Data Protection Policy All Services

Reviewed: September 2024

The Polaris Community processes a high volume of personal data relating to its workforce and stakeholders (known collectively as data subjects). External third parties may also process personal data on behalf of Polaris. Polaris has a legal duty under data protection law to ensure the privacy of all data subjects by ensuring that their personal data is protected against unauthorised or unlawful processing and against accidental disclosure, loss, destruction or damage. All individuals and organisations who process personal data for or on behalf of Polaris are expected to comply with the Polaris data protection policy and relevant security policies and procedures.

Introduction

This policy sets out Polaris commitment to achieving good practice in the safe management of the services we provide in order to minimise potential breaches of information and ensure that all personal and sensitive information (also known as personal data) we hold relating to children, foster parents/carers, adopters, applicants, service users, care receivers, pupils, workforce, visitors, stakeholders and other connected people is collected, processed, transferred, stored and disposed is in accordance with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

All personal information will be processed in accordance with the six 'Data Protection Principles'. Personal data must be:

1. Processed lawfully and fairly.
2. Collected for specified, explicit and legitimate purposes.
3. Adequate, relevant and not excessive.
4. Accurate and kept up -to-date.
5. Kept for no longer than is necessary.
6. Processed in a secure manner.

Polaris is committed not only to the letter of the law, but also to the spirit of the law, and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

In many circumstances, Polaris acts as the Data Controller in terms of the records we process. A Data Controller is the main decision maker and they exercise overall control over the purposes and means of the processing of personal data. In other instances Polaris will act as the Data Processor whereby the information is controlled by another person or organisation (such as Local Authorities, Health Care, statutory bodies, MOD etc.) and we process the information on their instructions. Polaris and all companies within the Polaris community are registered as a Data Controller with the ICO.

This policy applies to all individuals and organisations who process personal data for or on behalf of Polaris. This includes the workforce (i.e. employees, casual workers, agency workers, independent work workers and contractors), stakeholders (such as foster parents/carers) as well as external third parties (e.g. suppliers to Polaris such as auditors, insurers and training providers).

Each individual who completes work on behalf of Polaris is responsible for the information they collect and process and accordingly could be held responsible for any breach or misuse of data. Where any suspected breach of data protection policy occurs, all individuals share the obligation to inform the Data Protection Officer as a matter of urgency together with their line manager. All individuals should be aware that non-compliance with this policy could result in disciplinary action.

Definitions

Personal Data - is any information that relates to a living person who can be directly or indirectly identified from that information. This can include name, address, date of birth, an identification number, online identifier (eg. username) or anything specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person. It also includes any expression of opinion about that person. UK GDPR does not include anonymised data ie. where all identifying particulars have been removed and you cannot be personally identified.

Special Category Data - is a type of personal data which is more sensitive than other personal data and which therefore requires additional protection. Special category data includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics or biometric data, health (physical or mental), sex life and sexual orientation, criminal

NB/ personal and special category data are collectively referred to as "personal data" in the rest of this document unless specified otherwise.

Processing - means the collection, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying of personal data. Processing can be automated or manual.

Data Controller - a person or organisation who (either alone or jointly with another person/organisation) determines the purposes and manner in which any personal data is processed.

Data Processor - a person or organisation who processes personal data on behalf and instruction of the Data Controller.

Data Breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Responsibilities

Data Protection Officer

Polaris has appointed a Data Protection Officer (DPO) who can be contacted at DPO@polariscommunity.co.uk. The DPO is responsible for advising on all elements of this policy; monitoring and maintaining compliance with Data Protection Law and appropriate data protection registers and ICO memberships; championing privacy best practice; ensuring all staff are trained and aware of their responsibilities; developing related polices and guidelines to safeguard and mitigate any risks to the rights and interests of data subjects.

The DPO also provides advice and guidance on actions and responses for subject access requests, data breaches and Data Protection Impact Assessments (DPIA). They are also the point of contact for individuals about issues relating to the processing of personal information and for the Information Commissioners Office (ICO). The DPO is responsible for the timely reporting of any notifiable data breaches to the ICO that meet relevant thresholds under the UK GDPR.

Chief Executive Officer (CEO)

The CEO has overall responsibility and accountability for ensuring that Polaris complies with all relevant data protection obligations, including data quality, records management, ensuring compliance with all relevant legislation and privacy laws, risk management, incident management

and information assets. Whilst responsibilities can be delegated, accountability cannot be delegated and remains with the CEO.

Senior Information Risk Owners (SIRO)
The Senior Information Risk Owners (SIRO) have a key role in maintaining and promoting a positive culture of information risk management at the highest levels within Polaris. Because of this, the SIROs are at executive level (Directors) and report directly to the Chief Executive Officer. They are responsible for leading, escalating and resolving information risk matters and investigations.

Line Managers
All senior managers have an extremely important role for ensuring and promoting good practice in the safe management of personal information. They are responsible for the implementation of this policy and ensuring compliance with data protection principles within their teams. They will: support incident Standards investigations; ensure subject access requests and data breaches are addressed and recorded promptly and correctly; identify and address any training or additional training needs within their teams; report any incidents of non-compliance to the SIRO and DPO; ensure all access rights for theirs teams are correct and closed swiftly when any individual leaves; ensure that data protection is routinely discussed at team meetings in order to raise awareness of responsibilities which allows for questions and support.

Workforce
Every individual responsible for using personal data has a responsibility under UK GDPR to ensure it is collected and processed fairly and lawfully. Any individual who completes work for or on behalf of Polaris must do so in accordance with this Policy and must only access and process personal information that is relevant for them to perform their assigned roles and duties.

Other responsibilities and obligations include:

- Raising any concerns with their line manager or DPO if they become aware that this policy is not being followed;
  iInforming Polaris of any changes to personal data;
- reading and understanding any policies and procedures relevant to their role;
- reporting any data breaches swiftly;
- complete all relevant mandatory training promptly or raise if additional training or support is needed to understand their responsibilities under UK GDPR.

Data Protection Principle 1: Lawfulness, Fairness and Transparency

Collecting Personal Information
Polaris will only processes personal information where the law permits it. This is known as the legal basis for processing and there are 6 lawful bases (legal reasons):

- Consent – the data subject has given specific consent to process their personal information, e.g. in the course of subscribing to Polaris newsletters, completing surveys, signing-up to events or creating an online account via our websites;
- contract – is necessary to fulfil a contract or relationship we have with the data subject, or they have asked us to take specific steps before entering into a contract;
- legitimate Interest - where we, or a third party, have a legitimate interest in processing the personal information. A legitimate interest is where the processing of personal information is necessary to pursue legal or commercial interests in a way which is reasonably expected

as part of running a business, but which is not detrimental to the fundamental rights and freedoms of the data subject and would have a minimal impact on their privacy;
- public interest – is necessary to carry out a task or exercise a duty in the public interest
- legal obligation – is necessary to comply with legal or regulatory obligations;
- vital interest - processing is necessary in order to protect the vital interests of a data subject or another natural person and generally applies to matters of life and death Polaris may process personal data for more than one lawful ground depending on the specific purpose for which we are using the information.

Data Protection Principle 2, 3 and 4: Specified, Relevant and Accurate

Processing Personal Information

Specified - Polaris will only collect personal data for specified, explicit and legitimate reasons. These reasons will be explained to data subjects when we first start to collect their data and is covered in the Polaris Privacy Notice and specific service branded privacy policies which are published and linked on all the Polaris company websites.

Workforce, stakeholders and third parties must only process personal data where it is necessary in order to administer their roles. When personal data is no longer needed they must ensure it is deleted or anonymised. This will be done in accordance with the statutory regulations with which each service is registered.

Relevant - Polaris will only use personal data for the purposes for which it was collected, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use personal data for an unrelated purpose, we will notify the data subject and will explain the legal basis which allows us to do so or seek consent where necessary. There may be times, where required or permitted by law, that Polaris processes personal data without the data subject's knowledge or consent.

Accurate – Polaris will ensure that all personal information collected, processed and stored remains accurate and up-to-date. Information will be checked when it is collected and at regular intervals/auditing and will be corrected where appropriate.

Data Protection Principle 5: Kept For No Longer Than Necessary

Data Retention

Polaris will not keep personal information for any longer than for the purpose for which it was collected and processed, and in accordance with applicable law and regulations. Retention periods vary depending on the nature and context of the personal information and are based on the following criteria:

- For as long as we have reasonable business needs, such as managing our relationship with the data subject, and will only be as long as necessary to fulfil the purposes we collected it for;
- for as long as someone could bring a claim against us;
- retention periods in line with legal and regulatory requirements or guidance.

Personal information that is no longer required will be disposed of securely in accordance with Polaris processes. Where we use third parties to safely dispose of records on Polaris' behalf we require these third parties to provide sufficient guarantees that it complies with Data Protection law.

Data Protection Principle 6: Processed in a Secure Manner

Data Security
Polaris is committed to the effective security of its people, equipment, offices and information. It has security measures in place to keep personal data safe and prevent it from being accidently or unlawfully lost, used or accessed in an unauthorised or unlawful way, altered, disclosed or damaged. In addition, personal data (and other non-personal data) is protected by the cyber security measures put in place, and Polaris is Cyber Essentials and Cyber Essentials Plus certified.

Polaris limits access to personal data to those employees, agents, contractors and other third parties who have a business need to know only. They will only process personal information on our instructions, and are subject data protection law and confidentiality.

Polaris requires all third party service providers and other entities in the organisation to respect the security of personal data. Polaris will only share personal information where it is allowed or required by law, where it is necessary to administer the relationships with data subjects or where we have a Page 7 ©Copyright Polaris – produced by Polaris Standards legitimate interest to do so. We do not allow third party service providers to use personal data for their own purposes and we only permit them to process personal data for specified purposes and in accordance with our instructions and agreements.

Third parties we may share with include:

- **IT** - such as other companies in our group and other service providers who support our website, IT and system administration services and reporting activities.

- **Advisors** - such as professional advisers, including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.

- **Authorities** - such as HM Customs & Excise, regulators, police and government bodies, or to otherwise comply with the law and other authorities who require reporting of processing activities.

- **Partnering Organisations** - who assist us to provide or improve our services (e.g. by analysing and modelling statistics/data).

When doing this, Polaris will only appoint suppliers or contractors which can provide sufficient guarantees that they comply with Data Protection Law and we establish data sharing agreements where needed.

Polaris may also, at times need to share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our children, service users or workforce.

Polaris expects all who undertake work on its behalf to use systems, equipment and data in an appropriate and responsible way and must observe the guidance and guidelines as detailed in the Polaris IT associated policies and procedures to ensure usage is appropriate, ethical and lawful.

Data Subject Rights in Connection With Personal Information

Data protection law gives data subjects certain rights in respect of their personal data. Data subjects have the following rights:

- **Right to be informed about the collection and processing of their personal information.** This is covered in the Polaris Privacy Notice and specific service branded privacy policies which are published and linked on all the Polaris company websites.

- **Right to request access to your personal data** (commonly known as a "Subject Access Request). This enables data subjects to receive a copy of the personal data we hold about them and to check that we are lawfully processing it.

- **Right to request correction of the personal data** that we hold about them. This enables data subjects to have any incomplete or inaccurate data we hold corrected, however we may need to verify the accuracy of the new data provided.

- **Right to request erasure of the personal data** which enables data subjects to request deletion or removal of personal data where we no longer have a reason to process it or it is different to the purposes for which we originally collected it. However, we may not always be able to comply with this request of erasure dependent on specific legal or regulatory reasons.

- **Right to object to processing of the personal data** where we are relying on a legitimate interest (or those of a third party), and there is something about a data subject's particular situation which they believe impacts on their fundamental rights and freedoms. However this may be overridden where we can demonstrate we have compelling legitimate grounds to process the information which overrides their rights and freedoms. They also have the right to object where we are processing their personal data for direct marketing purposes.

- **Right to request restriction of processing of their personal data** which enables data subject's to ask us to suspend the processing of their personal data in the following scenarios: (a) they want to establish the data's accuracy; (b) where the use of the data is unlawful but they do not want us to erase it; (c) where they need us to hold the data even if we no longer require it as they need it to establish, exercise or defend legal claims; or (d) they have objected to our use of the data but we need to verify whether we have overriding legitimate grounds to use it.

- **Right to request the transfer of your personal data** which enables the data subject or their nominated third party to receive personal data that they have provided to us in a structured, commonly used and machine readable format.

- **Rights related to automated decision making including profiling** which enables the data subject to object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement) that might negatively affect them). However Polaris does not envisage that any decisions relating to individuals will be made via automated decision-making, including profiling.

All requests should normally be actioned within one calendar month. However, in exceptional circumstances this could be extended for up to a further two months and should be discussed with the Data Protection Officer.

Some of these rights are not absolute and therefore will not automatically apply when a data subject seeks to exercise their rights. Polaris will give written reasons it they believe that any given right does not apply.

Consent
In addition to the above rights individuals also have the right to withdraw their consent to processing at any time where we are relying on consent only to process their personal information. However, this will not affect the lawfulness of any processing carried out before consent was withdrawn. NB/ this will not apply where there is another legal basis or legitimate interest that overrides this consent.

Individuals should be encouraged, where possible, to submit any request to exercise their rights to the relevant manager of the service brand in the first instance and/or to the Polaris Data Protection Officer. If staff receive such a request directly, they must immediately inform and discuss with their line manager and/or Data Protection Officer and appropriate action will be agreed. All requests are to be recorded on the Incident Portal.

Refer to the Incident Reporting Procedure which outlines the process for the central reporting of incidents relating to key areas of the business. This reporting ensures appropriate incident management, risk mitigation and information analysis to minimise future risks.

Personal Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. This includes breaches that are the result of both accidental and deliberate cause.

- Examples of personal breaches can include:
- Sending personal data to an incorrect recipient
- Computer devices containing personal data being lost or stolen
- Alteration of personal data
- Access by an unauthorised third party
- Loss of availability of personal data (e.g. when it has been encrypted by ransomware or accidently lost or destroyed)

Each service brand will make all reasonable endeavours to reduce personal data breaches by minimising risks through good working practices as outlined in this Policy.

In the event of a suspected data breach, the following steps should be taken:

As soon as you suspect a breach of data protection has occurred immediately try to resolve/ reduce the impact of the breach eg. recall the email if it has been sent to an incorrect recipient, phone the recipient and ask them to delete etc.
You must notify your line manager and/or the Data Protection Officer as soon as possible, and details must also be recorded on the Incident Portal.

If there is a significant risk to people's rights and freedoms, the breach must be reported to the ICO without undue delay but not later than 72 hours after becoming aware of it. Failure to report within 72 hours must be explained to the ICO, and could result in a non-compliance and/or significant financial penalty. Reporting to the ICO is the responsibility of the DPO but in their absence will be the Senior Lead within the service brand.

Reporting a data breach as soon as it occurs will enable the correct advice to be given and appropriate action to be taken promptly. Effective management of such an incident can be vital in protecting Polaris against financial, reputational and legal risks, and as such, it is essential that all those who discover a potential breach adhere to the following:

- Collect as many details about the incident as possible including the time, how the incident occurred, and who was involved, including the number of individuals and any contact details. Whilst exact details available will vary according to circumstance, ensure all possible details are collected as soon as possible.

- Whilst collecting the above details, make a written note of any telephone calls received or discussions held about the incident, including the date and time of conversation.

- Report the incident immediately to your Line Manager and/or Data Protection Officer.

- The Data Protection Officer and relevant Senior Lead will agree a course of action and, if necessary, recommend that the Chief Executive Officer be informed.

- Report the incident on the Incident Portal.

- The severity of the incident will be assessed and, if necessary, a team will be identified who will be responsible for managing the incident. Precise membership may vary however a member of senior management will be required as the ultimate decision maker. The team must also have detailed knowledge as to any sector specific guidance as to the actions required in the event of a data protection breach.

The team will carry out the following:

- An investigation of the facts which will include the nature of the incident and the damage/harm that results or could result from the incident.

- Take action to ensure a further breach does not occur and mitigate the harm caused as a result and/or any harm that may continue to result from the incident.

- Determine the identity of the Data Controller for the purpose of the incident (which can often be the customer to whom services are being provided).

- Consider which parties need to be notified of the incident. If there is a risk to people's rights and freedoms and it meet's the threshold for reporting, then the Information Commissioner's Office (ICO) will need to be notified. Consideration should also be given as to whether or not a third party may notify the ICO of the incident.

- Other parties that need to be informed may include the individual(s) whose information was disclosed, Polaris customers and Polaris insurers.

- If the Data Controller is identified as a Polaris customer, the contract for services will be checked in order to safeguard against any potential claim for liability.

- An investigation into any individual(s) who caused the incident may need to be carried out in conjunction with HR to decide whether or not disciplinary action is appropriate and to ascertain produced by Polaris Standards whether levels of training and guidance given were adequate or further is needed.

- A full review as to whether or not appropriate policies and procedures were in place and were followed, and whether any action needs to be taken in order to raise data protection and security compliance awareness.

Subject Access Requests

Every individual has a right to make a 'subject access request' to gain access to their personal information and includes:

- Confirmation that their personal data is being processed;
- access to a copy of the data;
- the purposes of the data processing;
- the categories of personal data concerned;
- who the data has been, or will be, shared with;
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- the source of the data, if not the individual;
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject Access Requests should be submitted wherever possible in writing via email or letter, to ensure clarity of the request, to the manager of the service or to the Data Protection Officer. This should include:

- Name of individual;
- correspondence address;
- contact number and email address;
- details of the information requested.

Staff must follow the guidance set out in Subject Access Policy, Subject Access Procedure and SAR Glossary of Documents when receiving a SAR. The completion and discharge of a SAR is the responsibility of the service the data subject is associated with. Ultimate management responsibility for the SAR sits with the registered manager or locally nominated manager, Director or Head of Service or an appropriately delegated manager.

CCTV

Polaris uses CCTV in various locations and sites to ensure they remain safe and for certain safeguarding purposes. Polaris will adhere to the ICO's code of practice for the use of CCTV to ensure that individual's rights and privacy are protected.

Polaris does not need to ask an individual's permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by clear signs

explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the relevant manager of the service.

CCTV footage is subject to UK GDPR in the same way as personal information and will be processed in line with this Data Protection Policy.

Photographs and Video

Polaris and its service provisions may take photographs or record images of individuals undertaking different activities from time to time. Where this happens we will obtain consent from the individuals involved, whether they are an employee, a person we support or a care receiver. For children consent will be also gained from a birth parent, foster parent/carer or whoever has parental responsibility and we will clearly explain how the photograph will be used.

Uses may include:

- On Polaris or service-specific websites and social media pages;
- on notice boards and in company magazines, brochures, newsletters, etc;
- by external agencies such as the promotion, newspapers, campaigns.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will ensure that the photographs or video is deleted and not distributed any further.

Training

All staff are provided with data protection training as part of their induction process to ensure they are able to demonstrate competence in their understanding of relevant legislation and best practice. Data protection training is available via Learnative and is mandatory for all staff, as well as those who complete work on behalf of Polaris and should be monitored via the supervisory process.

Data protection also forms part of continuing professional development and refresher training, where changes to legislation, guidance or the organisation's processes make it necessary. Records of all training activities are held with Human Resources.

Data Protection by Design and Default / Data Protection Impact Assessments

Data Protection by Design and Default is a legal requirement to ensure that we have considered data protection and privacy issues into all of our processing activities and business practices from the design stage of any system, service or process, at every stage of planning and then throughout the lifecycle.

Article 25(3) of the Data Protection Act 2018
'The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed'

The Polaris change process is documented in the Polaris Group Business Management System ISO 9001:2015 and includes the requirement to identify changes that involve personal data and to ensure appropriate controls are in place.

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project and must be completed for any processing that is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA must:

- Describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals;
- identify any additional measures to mitigate those risks.

If you are planning a change which will impact personal data and are unsure if a DPIA should be completed, please consult the Data Protection Officer or Business Change Team.

Data Protection Principle 7: Accountability

UK GDPR requires organisations to put in place appropriate technical and organisational measures to demonstrate compliance with data protection law.

Polaris:

- Has appointed a Data Protection Officer;
- has produced clear, comprehensive data protection and data security policies and procedures;
- has produced a detailed Privacy Notice and service specific privacy policies which explains to data subjects how Polaris will process and protect their personal data;
- has implemented appropriate cyber and IT security measures and maintains external Cyber accreditations;
- conducts reviews and audits to test privacy measures and to ensure compliance;
- only process personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant Data Protection Law;
- ensures access to personal data is monitored and limited to those who have a business need to know only;
- implements data protection by design so as to pre-empt data protection breaches and using Data Protection Impact Assessments where appropriate;
- has written agreements, as appropriate, with external third parties who act in the capacities of Data Processors or Data Controllers and/or Joint Data Controllers;
- maintains records of processing activities;
- has a process for managing SAR and reporting data breaches;
- provides data protection training;
- uses retention schedules in line with applicable law and regulations.

Compliance/Monitoring

The Polaris Board and Senior Leadership Team have overall responsibility for ensuring that the organisation complies with all business and UK GDPR obligations. Every individual who completes work on behalf of Polaris will abide by this Data Protection Policy and other relevant security procedures to ensure any personal data they process is protected.

The Data Protection Officer will monitor and review compliance with this policy and is a member of the Polaris risk management team. The risk management team meet monthly, and this informs

compliance to the Senior Leadership Team and ultimately to the Polaris Board. Information reported can cover:

- Details of subject access requests;
- details of the exercise of other individual rights;
- completion/uptake of mandatory training on Learnative;
- breaches and the responses to each including ICO reporting;
- other contact with ICO;
- results of internal audits;
- results of cyber security testing.

Transferring Personal Data Overseas

Polaris does not envisage that personal data will be transferred outside of the UK or the EU. However if at any time this was necessary this would be in line with UK Data Protection Law where the UK government has decided the particular country or international organisation ensures an adequate level of protection of personal data (known as an 'Adequacy Decision').

Complaints about Data Processing

All data subjects have the right to make a complaint if they have concerns about how their personal information is being processed by Polaris. Complaints should be made directly to the manager of the relevant service brand in the first instance and will be handled in accordance with the Polaris complaints policies.

Should data subjects have concerns about how their complaint has been handled then they have the right to make a complaint directly to the Information Commissioner's Office (ICO) which is the UK supervisory authority for data protection issues (www.ico.org.uk).