Govilon Activity Centre

DATA PROTECTION POLICY

Reviewed By: Jon Cholakian **Date:** 16th January 2019

General Data Protection Regulation (GDPR)

Our Commitment:

Govilon Activity Centre is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA).
https://ico.org.uk/for-organisations/guide-to-data-protection/data-protectionprinciples/

Changes to data protection legislation (GDPR May 2018) are being monitored and the Centre is working towards implementing these changes and a Data Protection review is to take place on 30th August 2018 in order to become compliant with all requirements.

The possible grounds for processing are:

- Consent - The member of staff/student/parent has given clear consent for The Centre to process their personal data for a specific purpose.
- Performance of a contract to which the data subject is party, or to take steps prior to entering into a contract at the request of the data subject
- Compliance with a legal obligation which the controller is bound to comply with
- Protection of the vital interests of the data subject or another natural person
- Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Legitimate interests pursued by the controller or a third party

For the last of these there is an exception where the interests in question are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This basis also has restrictions on its use in the public sector.

Where the basis for processing is a legal obligation, or a task carried out in the public interest, or exercise of official authority, then the parameters will be determined by EU law or domestic law of the relevant member state.

The members of staff responsible for data protection are Nick Fitzgerald (Centre Manager), Jonathan Cholakian (Deputy Centre Manager) and Joanna Phillips (Centre Administrator). However **all** staff must treat **all** student information in a confidential manner and follow the guidelines as set out in this document.

The Centre is also committed to ensuring that all staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by The Centre and any third party contracted to provide services within the Centre.

Notification:

Our data processing activities are registered with the Information Commissioner's Office – (Reg No 07E784A00109) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data:

All data within the Centre's control shall be identified as personal, sensitive or both, to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/

The principles of the Data Protection Act shall be applied to all data processed:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data longer than is necessary
- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and young people prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and-control/

There may be circumstances where the Centre is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Exam Boards, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.
The intention to share data relating to individuals or an organisation outside of The Centre shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

Under no circumstances will the Centre disclose information or data:

- That would cause serious harm to the child or anyone else's physical or mental health or condition
- Indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- Recorded by the student in an examination
- That would allow another person to be identified or identifies another person as the source, unless the person is an employee of the Centre or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent.
  The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- In the form of a reference given to any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

Remote Access to Computer Systems and Data

The maintenance of the Centre's computer network is managed by Melrose IT Solutions, solely by Glen Jones its Director. Mr Jones undertakes the maintenance of, and manages routine system & security updates remotely and on-site, on our behalf. He is an integral part of the Centre's data protection team and is approved by Centre management to undertake these tasks.

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact-assessments-code-published/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

Nick Fitzgerald (Data Protection Officer)
Centre Manager
Govilon Activity Centre
School Lane
Govilon
Abergavenny
Monmouthshire NP7 9RH

**No charge will be applied to process the request*

Personal data about young people will not be disclosed to third parties without the consent of the young person's parent or carer, unless it is obliged by law or in the best interest of the child.

Data may be disclosed to the following third parties **without** consent:

• **Examination Authorities** - This may be for registration purposes, to allow the pupils at our Centre to sit examinations set by external exam bodies.

• **Health Authorities** - As obliged under health legislation, the Centre may pass on information regarding the health of children in the Centre to monitor and avoid the spread of contagious diseases in the interest of public health.

• **Police and Courts** - If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

• **Social Workers and Support Agencies** - In order to protect or maintain the welfare of young people or vulnerable adults, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

• **Educational Division** – The Centre could potentially be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

• **Right to be Forgotten** – Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the Centre including any data held by contracted processors.

Photographs and Video:
Images of staff and young people may be captured at appropriate times and as part of educational activities for use in Centre only with prior consent from parents/Young people and accompanying staff.

Unless prior consent from parents/young people/staff has been given, the Centre shall not utilise such images for publication or communication to external sources.

It is the Centre's policy that external parties (including parents) will not capture images of staff or young people during such activities without prior consent.

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard.

Exceptions

1) A group photograph is routinely displayed on the wall at the centre, with consent from the school or organisation.
2) Medical information that may require immediate access during the Centre day. This will be carried by accompanying staff or trip leader at all times. This information will return back to the school or organisation on completion of the course.
   Medical information will only be held if related to an accident, incident or illness. The school or organisation or individual will be informed of this in writing.

Sensitive or personal information and data should not be removed from the Centre site, with the exception of medical forms carried on all activities and visits by accompanying staff as described above.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the Centre site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the Centre site, the information should not be on view in public places, or left unattended under any circumstances. The only exception to this is individual medical questionnaires as described above in 'Exceptions 2)'.

- Unwanted paper copies of data or sensitive information should be shredded. This also applies to handwritten notes if the notes reference any other staff member or young person by name.

- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

- If it is necessary to transport data away from the Centre, it should be downloaded onto a Centre USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB stick only.

- USB sticks that staff use must be password protected and stored securely in the Centre office when not in use.

- All unnecessary data stored on USB Sticks should be deleted as soon as practical

These guidelines are clearly communicated to all Centre staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:

The Centre recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

The Centre will dispose of IT assets & collections and sensitive data that is no longer required, as per the above recommendations.

Breach Reporting Policy:

In the event of a security breach and personal data becoming compromised, The Centre will immediately report details of the breach, along with the nature of any data known to be compromised, to the following bodies:- Govilon Management Committee, the School or Organisation whose data was affected, relevant Local Education Authority (LEA) and the Police, as necessary.

Business Continuity Plan:

Following a security breach, The Centre will remotely recover any lost personal data from its encrypted server, in order to resume normal business without delay.

Data Protection Policy

For all permanent staff, associate instructors, volunteers and external consultants who have access to data at Govilon Activity Centre.

I have read and understood the contents of the above document and agree to work to this policy and within the boundaries laid out in it.

I will act on all new entries made in the *"Revision Log"* on page 1 of the GOVILON ACTIVITY CENTRE Operating Procedure Document.

Name: _____

Signed: _____

Position: _____

Date: _____