1.2. data protection and GDPR policy

introduction

The asphaleia Group are committed to protecting and respecting the privacy of individuals. We are committed to the Data Protection Act 2018 and GDPR compliance and meet the requirements of the Protection of Freedoms Act 2012.

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

asphaleia is registered with the ICO as a data controller:

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

This policy applies to all personal data, regardless of whether it is in paper or electronic form.

For the purposes of this policy the following definitions are used.

term	definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individuals name and/or include factors specific to the individuals physical, physiological, genetic, mental, economic, cultural or social identity
Special categories of personal data	Personal data, which is more sensitive, including information above an individuals race, ethnic origin, political views, religion or philosophical beliefs, genetics, biometrics, health or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying
Data subject	The identified or identifiable individual whose personal data is held of processed
Data controller	A person or organisation that determines the purposes and the means of processing personal data
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data

organisational practices

GDPR is based on data protection principles that asphaleia comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how asphaleia will comply with these principles.

collecting personal data
asphaleia will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that asphaleia can fulfil a contract with the individual, or the individual has asked asphaleia to take specific steps before entering into a contract
- The data needs to be processed so that asphaleia can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that asphaleia can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of asphaleia or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a service user) has freely given clear consent

For special categories of personal data, asphaleia will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

limitation, minimisation and accuracy
asphaleia will only collect personal data for specified, explicit and legitimate reasons. These reasons will be explained to the individuals when the data is first collected.

If asphaleia want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with asphaleia's document retention policy.

sharing personal data
asphaleia will not normally share personal data with anyone else, but may do so where:

- There is a concern that puts the safety of staff or service users at risk
- We need to liaise with other agencies – asphaleia will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable asphaleia to provide services to our service users e.g. IT companies, external consultants. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, within our contractor agreements, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with asphaleia

asphaleia will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our services. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

subject access requests
Individuals have a right to make a 'subject access request' to gain access to personal information that asphaleia holds about them. This 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 if any significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the Leadership Team and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the Leadership Team and not share any information at this stage with the individual.

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent. The only except to this is the parent having a legal right to access to their child's education record.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children at asphaleia may not be granted without the express permission of the child. This is not a definitive rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

asphaleia provides commissioned services and may assist the funder with information related to subject access requests. The scope and nature of our duty to respond to these requests are detailed in the commissioned contracts.

responding to subject access requests
When responding to requests, asphaleia will:

- Ask the individual to provide 2 forms of identification
- Contact the individual via phone to confirm the request was made
- Respond within 1 month of receipt of the request
- In the majority of cases provide the information free of charge
- Tell the individual, asphaleia will comply within 3 months of receipt of the request. Where a request is complex or numerous, we will inform the individual of this within 1 month, and explain why an extension of time is necessary
- We will not disclose information if it:
    - Might cause serious harm to the physical or mental health of the individual or another individual
    - Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
    - Is contained in adoption or parental order records
    - Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, asphaleia may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. When asphaleia refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO if they wish.

other data protection rights of an individual
In addition to the right to make a subject access request, and to receive information when asphaleia are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask asphaleia to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing

- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Leadership Team. If staff receive such a request, they must immediately forward it to the Leadership Team and take no further action at this stage.

CCTV usage
asphaleia use CCTV in our premises to safeguard staff, service users and visitors. We adhere to the ICO's code of practice for the use of CCTV and complete DPIA's where required. See closed circuit television policy for more information.

photographs and videos
asphaleia may take photographs and record images of individuals within our settings for communication, marketing and promotional materials. We obtain written consent from all service users at the start of their time at asphaleia and will uphold any persons decision to withhold consent. Consent may be refused or withdrawn at any time.

When using photographs and videos for marketing and promotional materials asphaleia will not accompany them with any other personal information about the individual, to ensure they cannot be identified.

data security and storage of records
asphaleia will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept in a lockable cabinet when not in use
- Papers containing confidential personal data will not be left on desks, staffroom tables, pinned to noticeboards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing numbers, symbols and upper/lower case letters are used to access school computers, laptops and other electronic devices.
- Encryption software is used to protect highly confidential information being shared electronically
- Staff, are prohibited from storing personal information on their personal devices
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

disposal of records
Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely if asphaleia are not updating the information. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on asphaleia's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

personal data breaches
asphaleia will make all reasonable endeavours to ensure there are no personal data breaches. Such breaches may include but are not limited to:

- A non-anonymised dataset being published on our website which shows qualifications and/or progress of service users
- Safeguarding information being made available to an unauthorised person
- The theft of an asphaleia laptop containing non-encrypted personal data

In the unlikely event of a suspected data breach, asphaleia will follow the procedure set out below which is based on guidance by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Leadership Team
- The Leadership Team will nominate a Director to investigate the report and determine whether a breach has occurred. To decide, the Director will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Director will alert the Leadership Team and Service Managers as appropriate, of their findings
- The Director will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary
- The Director will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Director will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the Director will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual concerned

If it is likely that there will be a risk to people's rights and freedoms, the Director must notify the ICO.

- The Director will document the decision (either way), in case it is challenged at a later date by the ICO, or an individual affected by the breach. Documented decisions are stored within the incidents management and notification data

- Where the ICO must be notified, the Director will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Director will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
        - The name and contact details of the Director
        - A description of the likely consequences of the personal data breach
        - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the Director will report as much as they can within 72 hours. The report will document that there is a delay, the reasons why, and when the details are expected to be known and submitted

- The Director will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Director will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the Director
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual concerned

- The Director will notify any relevant third parties who can help mitigate the loss to the individual e.g. the police, insurers, banks or credit card companies

- The Director will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored within the incidents management and notification data.

- The Director and Managing Director will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error. Members of staff who receive personal data sent in error must alert the sender as soon as they become aware of the error.

In any cases where asphaleia staff have sent the information and the recall is unsuccessful, the staff member will contact the relevant unauthorised individual who received the email, explain that the information was sent in error, and request that those individuals delete the

information and do not share, publish, save or replicate it in any way. The staff member will ensure they receive a written response from all the individuals who received the data, confirming that they have complied with this request. The staff member will complete an incident report detailing their actions taken and confirmation that the information has been deleted.

asphaleia's website privacy policy

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 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 policies 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 EU. These countries may not have similar data protection laws to the UK. By submitting personal data, agreement is given for this transfer, storing or processing. If asphaleia transfer the information outside of the EU in this way, they will take steps to ensure that appropriate security measures are taken with the aim of ensuring that privacy rights continue to be protected as outlined in this policy.

If asphaleia services are used while outside the EU, the information may be transferred outside the EU in order to provide the user with those services.

our contact details
asphaleia Limited is registered in the UK under Company registration number 3865521. asphaleia Action is a registered Charity, registration number 1081728.