



QEII CENTRE
GDPR DATA PROTECTION POLICY

Policy Agreed: May 2018

Next Review date: May 2020

Review Cycle: 2 Years

1. Policy statement and objectives

- 1.1 The objectives of this Data Protection Policy are to ensure that The Queen Elizabeth II Centre (the “QEII Centre”) and its employees are informed about, and comply with, their obligations under the General Data Protection Regulation (“the GDPR”) and other data protection legislation.
- 1.2 The QEII Centre is the Data Controller for all the Personal Data processed by the QEII Centre.
- 1.3 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner.
- 1.4 The type of information that we may be required to handle include details of job applicants, current, past and prospective employees, clients, delegates, suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the GDPR and other legislation. The GDPR imposes restrictions on how we may use that information.
- 1.5 This policy does not form part of any employee’s contract of employment and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the GDPR may expose the QEII Centre to enforcement action by the Information Commissioner’s Office (ICO), including the risk of fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the QEII Centre’s employees. At the very least, a breach of the GDPR could damage our reputation and have serious consequences for the QEII Centre and for our stakeholders.

2. Status of the policy

- 1.1 This policy has been approved by the Directorate of the QEII Centre. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

3. Data Protection Officer/Data Privacy Team

- 3.1 The Data Protection Officer (the “DPO”) is responsible for ensuring the QEII Centre is compliant with the GDPR and with this policy. This post is held by Maewyn Cumming, on behalf of the Ministry of Housing, Communities and Local Government (MHCLG). In addition, a Data Privacy Team will be appointed by the QEII Centre. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Privacy Team.
- 3.2 The Data Privacy Team will play a major role in embedding essential aspects of the GDPR into the QEII Centre’s culture, from ensuring the data protection principles are respected to preserving data subject rights, recording data processing activities and ensuring the security of processing.
- 3.3 The Data Privacy Team should be involved, in a timely manner, in all issues relating to the protection of personal data. To do this, the GDPR requires that the Data Privacy Team is provided with the necessary support and resources to enable the Data Privacy Team to effectively carry out their tasks. Factors that should be considered include the following:

- 3.3.1 senior leadership support;
- 3.3.2 time for the Data Privacy Team to fulfil their duties;
- 3.3.3 adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate;
- 3.3.4 official communication of the designation of the Data Privacy Team to make known existence and function within the organisation;
- 3.3.5 access to other services, such as HR, IT and security, who should provide support to the Data Privacy Team;
- 3.3.6 continuous training so that Data Privacy Team can stay up to date with regard to data protection developments;
- 3.3.7 a clear infrastructure detailing roles and responsibilities of each team member;
- 3.3.8 whether the QEII Centre should give the Data Privacy Team access to external legal advice to advise the Data Privacy Team on their responsibilities under this Data Protection Policy.

3.4 The Data Privacy Team is responsible for ensuring that the QEII Centre's Processing operations adequately safeguard Personal Data, in line with legal requirements. This means that the governance structure within the QEII Centre must ensure the independence of the Data Privacy Team.

3.5 The QEII Centre will ensure that the Data Privacy Team does not receive instructions in respect of the carrying out of their tasks, which means that the Data Privacy Team must not be instructed how to deal with a matter, such as how to investigate a complaint or what result should be achieved. Further, the Data Privacy Team should report directly to the highest management level, i.e. the Directorate.

3.6 The requirement that the Data Privacy Team reports directly to the Directorate ensures that the QEII Centre's Directors are made aware of the pertinent data protection issues. In the event that the QEII Centre decides to take a certain course of action despite the Data Privacy Team's advice to the contrary, the Data Privacy Team should be given the opportunity to make their dissenting opinion clear to the Directorate and to any other decision makers.

3.7 If you consider that the policy has not been followed in respect of Personal Data about yourself or others you should raise the matter in the first instance with the Data Privacy Team.

4. Definition of terms

4.1 **Biometric Data** means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images;

4.2 **Consent** of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her;

- 4.3 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;
- 4.4 **Data Subjects** for the purpose of this policy include all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.
- 4.5 **Data Controllers** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
- 4.6 **Data Users** include employees whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our data protection and security policies at all times;
- 4.7 **Data Processors** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;
- 4.8 **Personal Data** means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- 4.9 **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 transmitted, stored or otherwise processed;
- 4.10 **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR;
- 4.11 **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- 4.12 **Special Category (Sensitive Personal) Data** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

5. **Data protection principles**

- 5.1 Anyone processing Personal Data must comply with the enforceable principles of good practice. These provide that Personal Data must be:
- 5.1.1 processed lawfully, fairly and in a transparent manner in relation to individuals;
 - 5.1.2 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 purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

- 5.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - 5.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - 5.1.5 kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
 - 5.1.6 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.
- 5.2 Processed lawfully, fairly and in a transparent manner
- 5.2.1 The GDPR is intended not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is (in this case the QEII Centre), who the Data Controller's representative is (in this case the Data Privacy Team) the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.
 - 5.2.2 For Personal Data to be processed lawfully, certain conditions have to be met. These may include:
 - 5.2.2.1 where we have the consent of the Data Subject;
 - 5.2.2.2 Where we require the data to fulfil our contractual obligations;
 - 5.2.2.3 where it is necessary for compliance with a legal obligation;
 - 5.2.2.4 where processing is necessary to protect the vital interests of the Data Subject or another person;
 - 5.2.2.5 where it 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.
 - 5.2.3 Personal Data may only be processed for the specific purposes notified to the Data Subject when the data was first collected, or for any other purposes specifically permitted by the Act. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose before any processing occurs.
- 5.3 Special Category (Sensitive Personal) Data
- 5.3.1 The QEII Centre will be processing Special Category Data about our stakeholders. We recognise that the law states that this type of data needs

more protection. Therefore, Data Users must be more careful with the way in which we process Special Category Data.

5.3.2 When Special Category Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 5.1 above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

5.3.2.1 the Data Subject's explicit consent to the processing of such data has been obtained

5.3.2.2 processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, where we respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

5.3.2.3 processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

5.3.2.4 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

5.3.3 The QEII Centre recognises that in addition to Special Category Data, we are also likely to process information about our stakeholders which is confidential in nature. Appropriate safeguards must be implemented for such information, even if it does not meet the legal definition of Special Category Data.

5.4 Biometric Data

5.4.1 The QEII Centre processes Biometric Data as part of an automated biometric recognition system, for example staff passes, CCTV and fingerprint scanning. Biometric Data is a type of Special Category Data.

5.4.2 Where Biometric Data relating to staff, contractors or clients is processed, the QEII Centre must ensure that each member of staff is aware that Biometric Data is being collected and for what specific purpose.

5.4.3 The QEII Centre must obtain the explicit Consent of staff or other Data Subjects before Processing their Biometric Data.

5.5 Criminal convictions and offences

5.5.1 There are separate safeguards in the GDPR for Personal Data relating to criminal convictions and offences.

5.5.2 It is possible that the QEII Centre will Process Data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff due to information which we may acquire during the course of their employment or appointment.

- 5.5.3 In addition, from time to time we may acquire information about criminal convictions or offences involving staff. This information is not routinely collected and is only likely to be processed by the QEII Centre in specific circumstances.
- 5.5.4 Where appropriate, such information may be shared with external agencies such as the Police. Such information will only be processed to the extent that it is lawful to do so, and appropriate measures will be taken to keep the data secure.
- 5.6 Transparency
 - 5.6.1 One of the key requirements of the GDPR relates to transparency. This means that the QEII Centre must keep Data Subjects informed about how their Personal Data will be processed when it is collected.
 - 5.6.2 One of the ways we provide this information to individuals is through a privacy notice which sets out important information what we do with their Personal Data. The QEII Centre has developed Privacy Notices for the following categories of people:
 - 5.6.2.1 Staff, including contractors and the Centre's partners
 - 5.6.2.2 Clients
 - 5.6.3 The QEII Centre wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. This means that the Privacy Notice is just one of the tools we will use to communicate this information. Employees are expected to use other appropriate and proportionate methods to tell individuals how their Personal Data is being processed if Personal Data is being processed in a way that is not envisaged by our Privacy Notices and / or at the point when individuals are asked to provide their Personal Data.
 - 5.6.4 We will ensure that Privacy Notices are concise, transparent, intelligible and easily accessible; written in clear and plain language, and free of charge.
- 5.7 Consent
 - 5.7.1 The QEII Centre must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent. Consent is not the only lawful basis and there are likely to be many circumstances when we process Personal Data and our justification for doing so is based on a lawful basis other than Consent.
 - 5.7.2 A Data Subject consents to processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.
 - 5.7.3 Data Subjects must be easily able to withdraw Consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.
 - 5.7.4 Unless we can rely on another legal basis of processing, Explicit Consent is usually required for processing Special Category Data. Often we will be relying

on another legal basis (and not require Explicit Consent) to process most types of Sensitive Data.

5.7.5 Evidence and records of Consent must be maintained so that the QEII Centre can demonstrate compliance with Consent requirements.

6. Specified, explicit and legitimate purposes

6.1 Personal Data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject, for example, in the Privacy Notice or at the point of collecting the Personal Data. Any data which is not necessary for that purpose should not be collected in the first place.

6.2 The QEII Centre will be clear with Data Subjects about why their Personal Data is being collected and how it will be processed. We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

7. Adequate, relevant and limited to what is necessary

7.1 The QEII Centre will ensure that the Personal Data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary.

7.2 In order to ensure compliance with this principle, the QEII Centre will check records at appropriate intervals for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of data.

7.3 Employees must also give due consideration to any forms stakeholders are asked to complete and consider whether all the information is required. We may only collect Personal Data that is needed to operate within our function and we should not collect excessive data. We should ensure that any Personal Data collected is adequate and relevant for the intended purposes.

7.4 The QEII Centre will implement measures to ensure that Personal Data is processed on a 'Need to Know' basis. This means that the only members of staff who need to know Personal Data about a Data Subject will be given access to it and no more information than is necessary for the relevant purpose will be shared. In practice, this means that the QEII Centre may adopt a layered approach in some circumstances, for example, members of staff may be given access to basic information about a client or employee if they need to know it for a particular purpose but other information about a Data Subject may be restricted to certain members of staff who need to know it, for example, where the information is Special Category Data, relates to criminal convictions or offences or is confidential in nature (for example, disciplinary measures).

7.5 When Personal Data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the QEII Centre's data retention guidelines.

8. Accurate and, where necessary, kept up to date

8.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

8.2 If a Data Subject informs the QEII Centre of a change of circumstances their records will be updated as soon as is practicable.

8.3 Where a Data Subject challenges the accuracy of their data, the QEII Centre will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Data Protection Team for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the Information Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

8.4 Notwithstanding paragraph 8.3, a Data Subject continues to have rights under the GDPR and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out in paragraph 8.3 has been followed.

9. Data to be kept for no longer than is necessary for the purposes for which the Personal Data is processed

9.1 Personal data should not be kept longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required.

9.2 It is the duty of the Data Privacy Team, after taking appropriate guidance for legal considerations, to ensure that obsolete data is properly erased. The QEII Centre has a retention schedule for all data.

10. Data to be processed in a manner that ensures appropriate ` of the Personal Data

10.1 The QEII Centre has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

10.2 The GDPR requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

10.3 We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data.

10.4 Data Users are responsible for protecting the Personal Data we hold. Data Users must implement reasonable and appropriate security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Data Users must exercise particular care in protecting Special Category Data from loss and unauthorised access, use or disclosure.

10.5 Data Users must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Data Users must comply with all applicable aspects of our DATA SECURITY POLICY and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

10.6 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:

10.6.1 **Confidentiality** means that only people who are authorised to use the data can access it.

- 10.6.2 **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed.
- 10.6.3 **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.
- 10.7 It is the responsibility of all members of staff to ensure that the Personal Data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Data Privacy Team.
- 10.8 Please see our Information Asset Audit for details for the arrangements in place to keep Personal Data secure
- 11. Processing in line with Data Subjects' rights**
- 11.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:
- 11.1.1 withdraw Consent to processing at any time;
 - 11.1.2 receive certain information about the Data Controller's processing activities;
 - 11.1.3 request access to their Personal Data that we hold;
 - 11.1.4 prevent our use of their Personal Data for direct marketing purposes;
 - 11.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
 - 11.1.6 restrict processing in specific circumstances;
 - 11.1.7 challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
 - 11.1.8 request a copy of an agreement under which Personal Data is transferred outside of the EEA;
 - 11.1.9 object to decisions based solely on automated processing, including profiling (automated decision making);
 - 11.1.10 prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
 - 11.1.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
 - 11.1.12 make a complaint to the supervisory authority (the ICO); and
 - 11.1.13 receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.
- 11.2 We are required to verify the identity of an individual requesting data under any of the rights listed above. Members of staff should not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

12. Dealing with subject access requests

- 12.1 The GDPR extends to all Data Subjects a right of access to their own Personal Data. A formal request from a Data Subject for information that we hold about them must be made in writing. The QEII Centre can invite a Data Subject to complete a form but we may not insist that they do so.
- 12.2 It is important that all members of staff are able to recognise that a written request made by a person for their own information is likely to be a valid Subject Access Request, even if the Data Subject does not specifically use this phrase in their request or refer to the GDPR. In some cases, a Data Subject may mistakenly refer to the “Freedom of Information Act” but this should not prevent the QEII Centre from responding to the request as being made under the GDPR, if appropriate. Some requests may contain a combination of a Subject Access Request for Personal Data under the GDPR and a request for information under the Freedom of Information Act 2000 (“FOIA”). Requests for information under the FOIA must be dealt with promptly.
- 12.3 Any member of staff who receives a written request of this nature must immediately forward it to the Data Privacy Team as the statutory time limit for responding is **one calendar month**. Under the Data Protection Act 1998 (DPA 1998), Data Controllers previously had 40 calendar days to respond to a request.
- 12.4 As the time for responding to a request does not stop during the periods when the QEII Centre is closed for the holidays, we will attempt to mitigate any impact this may have on the rights of data subjects to request access to their data by implementing the following measures:
- The email address for the Data Privacy Team will be checked at a regular basis during holidays.
- 12.5 A fee may no longer be charged to the individual for provision of this information (previously a fee of £10 could be charged under the DPA 1998).
- 12.6 The QEII Centre may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person’s identity before disclosing the information.
- 12.7 In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.
- 12.8 Following receipt of a Subject Access Request, and provided that there is sufficient information to process the request, an entry should be made in the QEII Centre’s Subject Access log book, showing the date of receipt, the Data Subject’s name, the name and address of requester (if different), the type of data required and the planned date for supplying the information (not more than one calendar month from the request date). Should more information be required to establish either the identity of the Data Subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.
- 12.9 Where requests are “manifestly unfounded or excessive”, in particular because they are repetitive, the QEII Centre can:
- 12.9.1 charge a reasonable fee taking into account the administrative costs of providing the information; or
- 12.9.2 refuse to respond.

- 12.10 Where we refuse to respond to a request, the response must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Members of staff should refer to any guidance issued by the ICO on Subject Access Requests and consult the Data Privacy Team before refusing a request.
- 12.11 Certain information may be exempt from disclosure, so members of staff will need to consider what exemptions (if any) apply and decide whether you can rely on them. For example, information about third parties may be exempt from disclosure. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support from the Data Privacy Team if you are unsure which exemptions apply.
- 12.12 [Further information about exemptions will be added once the Data Protection Bill becomes law.]

13. Providing information over the telephone

- 13.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by the QEII Centre whilst also applying common sense to the particular circumstances. In particular they should:
- 13.1.1 Check the caller's identity to make sure that information is only given to a person who is entitled to it.
 - 13.1.2 Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
 - 13.1.3 Refer to their line manager or the Data Privacy Team for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

14. Authorised disclosures

- 14.1 The QEII Centre will only disclose data about individuals if one of the lawful bases apply.
- 14.2 Only authorised and trained staff are allowed to make external disclosures of Personal Data. The QEII Centre will regularly share Personal Data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:
- 14.2.1 The Ministry of Housing, Local and Communities Government
 - 14.2.2 the Local Government Pension Scheme which is administered by MyCSP
 - 14.2.3 Moorepay (our external payroll provider)
 - 14.2.4 HMRC
 - 14.2.5 the Police or other law enforcement agencies
 - 14.2.6 Duradiamond our occupational health advisors
 - 14.2.7 Courts, if ordered to do so;
 - 14.2.8 confidential waste collection companies;
 - 14.2.9 Our suppliers

- 14.3 Some of the organisations we share Personal Data with may also be Data Controllers in their own right in which case we will be jointly controllers of Personal Data and may be jointly liable in the event of any data breaches.
- 14.4 Data sharing agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. However, they are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.
- 14.5 All data sharing agreements must be signed off by the Data Privacy Team who will keep a register of all data sharing agreements.
- 14.6 The GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the data is Processed ("GDPR clauses"). A summary of the GDPR requirements for contracts with Data Processors is set out in Appendix 1. It will be the responsibility of the QEII Centre to ensure that the GDPR clauses have been added to the contract with the Data Processor. Personal data may only be transferred to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.
- 14.7 In some cases, Data Processors may attempt to include additional wording when negotiating contracts which attempts to allocate some of the risk relating to compliance with the GDPR, including responsibility for any Personal Data Breaches, onto The QEII Centre. In these circumstances, the member of staff dealing with the contract should contact the Data Privacy Team for further advice before agreeing to include such wording in the contract.

15. Reporting a Personal Data Breach

- 15.1 The GDPR requires Data Controllers to notify any notifiable Personal Data Breach to the ICO and, in certain instances, the Data Subject.
- 15.2 A notifiable Personal Data Breach must be reported to the ICO without undue delay and where feasible within 72 hours, unless the data breach is unlikely to result in a risk to the individuals.
- 15.3 If the breach is likely to result in high risk to affected Data Subjects, the GDPR, requires organisations to inform them without undue delay.
- 15.4 It is the responsibility of the DPO, or the Data Privacy Team, to decide whether to report a Personal Data Breach to the ICO.
- 15.5 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.
- 15.6 As the QEII Centre is closed or has limited staff available during holidays, there will be times when our ability to respond to a Personal Data Breach promptly and within the relevant timescales will be affected. We will consider any proportionate measures that we can implement to mitigate the impact this may have on Data Subjects.
- 15.7 If a member of staff suspects that a Personal Data Breach has occurred, the Data Privacy Team must be notified immediately. You should preserve all evidence relating to the potential Personal Data Breach.

16. Accountability

- 16.1 The QEII Centre must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The QEII Centre is responsible for, and must be able to demonstrate, compliance with the data protection principles.
- 16.2 The QEII Centre must have adequate resources and controls in place to ensure and to document GDPR compliance including:
- 16.2.1 appointing a suitably qualified DPO and an executive team accountable for data privacy;
 - 16.2.2 implementing Privacy by Design when processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where processing presents a high risk to rights and freedoms of Data Subjects;
 - 16.2.3 integrating data protection into internal documents including this Data Protection Policy, related policies and Privacy Notices;
 - 16.2.4 regularly training employees on the GDPR, this Data Protection Policy, related policies and data protection matters including, for example, Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches. The QEII Centre must maintain a record of training attendance by all personnel; and
 - 16.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. Record keeping

- 17.1 The GDPR requires us to keep full and accurate records of all our Data Processing activities.
- 17.2 We must keep and maintain accurate records reflecting our processing including records of Data Subjects' Consents and procedures for obtaining Consents.
- 17.3 These records should include, at a minimum, the name and contact details of the Data Controller, the DPO and the Data Privacy Team, clear descriptions of the Personal Data types, Data Subject types, processing activities, processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

18. Training and audit

- 18.1 We are required to ensure all personnel have undergone adequate training to enable us to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.
- 18.2 Members of staff must attend all mandatory data privacy related training.

19. Privacy By Design and Data Protection Impact Assessment (DPIA)

- 19.1 We are required to implement Privacy by Design measures when processing Personal Data by implementing appropriate technical and organisational measures (like

pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

19.2 This means that we must assess what Privacy by Design measures can be implemented on all programs/systems/processes that process Personal Data by taking into account the following:

19.2.1 the state of the art;

19.2.2 the cost of implementation;

19.2.3 the nature, scope, context and purposes of processing; and

19.2.4 the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.

19.3 We are also required to conduct DPIAs in respect to high risk processing.

19.3.1 The QEII Centre should conduct a DPIA and discuss the findings with the Data Privacy Team when implementing major system or business change programs involving the processing of Personal Data including:

19.3.1.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

19.3.1.2 Automated processing including profiling and ADM;

19.3.1.3 large scale processing of Special Category Data; and

19.3.1.4 large scale, systematic monitoring of a publicly accessible area.

19.4 We will also undertake a DPIA as a matter of good practice to help us to assess and mitigate the risks to clients. If our processing is likely to result in a high risk to the rights and freedom of clients, then a DPIA should be undertaken.

19.5 A DPIA must include:

19.5.1 a description of the processing, its purposes and the QEII Centre's legitimate interests if appropriate;

19.5.2 an assessment of the necessity and proportionality of the processing in relation to its purpose;

19.5.3 an assessment of the risk to individuals; and

19.5.4 the risk mitigation measures in place and demonstration of compliance.

20. Policy Review

20.1 It is the responsibility of the Directorate to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be reported to the Data Privacy Team.

20.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

21. Enquiries

- 21.1 Further information about the QEII Centre's Data Protection Policy is available from the Data Privacy Team.
- 21.2 General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk

Document Control

Date modified	Description of modification	Modified by

Appendix 1 – GDPR Clauses

The GDPR requires the following matters to be addressed in contracts with Data Processors. The wording below is a summary of the requirements in the GDPR and is not intended to be used as the drafting to include in contracts with Data Processors.

1. The Processor may only process Personal Data on the documented instructions of the controller, including as regards international transfers. (Art. 28(3)(a))
2. Personnel used by the Processor must be subject to a duty of confidence. (Art. 28(3)(b))
3. The Processor must keep Personal Data secure. (Art. 28(3)(c) Art. 32)
4. The Processor may only use a sub-processor with the consent of the Data Controller. That consent may be specific to a particular sub-processor or general. Where the consent is general, the processor must inform the controller of changes and give them a chance to object. (Art. 28(2) Art. 28(3)(d))
5. The Processor must ensure it flows down the GDPR obligations to any sub-processor. The Processor remains responsible for any processing by the sub-processor. (Art. 28(4))
6. The Processor must assist the controller to comply with requests from individuals exercising their rights to access, rectify, erase or object to the processing of their Personal Data. (Art. 28(3)(e))
7. The Processor must assist the Data Controller with their security and data breach obligations, including notifying the Data Controller of any Personal Data breach. (Art. 28(3)(f)) (Art. 33(2))
8. The Processor must assist the Data Controller should the Data Controller need to carry out a privacy impact assessment. (Art. 28(3)(f))
9. The Processor must return or delete Personal Data at the end of the agreement, save to the extent the processor must keep a copy of the Personal Data under Union or Member State law. (Art. 28(3)(g))
10. The Processor must demonstrate its compliance with these obligations and submit to audits by the Data Controller (or by a third party mandated by the controller). (Art. 28(3)(h))
11. The Processor must inform the Data Controller if, in its opinion, the Data Controller's instructions would breach Union or Member State law. (Art. 28(3))