# POLYGON DATA PROTECTION POLICY

# Document Control

## Document Storage

**Document Title** Polygon Data Protection Policy
**Document Location** Intranet

## Version History

| Version No | Version Date | Author | Summary of Changes |
|---|---|---|---|
| 1.0 | 21/10/2017 | Andy Clark | First Issue |
| 1.1 | 27/12/2018 | Andy Clark | Annual Review |
| 1.2 | 16/12/2019 | Andy Clark | Annual Review |
| 1.3 | 12/01/2021 | Andy Clark | Annual Review |
| 1.4 | 20/04/2021 | Andy Clark | Additional review |
| 1.5 | 05/01/2022 | Andy Clark | Annual Review |
| 1.6 | 09/01/2023 | Andy Clark | Annual Review |
| 1.7 | 03/01/2024 | Andy Clark | Annual Review |
| 1.8 | 03/01/2024 | Andy Clark | Added customer feedback |
| 1.9 | 08/01/2025 | Andy Clark | Annual Review |

## Approvals

| Name | Title | Date of Approval | Version No |
|---|---|---|---|
| Andy Clark | IT Service Delivery Manager | 08/01/2025 | 1.9 |

## Distribution

| Name | Title | Date of Issue | Version No |
|---|---|---|---|
| Everyone | Intranet | 08/01/2025 | 1.9 |

# Table of Contents

## 1. Introduction

This policy sets out how we seek to protect personal data and ensure that all stakeholders understand the rules governing their use of personal data to which they have access in the course of their work. This policy requires staff to ensure that the Data Protection Officer (DPO) is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

## 2. Definitions

| | |
|---|---|
| Business purposes | The purposes for which personal data may be used by us:<br><br>Personnel, administrative, financial, regulatory, payroll, business development and claim administration purposes.<br><br>Business purposes include the following:<br>• Compliance with our legal, regulatory and corporate governance obligations and good practice<br>• Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests<br>• Ensuring business policies are adhered to (such as policies covering email and internet use)<br>• Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting.<br>• Investigating complaints<br>• Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments.<br>• Monitoring staff conduct, disciplinary matters.<br>• Marketing our business<br>• Improving services |
| Personal data | Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, customers, policyholders, suppliers and marketing contacts.<br><br>Personal data we gather may include individuals' contact and claim administration details, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV. |
| Sensitive personal data | Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy. |

## 3. Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms. This policy supplements our other company policies. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be available to staff via the intranet before being adopted.

For the avoidance of doubt, this policy includes all the Polygon companies and subsidiaries bought into the group from mergers and acquisitions.

## 4. Who is responsible for this policy?

Our Data Protection Officer has overall responsibility for the day-to-day implementation of this policy.

## 5. Data Protection Responsibilities

### 5.1. Responsibilities of the Data Protection Officer

- Keeping the Senior Management Team updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis
- Answering questions on data protection from staff, Senior Management Team members and other stakeholders
- Responding to individuals such as customers and employees who wish to know which data is being held on them.
- Complying with requests from Data Subjects

### 5.2. Responsibilities of the IT Service Delivery Manager

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Researching third-party services, such as cloud services the company is considering using to store or process data.

### 5.3. Responsibilities of the HR Director

- Making sure that training has been carried out in accordance with the internal training framework.

### 5.4. Responsibilities of the Commercial Operations Director

- Approving data protection statements attached to emails and other externally facing media.
- Ensure that Heads of Departments comply with customers reasonable requirements for records and data management including maintaining records of data lineage within their areas of responsibility.
- Addressing data protection queries from customers
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy
- Working with the Supplier Management Team to check and approve third parties that handle the company's data.

## 6. The Seven Key Principles of Data Protection

Personal data at Polygon shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency);

- 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 ('purpose limitation').

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 ('storage limitation');

- 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 ('integrity and confidentiality')."

  In addition:

- The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

## 7. Data Processing Activities

### 7.1. Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. The processing of all data must only happen when:

- It is necessary to deliver our services.
- There is an established legitimate interest, legal obligation or consent is given, and it will not unduly prejudice the individual's privacy.

In most cases this provision will apply to routine business data processing activities.

We will ensure any use of personal data is justified using at least one of the six conditions for processing and this will be specifically documented. All staff 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. We will occasionally process personal data which requires the consent of the data subject such as for employer/employee data. If you are in doubt about which condition needs to exist for the processing, please consult the DPO.

### 7.2. Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

## 8. Obtaining Personal data

Personal data may be obtained from a customer in the case of an insurance claim, or it may be obtained directly from an individual (data subject) for a private job. You must take reasonable steps to ensure that personal data you process is accurate, recorded in the correct field in our systems, and updated as required.

## 9. Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

### 9.1. Processing data securely

- Please consider not printing data at all and if you do print, when the print is no longer needed it should be shredded straight away.
- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it – remember your “Clear Desk Policy”.
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used and their contents should also be password protected.
- The DPO must approve any “cloud” based data storage.
- Servers containing personal data must be kept in a secure location, away from general office space.
- All servers containing sensitive data must be approved and protected by security software and a strong firewall.
- Personal and/or sensitive information must not be sent in unencrypted emails. Instead consider sending a link to a location where the information is securely stored.
- Data should never be saved directly to devices such as PC’s laptops, tablets or smartphones, instead please store the information in OneDrive. Where it is necessary, please minimize the amount of personal data you are saving so that a person cannot be identified from it. In the rare circumstances where data is kept on such devices it

must be securely backed up at least weekly.

## 10. Data retention

We must not retain personal data for longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

## 11. Subject Access Requests

If you receive a subject access request, you should refer that request immediately to the DPO. You should note that there are restrictions on the information which can be given out to protect other individual's privacy.

A Subject Access Request is free for the Data Subject. You will need to verify the identity of the Data Subject in the normal way that we do for all contact with our customers.

### 11.1. Data portability

When a data subject access request is received, the data must be 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.

### 11.2. Right to be forgotten

A data subject 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 be refused in some circumstances if the lawful reason for processing the data is not consent, and that there is still a lawful reason to process the data – please also refer these requests to the DPO.

### 11.3. Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed. When we provide services for an insurance policyholder, this does not constitute a business relationship, and we must not market directly to such individuals.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

## 12. Training

All staff will receive training on data protection when they join Polygon, which will be refreshed at least annually. New joiners will receive training as part of the induction process. Further training will be provided whenever there is a substantial change in the law or our policy and procedure.

It will cover:

- The law relating to data protection.
- Our data protection and related policies and procedures.

Completion of training is compulsory, and you will be asked to complete a test upon completion.

## 13. Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- Identity and contact details of any data controllers.
- Details of transfers to third country and safeguards
- Retention period

## 14. Criminal record or financial background checks

Any criminal record or financial background checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

## 15. Privacy by design and default

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Heads of Departments are responsible for conducting Privacy Impact Assessments and ensuring that all 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.

## 16. International data transfers

No data may be transferred outside of the EEA without first discussing it with the Data Protection Officer.

## 17. 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.

Please refer to our Reporting Information Security Incidents Policy for full details.

## 18. Complaints from Supervisory Authorities (SA)

If Polygon receives a complaint from the Information Commissioners' Office (ICO) who is the Supervisory Authority in the UK, the person who receives the complaint must immediately pass this complaint to the DPO.

The DPO will:

- Investigate the matter and determine whether the matter is an area where Polygon is the Controller or the Processor.
- If the area of complaint is a matter where Polygon is the Controller, then the DPO will liaise with the Senior Management Team of Polygon and the SA to resolve the issue.
- If the area of complaint is a matter where Polygon is the Processor, then the DPO will liaise with the Senior Management Team of Polygon and the Controller to resolve the issue.
- Follow the process outlined in the Reporting Information Security Incidents Policy
- Report personal data incidents / breaches to the Customer, via the Customer's Supplier Manager, as soon as Polygon becomes aware of them and no more than 24 hours after identification or in line with agreed contractual obligations.
- Polygon will ensure complaints received from Supervisory Authorities and non-profit bodies, organisations or associations, whose statutory objectives are in the public interest, are forwarded to the Customer's Supplier Manager without delay and no more than 24 hours after receipt or in line with agreed contractual obligations. Polygon will assist the Customer, as necessary, in investigating and drafting any response to data privacy complaints received from Supervisory Authorities and non-profit bodies, organisations or associations, whose statutory objectives are in the public interest

## 19. Monitoring

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

## 20. Consequences of failing to comply.

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

## 21. Policy review

The policy will be reviewed at least annually by the Data Protection Officer. It will also be reviewed in response to changes in relevant legislation, contractual arrangements, good practice or in response to an identified failing in its effectiveness.