Commonwealth Games England

Data Protection (Information Security) Policy

Introduction

In order to preserve the confidentiality, integrity and security of Commonwealth Games England's (CGE) information assets, CGE must ensure that all data items are suitably protected against unauthorised access, modification, loss or disclosure. Whilst this is critical for assets falling under the remit of the UK's suite of data protection legislation, the protection is also relevant for general information assets across CGE.

This policy describes how these assets, and other associated business data, must be handled and stored to meet the organisation's data protection standards and to comply with the law.

Policy scope

This policy applies to:

- The head office of CGE, and any permanent or temporary satellite offices, including home working.
- All employees of CGE, including volunteers and secondees
- All contractors, suppliers and other people working on behalf of CGE

It applies to all data that the organisation holds relating to identifiable individuals. This can include, but is not limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus, any other information relating to individuals

Why this policy exists

This data protection policy ensures that CGE:

- Complies with data protection law and follow good practice
- Protects the rights of employees, athletes, and other partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The suite of Data Protection laws in the UK describes how organisations – including CGE – must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The fundamental requirements of data protection are underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred to a country outside of the UK, unless that country or territory also ensures an adequate level of protection

Responsibilities

Everyone who works for or with CGE has some responsibility for ensuring data is collected, stored, and handled appropriately. Each operational team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. Failure to adhere to the requirements and stipulations of this (and all related) policies will be regarded as a breach of the organisation's rules and may result in disciplinary action up to and including action for gross misconduct in the most serious or repeated cases.

However, these people have specific, key areas of responsibility:

- The Board of Directors, supported by its operating committees, is ultimately responsible for ensuring that CGE meets its legal obligations and ensures that adequate resource is made available for the implementation of this policy.
- The Chief Executive is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues including current compliance checks.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Ensuring that the Group has in place an adequate and effective management structure with supporting policies and procedures to execute its responsibilities under data protection legislation and generally accepted good practices.
- The Chief Financial Officer is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from employees and anyone else covered by this policy.
    - Producing and updating the review schedule for all data protection related policies.
    - Checking and approving any contracts or agreements with third parties that may handle the organisation's sensitive data.

- Evaluating any third-party services which the organisation is considering using to store / process data or provide IT / infrastructure support.

(note that external advisers and specialists will be used as required to support the Chief Financial Officer in the execution of these responsibilities)

- The Head of Media and Communications is responsible for:
  - Where necessary, working with other employees to ensure marketing initiatives and activities abide by data protection principles and to ensure marketing databases are checked against industry suppression files every six months.

General employee guidelines

CGE will provide training to all employees to help them understand their responsibilities when handling data. The only people able to access data should be those who need it for their work.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- Always handle personal data in the manner that you would expect your own data to be handled.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- In particular, strong passwords must be used and they should never be shared.
- Passwords for systems access will be required to conform to a complexity requirement which will be managed by CGE's IT services partner.
- Personal data should not be disclosed to unauthorised people, either within the organisation or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the Chief Financial Officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Chief Financial Officer.

When data is stored on paper, either because it is an original document, or it is a printed copy of an electronic record, it should be kept in a secure place where unauthorised people cannot see it. Specifically:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them e.g. on a printer.
- Data printouts should be disposed of securely when no longer required using document shredders or a confidential waste disposal service.
- Wherever possible keep your desk and working area clean and clear of all paperwork which may contain personal data.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data access should be protected by strong passwords that are changed regularly and never shared between employees. The password policy will be enforced by CGE's IT services partner.
- If data is stored on removable media (USB drive or optical disk) these should be kept locked away securely when not being used. All files saved on removable media should have local passwords and encryption set. Do not store or send password information with the removable media.
- Data should only be stored on designated drives and should only be uploaded to an approved cloud computing services.
- Data should never be saved directly to laptops / PCs (other than to the local copy of OneDrive for Business) or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software controlled by the Group's IT services partner.

Data use

Personal data is of no value to CGE unless the business can make use of it. However, it is when personal data is processed that it can be at the greatest risk of loss, corruption or theft. As such CGE has adopted some simple risk reduction measures:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. It should never be sent by open email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The Chief Financial Officer can explain how to safely send data to authorised external contacts.
- Personal data should never be transferred outside of the UK without the implementation of adequate safeguards. All of CGE's data processing systems have this requirement built in by default.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires CGE to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Employees should not create any unnecessary additional data sets and should ensure that de-duplication processes are followed when new records are created.
- Employees should take every opportunity to ensure data is updated. For instance, by confirming a customer's / candidate's details when they call.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Disclosing data for other reasons

In certain circumstances, data protection legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, CGE will disclose the requested data. However, the Chief Financial Officer will ensure the request is legitimate, seeking assistance from the board and from the organisation's external advisers where necessary.

Providing information

CGE aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the organisation has a privacy policy, setting out how data relating to individuals is used by the organisation.

This is available on request, and a copy of the live document is also available on the CGE website.

Related documents

CGE maintains the following policies in order to have a comprehensive policy and management framework through which the Group ensures its compliance with the prevailing Data Protection legislation

- Legal Processing under UK GDPR statement
- Data Classification Policy
- Data Asset Register
- Data Breach Incident Management Policy
- Data Subjects' Rights Policy
- Privacy Policy / notice
- Cookie Policy / notice