Confidentiality and Data Protection Policy

October 2019

Document Control

Document Information

Document title:	Confidentiality and Data Protection Policy
Document author:	Data Protection Officer
Document reference number:	CPOL-LGL-005
Date reviewed by Senior Management Team:	5 November 2019
Date approved by OC Board	Not applicable
Date and outcome of Equality Impact Assessment:	1st October 2019 – Positive impacts noted for special category data which is also a protected characteristic
Date document issued:	29 November 2019
Review date, if applicable:	Not applicable
Target audience: (e.g. all staff)	**All staff are required to read this policy**
Subject area: (e.g. Finance, HR, Legal)	Legal

Version History

Version No	Lead	Date change implemented	Reason for change
1	Data Protection Officer	Not applicable	No change – new document

Consultation History

Position	Organisation
Chief Information Officer	Birmingham Organising Committee for the 2022 Commonwealth Games Limited
Chief Legal Officer	Birmingham Organising Committee for the 2022 Commonwealth Games Limited
Senior Enterprise Architect	Birmingham Organising Committee for the 2022 Commonwealth Games Limited

Contents

1. Introduction

1.1. Protecting confidential information is vital to the work of the Birmingham Organising Committee for the 2022 Commonwealth Games Limited (Birmingham 2022). If we fail to do this, the consequences of a confidentiality breach could be serious. A confidentiality breach could:

- result in harm to individuals whose personal data has been compromised;
- cause Birmingham 2022 to suffer reputational damage;
- result in the information Commissioner's Office taking action and fining the organisation up to up to 4% of annual global turnover or €20 million – whichever is greater; and
- result in criminal offences.

1.2. This policy is intended to provide some basic practical guidance on how individuals working for Birmingham 2022 can improve the security of the confidential data they handle and comply with the legislation relating to the use of personal data. This policy is not a definitive guide to confidentiality and information security, it should be read alongside all relevant Birmingham 2022 policies relating to information security.

2. Purpose

2.1. The purpose of this policy is to:

- detail what constitutes confidential information, including the various categories of confidential information; personal data, commercially sensitive data and security related data;
- set out Birmingham 2022's responsibilities in relation to the use of confidential information and ensure Birmingham 2022 remains compliant with legislative and government requirements for dealing with confidential information;
- provide information and guidance to those working for Birmingham 2022 on how to process the various types of confidential information;
- establish processes and practical safeguards to enable employees to manage and protect confidential information and prevent confidentiality breaches.

3. Scope

3.1. This policy applies to all persons working for Birmingham 2022, or on its behalf in any capacity, (this could include: employees, secondees, consultants, contractors etc.) It includes those who work at home or work remotely.

3.2. This policy covers confidential information held and processed by, or on behalf of Birmingham 2022. This includes personal data, commercially sensitive data and security related data, regardless of the format in which it is held. Such formats may include information held manually or on paper, information held electronically, held in a visual or audio format or held in the memory of an

employee. This policy also applies to all information systems managed by or used by Birmingham 2022.

3.3. This policy is available on SharePoint or can be sourced directly from the Data Protection Officer.

4. Responsibilities

4.1. The Chief Executive Officer of Birmingham 2022 has overall responsibility for ensuring the organisation complies with data protection legislation.

4.2. The Chief Information Officer is responsible for providing IT systems and applications that comply with NCSC security guidelines and which securely store and process organisational data.

4.3. The Senior Enterprise Architect is responsible for ensuring IT systems and applications are designed with IT security in mind and updated as necessary to comply with NCSC guidelines. He will also be the point of contact for dealing with queries and issues relating to security of core systems.

4.4. Birmingham 2022's Data Protection Officer has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, and for dealing with any queries and issues relating to data protection and confidentiality.

4.5. Managers at all levels of the organisation are responsible for ensuring those reporting to them understand and comply with this policy.

4.6. All employees permitted to access confidential information must ensure that they read, understand and comply with this policy. They must also undertake mandatory confidentiality training appropriate to their role.

4.7. All employees must notify the Data Protection Officer as soon as possible if they believe there has been a breach of this policy.

5. Confidential information

5.1. There are three distinct categories of confidential information with which employees at Birmingham 2022 may come into contact. These are:

- **personal data** (also includes special category data and criminal offence data)
- **commercially sensitive data**; and
- **security related data**

5.2. There are a number of legal and professional requirements that must be considered when dealing with confidential information, including:

- the General Data Protection Regulation (EU) 2016/679) (GDPR);

- the Data Protection Act 2018 (DPA 2018);
- the Privacy and Electronics Regulations (EC Directive) 2003 (PECR);
- the Human Rights Act 1998;
- the common law duty of confidentiality;
- the Computer Misuse Act 1990;
- Government Security Classifications, May 2018;
- National Cyber Security Centre guidelines.

6. Government Security Classifications

6.1. To ensure information is properly protected the Government have adopted a security classification scheme for all information that it collects, stores, processes, generates or shares.

6.2. The security classifications indicate the sensitivity of information in terms of the likely impact of that information being lost, misused or compromised. Each classification provides for a baseline set of personnel, physical and information security controls that offer an appropriate level of protection against a typical threat profile. The three levels of classification are as follows:

1. **OFFICIAL** – this covers most of the information that is processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened risk profile.
2. **SECRET** – very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.
3. **TOP SECRET** –this covers the Government's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

6.3. All information dealt with by Birmingham 2022 (including confidential information) is subject to the Government Classification Scheme and should be marked accordingly.

6.4. The 'OFFICIAL' classification covers much of public sector business including, most policy development, administrative data, service delivery, legal advice, finance, personal data that requires protection under data protection legislation, contracts, statistics, case files, intellectual property, public safety, criminal justice and enforcement activities, some aspects of defence, security and resilience. There is no requirement to explicitly mark routine 'OFFICIAL' information, but security measures should still be enforced to protect such information.

6.5. Some information within the 'OFFICIAL' classification may be deemed to be of a more sensitive nature and so access to this information must only be granted on a 'need to know' basis. Additional security controls will also need to be adopted

for this type of information. In such cases, where there is a requirement to reinforce the 'need to know' basis this type of information should be conspicuously marked as 'OFFICIAL – SENSITIVE'.

6.6. 'OFFICIAL – SENSITIVE' information includes, but is not limited to the following:

- The most sensitive corporate information, such as organisational restructuring, negotiations and major security or business continuity issues.
- Very sensitive personal information (i.e. special category data), and information about vulnerable or at-risk people.
- Policy development and advice to ministers on contentious and very sensitive issues.
- Commercially or market sensitive information.
- Information about investigations and civil or criminal proceedings that could disrupt law enforcement or prejudice court cases.
- Sensitive diplomatic business or international negotiations.

7. Personal data

7.1. Some of the confidential information which Birmingham 2022 employees will process will involve personal data. Personal data should generally be classified as 'Official' under the Government Classification Scheme. Special category data (see section 8 below for further information) should be classified as 'Official Sensitive.

7.2. There is a range of legislation related to the use of personal data. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) form part of the data protection regime in the UK that governs the use of personal data. The GDPR applies to the processing of personal data that is:

- wholly or partly by automated means (i.e. by computer); or
- processed other than by automated means and forms part of, or is intended to form part of, a filing system.

7.3. Personal data only includes information relating to individuals who:

- can be identified or are identifiable, directly from the information in question; or
- can be indirectly identified from that information in combination with other information.

7.4. Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR. Such information may still however be considered to be confidential in nature and should be treated accordingly.

7.5. Information about companies or public authorities is not personal data. However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable, and the information relates to them as an individual, may constitute personal data.

8. Special category data and criminal offence data

8.1. Personal data may also include special categories of personal data and criminal conviction and offences data. These types of data are considered to be more sensitive, require greater protection and can only be processed in more limited circumstances.

8.2. Special category data is considered more sensitive because if this type of data were inappropriately accessed it could create more significant risks to a person's fundamental rights and freedoms, such as putting them at risk of unlawful discrimination. Special category data is information about an individual's:

- racial or ethnic origin;
- political, religious or philosophical beliefs;
- trade union membership;
- genetic and biometric data (where used for ID purposes);
- health, sex life or sexual orientation.

8.3. Criminal offence data includes data about criminal allegations, proceedings or convictions and personal data linked to related security measures. Before processing this data organisations must first have a lawful basis for doing so and either do so in an official capacity (such as the police) or comply with one of the conditions in Schedule 1 of the DPA 2018.

8.4. In order to lawfully process special category data, there must be both a lawful basis under Article 6 of GDPR (see point 12.1 below) and a separate condition for processing special category data under Article 9 of GDPR (see point 12.3 below) These bases do not have to be linked. The Article 9 GDPR conditions should also be read alongside the Data Protection Act 2018, which adds more specific conditions and safeguards in Schedule 1 Part 1 and Part 2. The Data Protection Officer can provide further guidance.

9. Pseudonymised and anonymised data

9.1. Pseudonymous data is personal data that has been modified so that it no longer directly identifies an individual without the use of additional information. Pseudonymising personal data can reduce the risks to data subjects, however, pseudonymisation is only a security measure. It does not change the status of the data which remains as personal data.

9.2. Anonymous data does not identify individuals and so is no longer considered to be personal data. Data protection legislation does not apply to personal data that has been anonymised.

10. The data protection principles

10.1. Article 5 (1) of the GDPR sets out six data protection principles which must be complied with by all employees of Birmingham 2022 when dealing with personal data. The principles state that personal data must be:

1) processed lawfully, fairly and in a transparent manner in relation to the data subject.

2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes (also known as the ‘purpose limitation' principle);

3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (also known as the 'data minimisation' principle);

4) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (personal data may be stored for longer periods for archiving purposes in the public interest, scientific, historical research or statistical purposes);

6) 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 ('integrity and confidentiality').

10.2. There is a seventh data protection principle, relating to accountability. It requires that a data controller, such as Birmingham 2022, shall be responsible for, and be able to demonstrate compliance with, the other data protection principles. To demonstrate compliance with the accountability principle, Birmingham 2022, undertakes the following:

- provides privacy notices informing individuals about the uses of their personal data;
- keeps records of processing activities involving the use of personal data;
- undertakes data protection impact assessments when required;
- produces policies and procedures for staff to follow when processing personal data;
- provides staff training in matters relating to data protection and information security; and
- implements data processing agreements and data sharing agreements where required.

11. Individual rights

11.1. The data protection legislation provides individuals (data subjects) with specific rights relating to the use of their personal data. These rights aim to provide individuals with greater control and autonomy over the use of their personal data.

11.2. Under data protection legislation, individuals have the following rights:

- the right to be informed (often achieved by use of privacy notices),
- the right of access (also known as a subject access request);
- the right of rectification;
- the right to erasure (also known as the right to be forgotten);
- the right to restrict processing;
- the right to data portability;
- the right to object to processing (including for direct marketing); and
- rights in relation to automated decision making and profiling.

11.3. Birmingham 2022 takes its responsibilities with respect to an individual's rights under the data protection legislation very seriously. There is a separate Data Subject Rights Policy and Procedure in place, which employees should read in conjunction with this policy.

12. Lawful basis for processing

12.1. The GDPR requires organisations to have a valid lawful basis in order to process personal data. There are 6 available lawful bases for processing, they are:

1. the individual has given consent to the processing of his or her personal data for one or more specific purposes;
2. processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller (i.e. Birmingham 2022) is subject;
4. processing is necessary in order to protect the vital interests of the individual or of another person;
5. 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 controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which require protection of personal data, in particular, where the data subject is a child.

12.2. The lawful basis for processing personal data and special category data will be recorded on Birmingham 2022's record of processing activities (see section 15 below) and notified to individuals via our Privacy Notices.

12.3. For processing special category data there must be one of the lawful bases listed above at point 12.1 **in addition** to one of the special conditions listed below:

1. the individual has given explicit consent to processing for one or more specified purposes, except where prohibited by other laws; or

2. processing is necessary for the controller (Birmingham 2022) to carry out obligations and rights in the field of employment law; or

3. processing is necessary to protect the vital interests of the individual or another person, where the individual is either physically or legally incapable of giving consent; or

4. processing is carried out in the course of a controller's legitimate activities with appropriate safeguards by a foundation, association or other non-profit seeking body with a political, philosophical, religious or trade-union aim. (NB: this condition does not apply to Birmingham 2022); or

5. the processing relates to personal data made public by the individual; or

6. processing is necessary for the establishment, exercise or defence of legal claims; or

7. processing is necessary for the performance of a task carried out in the public interest, or on the basis of law which provides suitable measures to safeguard the individual's legitimate interests; or

8. processing of data about health is necessary for health purposes and subject to the conditions and safeguards in Article 81 of GDPR; or

9. processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards in Article 83 of GDPR; or

10. processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or to comply with a legal or regulatory obligation, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by law providing for adequate safeguards.

The ten conditions listed above at point 12.3 should also be read alongside the Data Protection Act 2018, which adds more specific conditions and safeguards in Schedule 1 Part 1 and Part 2 for processing special category data. The Data Protection Officer can provide further guidance.

13. Consent

13.1. Consent is one of the six lawful bases for processing personal information and explicit consent is one of the bases for processing special category data. (see section 12 above) The GDPR sets a high standard for consent. Consent must be freely given; this means giving people genuine ongoing choice and control over how their personal information is used.

13.2. Consent is often not a suitable basis for processing personal and special category data, particularly if consent is a precondition of a service. If Birmingham 2022 would still process the personal data without consent, asking for consent is misleading and inherently unfair. In these circumstances, a different lawful basis for processing should be considered. Any uses of consent for processing personal data and special category data must first be agreed by the Data Protection Officer to ensure compliance with the GDPR. Any consent forms must also be reviewed and agreed by the Data Protection Officer.

13.3. For consent to be compliant with the GDPR, it must:

- be freely given
- be a positive opt-in by individuals, this means that Birmingham 2022 must not use pre-ticked boxes or any other method of default consent;
- be clear, concise, easy to understand and obvious;
- be specific and 'granular', i.e. separate consent must be sought for separate uses of the personal information. consent for the use of personal data must also be separate from other terms and conditions. Vague or blanket consent is not appropriate;
- make it easy for individuals to withdraw consent and they must be informed how to do this;
- not be a precondition of service;
- reveal the name of the organisation processing the personal data, the purposes of the processing and the types of processing activity;
- name any third-party data controllers who will rely on the consent; and
- explicit consent for the use of special category data must be a clear and specific statement of consent expressly confirmed in words, rather than by any other positive action.

13.4. Birmingham 2022 must keep records to evidence any consent which has been sought from individuals. These records must include; who consented, when, how, and what they were told.

13.5. Records of consent must be kept under constant review and refreshed when changes occur.

14. Data controller and data processor responsibilities

14.1. The GDPR applies to both data controllers and data processors.

14.2. Birmingham 2022 is a data controller, which means that we determine the purposes and means of processing the personal data that we hold. For example, we decide what personal data we need to collect, what it is going to be used for, whom we may need to share the data with and how long we need to retain the data.

14.3. Birmingham 2022 also uses other organisations to process personal data on our behalf. The GDPR refers to such organisations as 'data processors', but they may also be referred to as 'third party data processors' or 'service providers'.

14.4. GDPR places specific obligations on data controllers and they shoulder the highest level of compliance responsibility under the GDPR. Birmingham 2022 must comply with, and demonstrate compliance with, all of the data protection principles as well as the other GDPR requirements. We are also responsible for the compliance of any of our data processors.

14.5. The GDPR also places specific obligations on data processors; for example; they are required to maintain records of personal data processing activities and they also have legal liability if they are responsible for a breach of personal data.

15. Agreements with data processors and data controllers

15.1. Data processors are only permitted to process personal data on behalf of Birmingham 2022 if a written contract is in place. The contract should impose a number of mandatory legal obligations on the data processor, as set out in the GDPR, (in particular Articles 28-33). This contract may also be referred to as a 'data processing agreement.' If personal data will be processed outside of the EEA, additional safeguards will be required, such as using EU approved standard contractual clauses within the contract. Point 16.4 below provides a list of additional safeguards.

15.2. Staff who become aware of any new data processing activities that will be undertaken by data processors, should first check with the Chief Legal Officer whether there is a suitable contract in place before the processing can proceed.

15.3. Similarly, if a processor uses another organisation (i.e. a sub-processor) to help it process personal data for Birmingham 2022, it needs to have a written contract in place with that sub-processor which includes data protection clauses that relate to Article 28(3) of GDPR and offer an equivalent level of protection for the personal data as those in the contract between the processor and Birmingham 2022.

15.4. Birmingham 2022 will also share data with other data controllers, such as West Midlands Police, the Department for Digital, Culture, Media and Sport and Birmingham City Council. When sharing data with these organisations appropriate information sharing agreements should be in place. These agreements should cover the following:

- what personal data will be shared;

- what the recipient can and cannot do with the personal data;
- security measures in place to ensure the personal data remains secure;
- the procedure for dealing with confidentiality breaches;
- procedures for dealing with data subject requests;
- retention periods for the personal data and processes to ensure secure return or deletion of the personal data; and
- whether any of the personal data is to be transferred to a third party outside of the European Economic Area (**"EEA"**).

15.5. If a data sharing agreement is required for sharing personal data with another data controller please contact the Data Protection Officer for further assistance.

16. Record of processing activities

16.1. The GDPR requires organisations to maintain a record of their personal data processing activities. The record covers areas such as; the type of personal data being used, the purpose for processing the data, any data sharing arrangements and the retention period for the data. Both data controllers and data processors must record processing activities.

16.2. The Data Protection Officer maintains the organisation's record of personal data processing. Any new project or process that involves the processing of personal data must be reported to the Data Protection Officer to ensure it is appropriately recorded.

17. Transferring personal data outside of the EEA

17.1. Individuals risk losing the protection of the GDPR if their personal data is transferred outside of the EEA. On that basis, the GDPR restricts the transfer of personal data to countries outside the EEA, or international organisations. These restrictions apply to all transfers, no matter the size of transfer or how often they take place.

17.2. Putting personal data on to a website will often result in a restricted transfer. The restricted transfer takes place when someone outside the EEA accesses that personal data via the website. Similarly, if personal data is entered onto a UK based server which is then available through a website, which may be accessed from outside the EEA, then this becomes a restricted transfer of data outside of the EEA.

17.3. If the data is made anonymous so that it is never possible to identify individuals (even when combined with other information which is available to the receiver), then it is no longer considered to be personal data. This means that the restrictions do not apply and the anonymised data can be transferred outside the EEA.

17.4. Restricted transfers of personal data outside of the EEA can be made in a number of circumstances, these are listed below:

- If the EU Commission made an 'adequacy decision' about the country or international organisation. Full findings of adequacy have been made with regards to Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. Only partial findings of adequacy have been made with regards to Canada and the US and so transfers to these two countries need to comply with specific regulations.

- If there are adequate safeguards in place to cover the transfer of personal data, adequate safeguards include the following:

    - A legally binding and enforceable agreement between public authorities or bodies;
    - Administrative arrangements between public authorities or bodies which include enforceable and effective rights for the individuals whose personal data is transferred, and which have been authorised by a supervisory authority;
    - Binding corporate rules;
    - Standard data protection clauses adopted by the European Commission or adopted by a supervisory authority and approved by the European Commission;
    - An approved code of conduct together with binding and enforceable commitments of the receiver outside the EEA;
    - Certification under an approved certification mechanism together with binding and enforceable commitments of the receiver outside the EEA; and / or
    - Contractual clauses authorised by a supervisory authority.

17.5. If a restricted transfer is neither covered by an adequacy decision, nor an appropriate safeguard, then the transfer can only be made if it is covered by one of the 'exceptions' set out in Article 49 of the GDPR.

17.6. Before any personal data is transferred outside of the EEA, the Data Protection Officer must assess the transfer of data to ensure it is compliant with GDPR. Such transfers of data may be subject to assessment via a data protection impact assessment.

18. Privacy by design (data protection impact assessments)

18.1. Data protection impact assessments (DPIAs) are part of Birmingham 2022's accountability obligations under GDPR and help to identify and minimise the data protection risks of a project. Completing a DPIA helps to ensure that a 'data protection by design and by default' approach is integral to any new system, project, process or information sharing venture that involves the use of personal data.

18.2. DPIAs are a legal requirement for processing of personal data that is likely to be high risk, but they are not mandatory for every processing operation. The GDPR states that DPIAs must be carried out in the following circumstances:

- when the processing is likely to result in a high risk to the rights and freedoms of individuals;
- automated processing, including profiling which is based on a systematic and extensive evaluation of an individual, and on which decisions are based that produce legal effects or significantly affect the individual;
- large scale use of sensitive data, either special categories of data or of personal data relating to criminal convictions and offences;
- systematic monitoring of a publicly accessible area on a large scale.

18.3. The Information Commissioner's Office (ICO) has published a list of ten types of processing that is likely to be high risk and will automatically require a DPIA. Further information can be found in Birmingham 2022's Data Protection Impact Assessment Procedure which is available on SharePoint or can be sourced from the Data Protection Officer.

19. Retention periods and archiving confidential information

19.1. The fifth data protection principle of GDPR is known as the storage limitation principle. This means that personal data must not be kept for longer than it is needed.

19.2. Ensuring that personal data is deleted or archived when it is no longer required reduces the risk that it becomes irrelevant, excessive, inaccurate or out of date. It also reduces the risk that such data will be used in error.

19.3. Some confidential data, including personal data, must be retained for a specific period of time to comply with legal obligations. Other confidential data may need to be passed to the National Archives after Birmingham 2022 ceases to operate.

19.4. Birmingham 2022 will operate a separate Archiving, Destruction and Retention Policy with an accompanying retention schedule. This will list the type of information which Birmingham 2022 holds, what it is used for and how long it will be retained. Further details can be obtained from the Data Protection Officer.

20. Commercially sensitive information

20.1. Not all of the information processed by Birmingham 2022 will involve personal data and be subject to the rules laid out in data protection legislation. Some of the information which Birmingham 2022 uses may not fall within the definition of 'personal data' but may still require a high degree of confidentiality and protection and be 'commercially sensitive' in nature. Instances of confidential information that may be commercially sensitive include, but are not limited to the following:

- site plans for Games venues and the terms and specifications of bids for the fit-out of Games venues, including drawings and schematics containing confidential information;

- marketing plans and the identity and terms of bids for sponsorships and marketing rights;
- the details of tenders for goods and services being acquired as ell as the identity of tenderers;
- the existence and terms of competing bids for broadcasting rights;
- any proposed significant new project, acquisition of property, joint venture or similar development;
- Birmingham 2022 budgets, financial statements and projections prior to general release by Birmingham 2022 to the public;
- contract awards and cancellations;
- litigation matters and contractual disputes;
- information concerning negotiations in relation to any of the above matters.

20.2. Information that is considered to be commercially sensitive will not be subject to the GDPR or the Data Protection Act 2018 (unless it contains personal data) but it is subject to the Government Security Classifications and should be treated as confidential and marked according to the classifications. It should be classified as 'OFFICIAL' information in most instances and 'OFFICIAL – SENSITIVE' for more sensitive information. (See section 6 for further information)

20.3. Requests may be made to Birmingham 2022 under the Freedom of Information Act or Environmental Information Regulations by members of the public, (including journalists) for the disclosure of information considered to be commercially sensitive to Birmingham 2022. There may be a number of exemptions to providing this information.

20.4. Any such request should be forwarded immediately to the Data Protection Officer. These requests will be dealt with in accordance with Birmingham 2022's Freedom of Information Policy.

21. Security related information

21.1. The third category of confidential data which Birmingham 2022 employees may encounter in the course of carrying out their duties is security related information. This may include but is not limited to:

- design and implementation details of security systems related to the Games;
- information relating to Birmingham 2022 IT systems;
- security threat information.

21.2. Security related information should be classified under the Government Security Classifications Scheme. Such information may be classified as 'OFFICIAL – SENSITIVE' but it may also be classified as 'SECRET' or in rare cases 'TOP SECRET' depending on the threat profile associated with it (See section 6). More information can be found in the; Government Security Classifications, Version 1.1, May 2018 located at: www.gov.uk/government/publications/government-security-classifications

21.3. Employees must not, under any circumstances, disclose any security related information without first discussing the matter with the Director of Security and, if related to ICT, the Senior Enterprise Architect.

21.4. It is unlikely that any security related information would be disclosed as part of a Freedom of Information request. Exemptions exist within the Freedom of Information Act to protect information that should not be disclosed, for example because disclosing it would be harmful to another person or it would be against the public interest.

21.5. Any such request should be forwarded immediately to the Data Protection Officer. These requests will be dealt with in accordance with Birmingham 2022's Freedom of Information Policy.

22. Protecting confidential information

22.1. Employees of Birmingham 2022 are required to sign confidentiality clauses in their contracts before they are able to process any confidential information. Secondees, volunteers, work experience individuals and embedded contractors are required to sign a non-disclosure agreement. No confidential discussions should take place unless a non-disclosure agreement is signed by the other party. Please send any request for a non-disclosure agreement to the Chief Legal Officer.

22.2. The following practical safeguards should be put in place to protect confidential information:

- All confidential information, regardless of whether it is personal, commercially sensitive or security related must be dealt with in accordance with the Government Security Classification Scheme.

- No written document containing personal data shall be left where it can be read by individuals who have no right to see that information; this includes; letters, telephone messages, emails and other documentation. Birmingham 2022 operates a clear desk policy.

- Paper documentation that contains confidential information, must be contained within locked storage facilities with restricted access.

- Conversations of a confidential nature must not be conducted in public areas where individuals who have no right to hear that information are likely to overhear. Public areas include such places as corridors, stairways, lifts and kitchens.

- All confidential paper waste must be disposed of appropriately by placing it in the confidential waste bins provided.

- Confidential documents must be printed using the locked printing facility and should be collected from the printer immediately.

- Spam emails must never be opened. They should be deleted and reported to the IT department.

- Confidential information must not be stored on any portable media (such as laptops, USB sticks, disks etc) unless it has been encrypted. All portable media must be locked away when not in use.

- Confidential information must only be sent by email from one secure email address to another. Please see the Acceptable Use of Email Policy for further details.

- Computer screens must not be left on view or positioned in such a way that the public or employees who do not have the right to see the information can view personal data or other types of confidential information. Screens must always be locked by the user when leaving their computer or laptop.

- Employees must never share their passwords with anyone. Passwords must not be written down anywhere and must be of sufficient complexity to ensure they can't be 'cracked' or 'guessed' by others. The Information Security Policy provides further information about password security.

- Access to computer systems, software and shared drives that contain confidential information, must be strictly controlled.

- All electronic files containing personal data or confidential information must be held within a protected folder on SharePoint or in OneDrive and not stored on local hard drives.

- Computer and electronic equipment must be disposed of in accordance with instructions provided by the Chief Information Officer.

22.3. Working at home

- There will be occasions when employees need to work from home and have access to confidential information. Before employees are permitted to remove confidential information from their work place in any format they must first gain authority from their line manager.

- Employees must only remove the minimum amount of confidential information from their work place that is required for the purpose of their work.

- Secure bags must be used for the transportation of confidential information held in whatever format.

- During transit, documents and equipment containing confidential information should never be left on view and should be transported on the employee's person or out of sight in the boot of their vehicle.

- Documents and equipment containing confidential information must never be left unattended in vehicles.

- Whilst confidential information is being kept in an employee's home confidentiality must be maintained at all times. Documents or equipment must be securely locked away when not in use. Any other person(s) within the household, excepting the employee, must not be able to see the content of any confidential information held in a manual or paper format or have access to any equipment containing confidential information, such as laptops or USB sticks.

- If employees are using electronic equipment (such as laptops, USB sticks) to process confidential information they must only use equipment that they have been authorised to use and that has been encrypted. All such electronic equipment must be returned to the IT Services Team to ensure secure removal of the confidential information.

22.4. Remote working

- The principles outlined above in relation to working at home also apply to employees who are working remotely and are required to transport confidential information in the course of their work. This includes travel to and from various Games venues and attendance at any meetings on behalf of Birmingham 2022. It also includes any work undertaken at such locations.

- Employees who are working remotely and are required to transport confidential information should ensure they carry only the minimum confidential information required for the purpose of their work. Secure bags must be used for the transportation of confidential information held in whatever format.

- When an employee is unable to return documents and equipment containing confidential information to their work place after visits, confidentiality must be maintained within the employee's home and documents or equipment must be securely locked away. Documents and equipment should be returned to the work place as soon as possible.

- Employees working remotely may be working in public, open spaces where they are vulnerable to being observed and may subject to 'shoulder surfing' from other individuals. This can potentially compromise confidential information and so additional care must be taken in these instances.

- Any electronic equipment that is no longer required must be returned to the IT Services Team, so that it can be logged on the IT Asset Register.

23. Personal data breaches

23.1A A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A breach of personal data is therefore more than just a loss of personal data. Personal data breaches can include, but are not limited to the following:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a data controller or data processor;
- sending personal data to an incorrect recipient; for example, by email, post or fax;
- computing devices, such as laptops containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data.

23.2. The GDPR introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. In some cases, the individuals affected must also be notified of the breach.

23.3. Birmingham 2022 is also required to maintain a record of any personal data breach, regardless of whether we are required to notify the ICO.

23.4. To ensure Birmingham 2022 complies with the GDPR requirement relating to personal data breaches, all such breaches and any suspected security incident that relates to the loss of or unauthorised access to personal data, should be reported to the Data Protection Officer at: DP@birmingham2022.com and logged on the IT Service Management System.

24. Breaches of this policy

24.1. Any employee who breaches this policy, knowingly or recklessly processes confidential information for purposes other than those for which it is intended, or deliberately acts outside of their recognised responsibilities will be subject to Birmingham 2022's disciplinary procedures, which could result in dismissal for misconduct or gross misconduct, and possible legal action liable to prosecution.

24.2. Birmingham 2022 may terminate its relationship with other individuals and organisations working on its behalf if they breach this policy.

25. Monitoring

25.1. Compliance will be monitored via both the line management of employees and any incident reporting system put in place by Birmingham 2022.

25.2. The Data Protection Officer will monitor the implementation of this policy and any subsequent revisions. This will include:

- monitoring personal data breaches with a view to making any necessary amendments to the content of this or other related policies and procedures;
- monitoring data protection training undertaken across Birmingham 2022;
- monitoring Birmingham 2022's compliance with the Government Security Classifications and relevant data protection legislation;
- monitoring complaints made by individuals about the uses of their personal data; and
- undertaking confidentiality audits.

26. Review

26.1. This policy will be subject to review biannually after its approval date. Earlier review may be required if any of the following occur:

- the adoption of the policy highlights any errors or omissions in its content;
- following monitoring of potential or actual breaches of confidentiality by the Data Protection Officer, amendments are required to the content of the policy;
- where relevant changes in legislation or national guidance impact upon the content of this policy.

27. Guidance and legislation

- The Data Protection Act 2018: www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- The General Data Protection Regulation (EU) 2016/679
- The Computer Misuse Act 1990: www.legislation.gov.uk/ukpga/1990/18/contents
- Data Subject Rights Policy and Procedure, Birmingham 2022
- Information Security Policy, Birmingham 2022
- Acceptable Use of Email Policy, Birmingham 2022
- Data Protection Impact Assessment Procedure, Birmingham 2022
- Archiving, Destruction and Retention Policy, Birmingham 2022
- Government Security Classifications, version 1.1, May 2018: www.gov.uk/government/publications/government-security-classifications
- Information Commissioner's Office guidance at: www.ico.org.uk