising specific rights of the controller or the data subject in the field of employment and social security for appropriate safeguards;
- 9 (2) (c) – processing is necessary to protect the **vital interest** of data subject or other natural persons where the data subject is physically or legally incapable of giving consent;
- 9 (2) (d) – processing is carried out in the course of **legitimate activities**,

including not for profit organisations, with appropriate safeguards and on condition that it will not be disclosed without the consent of the data subjects;

- 9 (2) (e) – processing relates to personal data which are **manifestly made public** by the data subject;
- 9 (2) (f) – processing is necessary for the **establishment, exercise or defence of legal** claims or whenever courts are acting in their judicial capacity;
- 9 (2) (g) – processing is necessary for reasons of substantial public interest, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- 9 (2) (h) – processing is necessary for the purposes of **preventative or occupational medicine** for the assessment of the working capacity of the employee;
- 9 (2) (i) – processing is necessary for reasons of **public interest in the area of public health**, protecting against threats to health;
- 9 (2) (j) – processing is necessary for archiving purposes in the public interest, scientific, historical, statistical research/purposes in accordance with Article 89(1).

17. Contact Details

Any questions regarding this policy or data protection matters should be directed to:

Data Protection Lead:

[Victoria Lee]

Email:

[Victoria.lee@eastcoastvets.ie]

Telephone:

[07447 416385]

Address:

[East Coast Vets, 32 Beechwood Close, Boghall Road, Bray Co Wicklow, A98 DA39]

Version Control

Policy Owner: SMT

Version: 1.0

Effective Date: [16.06.2026]

Review Date: [16.06.2027]

Document Change History

Date	Version	Status	Author	Details of Change
16.06.2026	0.1	Draft	Victoria Lee – Data Protection Lead/Privacy Officer	Original Policy inserted within the employee handbook. Policy has been completely reviewed.