GDPR Policy

POLICY STATEMENT

Pendynas Ltd understands its obligations under the current Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 (GDPR). The Act regulates the use of personal data and this policy aims to inform anyone who comes into contact with data, within Pendynas Limited of their responsibilities, ensuring they adhere to the Act, minimising the risk of unintentional breaches.

PURPOSE AND SCOPE

Pendynas Ltd aims to ensure that all personal data collected about staff, young people, parents, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format. This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Student Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. **DATA PROTECTION DEFINITIONS**

Personal data

Any information relating to an identified, or living identifiable, individual. This may include the individual's:

- Name (including initials)
- Identification number
- Location data
- On-line identifier, such as a username

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories or personal data

Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Processing

Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data Subject

The identified or identifiable individual whose personal data is held or processed.

Data controller

A person or organisation that determines the purposes and the means of processing of 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 breech

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

THE DATA CONTROLLER

Pendynas Ltd processes personal data relating to parents, young people, staff, visitors and others, and therefore is a data controller.

ROLES AND RESPONSIBILITIES

This policy applies to Pendynas Ltd Directors, **all staff** employed by Pendynas Ltd, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

1. **Pendynas Ltd** will ensure that appropriate policies, procedures, systems and processes are in place and will ensure each hub adheres to the policies, procedures, systems and processes, to minimise the risk of a breach of the Act and the GDPR.
2. **The Directors** will monitor the implementation of this policy, with the DPO, to ensure it is implemented, monitored and reviewed effectively.
3. **The Hub managers** will act as representatives of the data controller on a day-to-day basis.
4. The **Data Protection Officer** (DPO) provides advice, guidance and expertise and is responsible for ensuring that staff are aware of the expectations surrounding data protection and the potential consequences should a breach occur. This involves overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. This will also include circulating appropriate policies, documentation and information to staff in relation to the Act.

   The DPO will log and report all data breaches to the Directors.

   The DPO is also the first point of contact for individuals whose data Pendynas Ltd process, and for the ICO.

   Pendynas Ltd DPO is **Clint Lanyon** and is contactable via: 01209 206379 or e-mail clanyon@pendynas.co.uk

5. **All Staff and Directors working on behalf of Pendynas Ltd** are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing Pendynas Ltd of any changes to their personal data, such as a change of address
- Compliance with the Pendynas Ltd privacy notice for both staff and students
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed o If they are unsure whether or not, they have a lawful basis to use personal data in a particular way
  - With any questions about the operation of this policy, data If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties
  - Ensuring contracts/agreements are in place with third parties where personal data is being shared

DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that Pendynas Ltd must 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 Pendynas Ltd aims to comply with these principles.

COLLECTING PERSONAL DATA

Lawfulness, fairness and transparency

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

- The data needs to be processed so that Pendynas Ltd can **fulfil a contract** with the individual, or the individual has asked Pendynas Ltd to take specific steps before entering into a contract
- The data needs to be processed so that Pendynas Ltd 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 Pendynas Ltd, as a public authority, 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 Pendynas Ltd, 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 young person) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a student) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a student) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified, adverse effects on them.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we 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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

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 the Pendynas Ltd Record Retention Schedule and any relevant laws or regulations

SHARING PERSONAL DATA

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any 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 us
    - Agree how long a third party will keep our data for and what process they have for destroying or transferring the data held at the end of the contract

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 young people or staff.

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 AND OTHER RIGHTS OF INDIVIDUALS

Subject access requests (Appendix 3)

Individuals have a right to make a 'subject access request' to gain access to personal information that Pendynas Ltd 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form to Pendynas Ltd, and we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request, they must immediately forward it to The Directors for logging.

Children and subject access requests

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.

Children below year 9 are generally not 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 students may be granted without the express permission of the student. Only subject access requests for data on a student in year 9 or above will require consent from the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay, and within 1 month of receipt of the request (or receipt of he additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we 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 the extension is necessary

We will not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the student 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
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we 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.

If a request is refused, the Directors will write to the individual to tell them why, advising them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Other data protection rights of the individual

In addition to the right to make a subject access request, and to receive information when we 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 us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

PARENTAL REQUESTS TO SEE THE EDUCATION RECORD

Parents, or those with parental responsibility, may request free access to their child's educational record (which includes most information about a student). Pendynas Ltd will provide this information within 15 school days of receipt of a written request.

BIOMETRIC RECOGNITION SYSTEMS

Where we use students' biometric data as part of an automated biometric recognition system, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. Pendynas Ltd will seek written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the biometric system(s). We will provide alternative means of accessing the relevant services.

Parents/carers and young people can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted. As required by law, if a young person refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members, or other adults, use the biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

CCTV

We use CCTV in various locations around our sites to ensure they remain safe. We will adhere to the ICO's code of practice and the Pendynas Ltd's CCTV policy for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV systems in Pendynas Ltd sites should be directed to the Hub Manager for the site.

PHOTOGRAPHS AND VIDEOS

As part of Pendynas Ltd activities, we may take photographs and record images of individuals within our hubs.

Pendynas Ltd will obtain written consent from parents/carers, or young people aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the young person how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at Pendynas Ltd events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other young people are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Uses may include:

- Within hubs on notice boards and in, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- On-line on our websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Child Protection Policy for more information on our use of photographs and videos.

DATA PROTECTION BY DESIGN AND DEFAULT

We have put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing 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
- Completing privacy impact assessments where Pendynas Ltd processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Hubs and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

DATA SECURITY AND STORAGE OF RECORDS

We 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 under lock and key when not in use
- Papers containing confidential personal data must not be left on office and work station desks, pinned to notice/display boards, or left anywhere else where there is general access

- Passwords that are at least eight characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Users are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, young people or Directors, who store personal information on their personal devices, are expected to follow the same security procedures as for Pendynas Ltd-owned equipment (see our ICT Acceptable Use Policy)
- 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, where we cannot or do not need to rectify or update it.

Destruction of confidential waste must be complete:

- Paper must be incinerated or shredded
- CD's can be cut up and disposed as per paper waste
- Destruction of electronic records, storage devices and tape must be by incineration or the use of a special equipment or software that will destroy the information

Confidential waste must be kept secure and protected against accidental loss, damage or unauthorised access up until its final destruction:

- Confidential waste should be kept separate from other waste material and confidential waste bins used where possible, otherwise waste should be bagged and clearly labelled "confidential waste"
- Only authorised personnel or an approved contractor should handle the waste
- Bagged waste awaiting collection must be kept secure at all times

PERSONAL DATA BREACHES

Pendynas Ltd will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a hub context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a Pendynas Ltd laptop containing non-encrypted personal data about a young person's **TRAINING**

All staff, and Directors are provided with data protection training as part of their induction process and they will continue to have on-going mandatory refresher training.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or Pendynas Ltd processes make it necessary.

MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF THIS POLICY

The DPO is responsible for monitoring and reviewing this policy.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO 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 DPO will alert the Directors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO and CEO will decide whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO 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(s) concerned

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

The DPO 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. The DPO will document breaches and outcome decisions which will be held centrally by the DPO for all the hubs within Pendynas Ltd.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO 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 DPO
- 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 DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

The DPO 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 DPO 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 DPO
- A description of the breach
- The reason why the breach has occurred
- 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(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO 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 on a centrally held record for all hubs within Pendynas Ltd
- The DPO and the Directors will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via e-mail 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 and the DPO as soon as they become aware of the error
- In cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the e-mail, 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 DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 2: Clear Desk Procedure

Confidential and sensitive information, whether held electronically or in paper format, must be secured appropriately when staff are absent from their workplace and at the end of each working day.

In order to ensure that this is applied across Pendynas Ltd, the procedure below is to be followed:

- Employees are required to ensure that all confidential and sensitive information in hardcopy or electronic form is secure in their work area at the end of the day or, if they leave their desk, at any point during the working day.
- To reduce the risk of a breach of confidentiality and to adhere to the Data Protection Act, confidential and sensitive documents, including person identifiable information, when no longer required, must be securely disposed of immediately.
- Computer desktops must be logged off or have a password locked screensaver when the employee is away from their work area.
- Filing cabinets, office cupboards or desk drawers must be kept closed and locked when not in use or unattended if they contain any confidential and sensitive information.
- Keys for locked areas must not be left unattended at the employee's work area. If the employee will be on annual leave or working outside the office, if appropriate, the keys should be left with a colleague in the same department or in a lockable key cabinet on site.
- When any confidential and sensitive information is requested over the phone, all employees must ensure they are speaking to the correct person to whom this information can be disclosed. This can be confirmed by calling the recipient back on a number that is already recorded or asking relevant questions to which the recipient would know the answer.
- Documents that contain confidential and sensitive information and which are being sent via e-mail must be encrypted (password protected). Employees must send a second e-mail to give the password once the document has been emailed across. The password must not be sent in the same e-mail as the document.
- Staff are encouraged not to store data locally on their device and if not based at their main place of working, to save data using the remote access.
- When saving confidential and sensitive information to SharePoint / Google Drive etc, it is the responsibility of the employee to check who has access to the file and ensure that the information is only shared with those authorised to access the information.

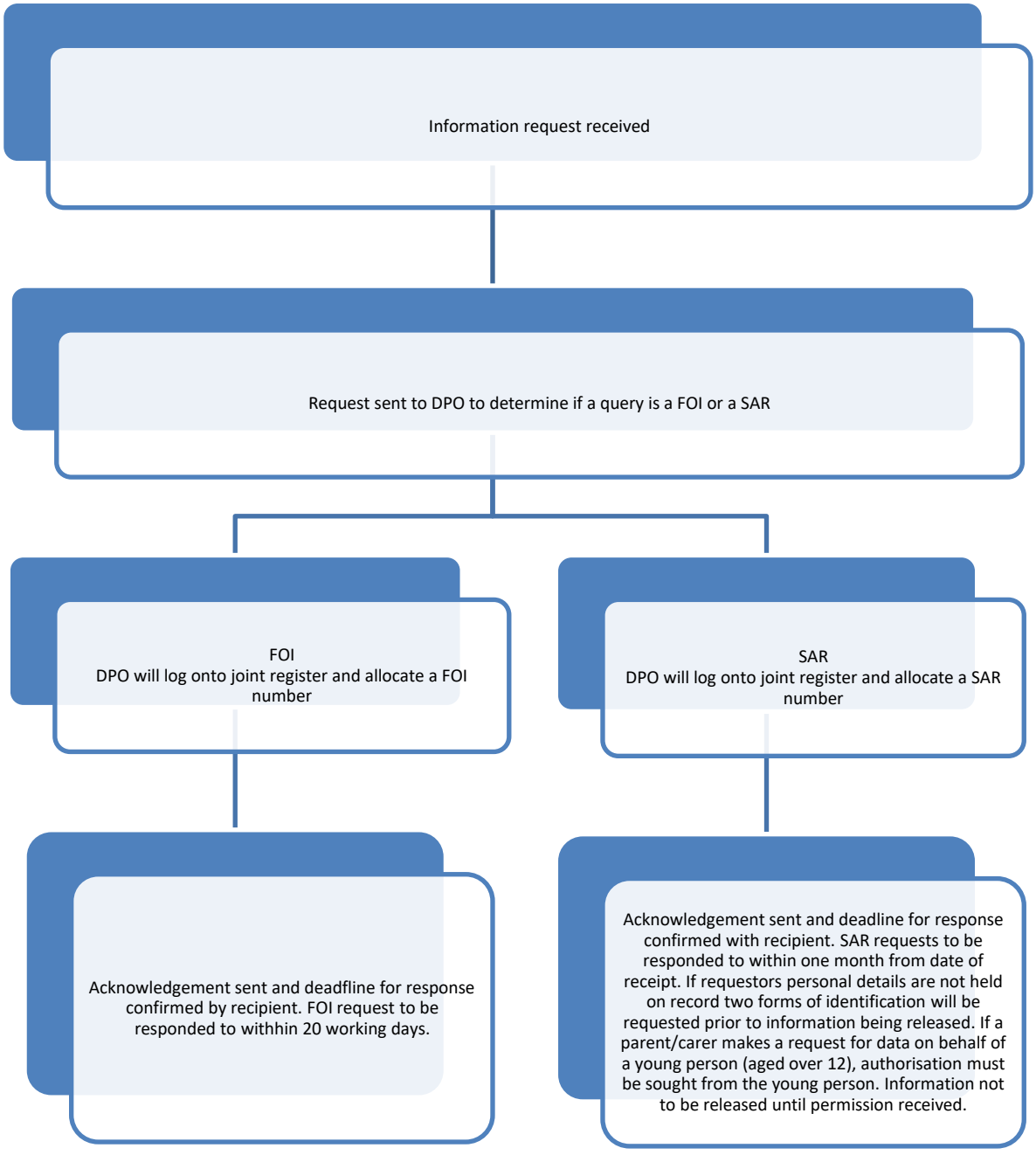
- No confidential or sensitive information is to be saved to USB drives or other external drives, even if the documents are encrypted (password protected). If there is a requirement for any of this information to be saved to external drives, the employee is required to obtain permission from the DPO before proceeding.
- All employees are advised to assess whether any confidential or sensitive information needs to be printed before doing so. If it is not required to print the information, Pendynas Ltd advises that the information is stored electronically. If printed, it must be stored securely and disposed of securely when no longer required.

Printers and Photocopiers

When sending scanned confidential or sensitive information from the printer to an e-mail address, all employees must send the documents from the printer to their work e-mail address and then forward on to the required person to ensure that only the correct recipient receives the information. It is not recommended that documents are scanned and sent from the printer to the recipient directly.

If it is necessary to copy any confidential or sensitive information, the employee must remain at the printer whilst the copy is being completed and ensure all copies are removed from the printing tray on completion.

Appendix 3: Subject Access Request and Freedom of Information Procedure



The DPO will ensure the staff member responsible for responding to requests has received a copy of information and is aware of deadlines

The DPO will ensure information is received prior to deadline and will collate a response. Full response checked by Directors prior to sending

DPO to send a final response once approved and update joint register. A full copy to be kept in the relevant FOI/SAR file