

1.2. GDPR & privacy policy

introduction

The asphaleia Group are committed to protecting and respecting the privacy of individuals. We are committing to the Data Protection Act 2018 and GDPR compliance and implementation.

asphaleia operates management of data in consideration of values, human rights, and equal opportunities. Within departments we would seek staff to observe due consideration of people's personal data and sensitive personal data.

asphaleia is registered with ICO:

- asphaleia limited registration number: ZA351494
- asphaleia action registration number: Z8195576

asphaleia processes personal data and special category data (sensitive personal data) concerning individuals (Data Subjects) it works with, in order to perform its functions and to comply with its statutory duties. The categories in which data is processed can vary by service although they will be defined clearly within service contracts. Special categories of data include:

- Personal data revealing
 - Racial or ethnic origin
 - Political opinion
 - Religious or philosophical beliefs
 - Trade union membership
- Genetic data
- Biometric data (where used for identification purposes) e.g. health, sexual orientation

organisational practices

There are a number of policies which include practices that relate to data protection such as safeguarding policies, confidentiality/information sharing and DBS. This is not an exhaustive list, and this policy should be read in conjunction with all our policies which will have some reference to GDPR.

asphaleia believe that processes, routines and habits are central to quality and consistent management of confidential information. This can be encouraged by adopting simple practices such as closing files when leaving desks, switching computer screens off and holding conversations regarding individuals in appropriate locations.

The organisation has generic data protection practices in place. Individual ventures and projects may have additional practices which are necessary due to the nature of the service being delivered. As asphaleia offers a wide range of services, from consultancy to fostering, there are several different approaches to protecting personal information. This privacy statement broadly covers all asphaleia ventures. If more detailed information is required about a particular area, please contact asphaleia.

These practices sit under the organisation's controls to enable good data and information management as well as successfully enabling services to be effectively monitored. All staff will receive a level of GDPR and Data Protection training relevant and appropriate to their role. These practices are defined, agreed, and reviewed by the Leadership Team and the Data Protection Officer.

data protection principles

The Data Protection Law 2018 require the Company acting as either data controller or data processor to process data in accordance with the principles of data protection. These require that personal data is:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and kept up to date; every reasonable step must be taken to ensure that personal data is accurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept for no longer than is necessary for the purposes for which the personal data are processed
- 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
- The data controller shall be responsible for, and be able to demonstrate, compliance with the principles

legal bases for processing

The lawfulness of processing conditions for personal data are:

- Consent of the individual for one or more specific purposes
- Processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract
- Processing is necessary for compliance with a legal obligation that the controller is subject to
- Processing is necessary to protect the vital interests of the individual or another person
- 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 data controller
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedom of the individual which require protection of personal data, in particular where the individual is a child

The legal bases we rely upon are:

- Consent - asphaleia will ensure that all consents obtained are current, effectively managed with positive opt-in possibilities and that consents can be easily and clearly withdrawn upon request
- Legitimate interest
- Legal obligation
- Contractual obligation

privacy by design and by default

asphaleia has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all processing activities. This includes implementing measures such as:

- Data minimisation: not keeping data for longer than is necessary
- Pseudonymisation: processing of personal data in such a manner that the personal data can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable individual
- Anonymization: the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified
- Cyber security: ensuring electronic data is kept safe

collecting information from individuals

asphaleia obtain information about individuals by a variety of methods such as when people use our website to apply for a job, when people contact us about our services, when they make a donation or if they register to receive any information from asphaleia. In the case of sensitive information collected from service users, this data is collected in various ways e.g. referral forms.

type of information collected from individuals

Depending on the nature of the individual's relationship and/or contract with asphaleia, we may collect personal data and sensitive personal data from individuals.

staff records

Throughout employment and for as long a period as is necessary following the termination of employment, asphaleia will need to keep information referring to any staff employment, including recruitment and termination details.

These records may include:

- Information gathered about a member of staff and any references obtained during recruitment
- Details of terms of employment
- Payroll, tax and National Insurance information
- Performance information
- Details of specific job duties
- Health records
- Absence records, including holiday records and self-certification forms
- Details of any disciplinary investigations or allegations
- Training records
- Contact names and addresses
- Disclosures and DBS related information

- Correspondence with asphaleia and other information provided to asphaleia

This information is managed securely by the HR Department. Access to this information will be limited by asphaleia HR practices. Selected information will be made available on request by the Leadership Team.

All post-employment information is archived for two years. Subsequently, information is shredded and only information relevant to ongoing reference requests or of investigations for example will be maintained. asphaleia is committed to meeting equal opportunity obligations and to achieve this staff personal details will be collated and monitored to produce statistics. All information will be displayed anonymously.

service user records

Throughout engagement and for as long a period as is necessary following the termination of engagement, asphaleia will need to keep information referring to any service user's receipt of support, including recruitment and progression details.

These records may include:

- Information gathered about a service user and any references obtained during recruitment
- Details of terms of the service received
- Progression information
- Immigration information
- Health records
- Absence records
- Details of any investigations or allegations
- Educational achievements
- Contact names and addresses
- Correspondence with asphaleia and other information provided to asphaleia
- Child Protection files. If a service user is moving on to another educational establishment, then these files will go with them. We may also return any CP files to the Local Authority in keeping with our 'Keeping Children Safe in Education' obligation

This information is managed securely by the Leadership Team and/or Service Managers. Access to this information will be limited by asphaleia archive practices. Some contracts and specific user file information is the ownership of the individual/funder. In these cases, clarity will be sought regarding the retention of data information and archiving procedures.

All personal data gathered by asphaleia is kept in accordance with GDPR. All information is archived, and any service users can access at any point upon request. To maintain our funding, we are required to provide statistics to our funders, to prove we are reaching our targets. The information supplied will be in a cumulative manner and individuals may need to be identified. The information is kept depending on the specifications of the funder. Once the information is no longer required it will be securely destroyed.

data protection impact assessments (DPIA)

asphaleia will ensure, where special category or criminal data is processed, that;

- A DPIA for any high-risk data processing which includes special category and criminal data is carried out by the Data Protection Officer
- There is a record of this processing
- The DPIA is reviewed by the DPO on an annual basis or updated sooner if required

using information

asphaleia will only process necessary data and will only use data in ways relevant to carrying out its legitimate purposes and functions as an organisation in a way that is not prejudicial to the interests of individuals. asphaleia will take due care in the collection and storage of any data.

asphaleia may use information to:

- Process a donation that an individual has made
- Carry out our obligations arising from any contracts entered into by an individual and asphaleia
- Seek views or comments on the services asphaleia provide
- Notify individuals of changes to our services
- Send individuals communications which they have requested and that may be of interest to them. These may include information about campaigns, appeals or other fundraising activities
- Process a job application

data retention

asphaleia review our retention periods of personal information on a regular basis. We are legally required to hold some types of information to fulfil our statutory obligations. The information asphaleia use for marketing purposes will be kept with asphaleia until the individual notifies asphaleia that they no longer wish to receive this information. Job applicants are informed that their data will be held for 6 months after the recruitment process in case of dispute/complaints.

The duration that confidential data is stored for is defined by legislative, contractual and funding requirements for the type of data. This is broadly categorised into organisational, employee and service user data, and is retained for varying periods depending on the type of data.

information access and sharing

asphaleia will only share personal data with other organisations and third parties where the sharing is necessary to achieve a clear objective and it is fair and lawful to do so. asphaleia will not sell or rent information to third parties. asphaleia will not share information with third parties for marketing purposes. asphaleia staff will only have access to information dependent on their job role and function. See confidentiality and information sharing policy for further details.

third party service providers working on behalf of asphaleia

asphaleia may pass information to third-party service providers in certain circumstances and only where necessary (for example to process donations). In these cases, we disclose only the personal information that is necessary to deliver the service and not for direct marketing purposes.

When using our secure online donation pages, the donation is processed by a third-party payment processor, Virgin Money Giving, who specialise in the secure online capture and processing of credit/debit card transactions.

asphaleia may transfer personal information to a third party if we are under a duty to disclose or share the personal data in order to comply with any legal obligation, safeguarding of an individual or to prevent fraud/crime. However, asphaleia will take steps with the aim of ensuring that the privacy rights continue to be protected as much as possible.

your rights

Individuals have rights as a data subject. If they want to receive communications from asphaleia about the work we do then they can select their choices by ticking the relevant consent boxes on forms and the website. We will record their consent, including how they have given consent, when they gave consent and if there are any conditions attached to the consent.

asphaleia will not contact individuals for marketing purposes by email, phone, text message or post unless they have given prior consent. Marketing preferences can be changed at any time by contacting asphaleia and we will update the preferences without undue delay and without penalty.

Under the GDPR, individuals have the following rights:

1. The right to be informed – asphaleia will confirm what data we are processing and why, how long it will be retained and who it will be shared with
2. The right of access – Data subjects have a right to ask asphaleia what data is held relating to them as individuals. All data subject Access Requests (DSARs) will be processed by the Data Protection Officer without undue delay and recorded by asphaleia
3. The right to rectification – The accuracy of information is important to asphaleia. If any information asphaleia holds is inaccurate or out of date, please contact asphaleia and it will be duly corrected or deleted
4. The right to erasure – under certain circumstances, an individual can ask for their data to be deleted. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary for compliance with a legal obligation for example
5. The right to restrict processing – Data subjects have the right to request a temporary halt in the processing of their data i.e. where there is a legal dispute, where data is in the process of being corrected etc
6. The right to data portability – Data subjects have a right to have any data returned to them in a portable, easily readable, structured format
7. The right to object – Data subjects have the right to object to the processing of their data if it becomes inconsistent with the original primary purpose for which it was collected
8. Rights related to automated decision making and profiling - asphaleia do not use profiling and/or automated decision making.

If an individual wishes to raise a complaint on how asphaleia have handled their personal data, they can contact asphaleia to have the matter investigated. If the person is not satisfied with asphaleia's response or believe personal data has not been processed in accordance with the law, the complaint can be escalated to the Information Commissioner's Office via their website: <https://ico.org.uk/>

security precautions in place to protect the loss, misuse or alteration of information

When an individual gives asphaleia personal information, asphaleia takes steps to ensure that it is treated securely. For instance, any sensitive or personal information is encrypted before sending electronically. Non-sensitive details, e.g. email addresses, are transmitted normally over the internet, and this can never be guaranteed to be 100% secure. As a result, while asphaleia strive to protect personal information, there is no guarantee of the security of any information that is transmitted to asphaleia, and it is done at the individuals own risk. Once asphaleia receive information, every effort is made to ensure its security on asphaleia systems. Where asphaleia have given or where individuals have chosen a password which enables access to certain parts of asphaleia's website, the individual is responsible for keeping this password confidential. We ask that passwords are not shared with anyone.

asphaleia's ICT equipment and usage is governed by our Cyber Essentials accreditation; including adequate password complexity, all computers set up to include restricted administrator accounts, restricted users on local accounts, ensuring the most up to date version of software and applications is used, restrictions of third-party use accessing asphaleia networks to name a few compliance elements.

website

overview

This privacy policy notice is served by The asphaleia Group under the website www.asphaleia.co.uk. The purpose of this policy is to explain to how asphaleia control, process, handle and protect personal information through the business and while people browse or use the website. If individuals do not agree to the following policy, they may wish to cease viewing or using the website, and or refrain from submitting their personal data.

use of 'cookies'

The asphaleia website uses cookies. 'Cookies' are small pieces of information sent by an organisation to the computer accessing the website and stored on the hard drive to allow that website to recognise the person when they visit. Cookies collect statistical data about the browsing actions and patterns and do not identify an individual. This helps asphaleia to improve the website and deliver a more personalised service.

asphaleia will ask the user to consent to the use of cookies in accordance with the terms of this policy when they first visit the website. It is possible to switch off cookies by setting the browser preferences. Turning cookies off may result in a loss of functionality when using the website.

links to other websites

The asphaleia website may contain links to other websites run by other organisations. This privacy policy applies only to the asphaleia website, and encourage the users to read the privacy statements on the other websites when they visit. asphaleia cannot be responsible for the privacy policies and practices of other sites even if accessed using links from the asphaleia website.

In addition, if a user is linked to asphaleia's website from a third-party site, asphaleia cannot be responsible for the privacy policies and practices of the owners and operators of that third party site and recommend that the policy of that third party site is checked.

16 or under

asphaleia are concerned to protect the privacy of children aged 16 or under. If users are aged 16 or under, they should get their parent/guardian's permission beforehand whenever they provide asphaleia with personal information.

transferring information outside of Europe

As part of the services offered through asphaleia's website, the information which is provided may be transferred to countries outside the European Union ("EU"). By way of example, this may happen if any asphaleia's servers are from time to time located in a country outside of the

