**The Decorum Group**
71 - 75, Shelton Street, Covent Garden, London, WC2H 9JQ

## 4. Policy

**4.1 GDPR Background**
GDPR came into force on the 25 May 2018 and replaced the Data Protection Act 1998.
Following the UK departure from the EU, UK GDPR was incorporated into domestic law that applies in the UK.
UK GDPR provides greater protection to individuals and places obligations on organisations, but can be dealt with in bite-size chunks to ensure that any impact on the provision of care and services is minimised.
**4.2** All staff need to ensure the ways in which they handle personal data meet the requirements of UK GDPR.
**4.3 The Decorum Group's Approach to UK GDPR**
The Decorum Group is required to take a proportionate and appropriate approach to UK GDPR compliance. The Decorum Group understands that not all organisations will need to take the same steps – it will depend on the volume and types of personal data processed by a particular organisation, as well as the processes already in place to protect personal data. We understand that if we process significant volumes of personal data, including **special categories of data**, or have unusual or complicated processes in place in terms of the way we handle personal data, we will consider obtaining legal advice specific to the processing we conduct and the steps we may need to take.
**4.4** UK GDPR does not apply to any personal data held about someone who has died. Both the Access to Medical Reports Act 1988 and the Access to Health Records 1990 will continue to apply.
**4.5 Process for Promoting Compliance at The Decorum Group**
To ensure The Decorum Group compliance with UK GDPR, a suite of documents are available and should be read in conjunction with this overarching policy to provide a framework:

- UK GDPR – Key Terms Guidance
- UK GDPR - Key Principles Guidance
- UK GDPR - Processing Personal Data Guidance
- Appointing a Data Protection Officer Guidance
- Data Security and Data Retention Policy and Procedure
- Website Privacy and Cookies Policy and Procedure
- Subject Access Requests Policy and Procedure
- Subject Access Requests Process Map
- Subject Access Requests - Request Letter
- Rights of a Data Subject Guidance
- Breach Notification Policy and Procedure
- Breach Notification Process Map
- Fair Processing Notice Policy and Procedure
- Consent Form
- UK GDPR - Transfer of Data Guidance
- Privacy Impact Assessment (Privacy Notice) Policy and Procedure

**4.6 Overview of Key Principles and Documents**
The key principles and themes of each of the documents listed above are summarised below:
**Key Terms**
UK GDPR places obligations on all organisations that process personal data about a Data Subject. A brief description of those three key terms is included in the Definitions section of this document and are expanded upon in the Key Terms Guidance.
The requirements that The Decorum Group need to meet vary depending on whether The Decorum Group is a Data Controller or a Data Processor. We recognise that in most scenarios, The Decorum Group will be a Data Controller. The meaning of Data Controller and Data Processor, together with the roles they play under UK GDPR, are explained in the Key Terms Guidance.
Special categories of data attract a greater level of protection, and the consequences for breaching UK GDPR in relation to special categories of data may be more severe than breaches relating to other types of personal data. This information is also covered in more detail in the Key Terms Guidance.

**Key Principles**

There are 7 key principles of UK GDPR which The Decorum Group must comply with. These 7 principles are very similar to the key principles that were set out in the Data Protection Act 1998. They are:

- Lawful, fair and transparent use of personal data
- Using personal data for the purpose for which it was collected
- Ensuring that the personal data is adequate and relevant
- Ensuring that the personal data is accurate
- Ensuring that the personal data is only retained for as long as it is needed
- Ensuring that the personal data is kept safe and secure
- Accountability - taking responsibility for what you do with personal data and how you comply with the other principles. The Decorum Group must have appropriate measures and records in place to be able to demonstrate compliance

These key principles are explained in more detail in the guidance entitled 'UK GDPR – Key Principles'.

The Decorum Group recognises that in addition to complying with the key principles, The Decorum Group must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance. We understand that we must also adopt 'privacy by design'. This means that data protection issues should be considered at the very start of a project, or engagement with a new Service User. Data protection should not be an after-thought. These ideas are also covered in more detail in the Key Principles Guidance.

**Processing Personal Data**

The position has been improved under UK GDPR in terms of the ability of care sector organisations to process special categories of data. The provision of health or social care or treatment or the management of health or social care systems and services is now expressly referred to as a reason for which an organisation is entitled to process special categories of data.

In terms of other types of personal data, The Decorum Group must only process personal data if it is able to rely on one of a number of grounds set out in UK GDPR. The grounds which are most commonly relied on are:

- The Data Subject has given his or her consent to the organisation using and processing their personal data
- The organisation is required to process the personal data to perform a contract; and
- The processing is carried out in the legitimate interests of the organisation processing the data – note that this ground does not apply to public authorities

The other grounds which may apply are:

- The processing is necessary to comply with a legal obligation
- The processing is necessary to protect the vital interests of the Data Subject or another living person
- The processing is necessary to perform a task carried out in the public interest

The grounds set out above and the impact of the changes made in respect of special categories of data are explained in more detail in the guidance entitled 'UK GDPR – Processing Personal Data'.

**Data Protection Officers**

The Decorum Group understands that some organisations will need to appoint a formal Data Protection Officer under UK GDPR (a "**DPO**"). The DPO benefits from enhanced employment rights and must meet certain criteria, so we recognise that it is important to know whether The Decorum Group requires a DPO. This requirement is outlined in the policy and procedure on Data Protection Officers.

Whether or not The Decorum Group needs to appoint a formal Data Protection Officer, The Decorum Group will appoint a single person to have overall responsibility for the management of personal data and compliance with UK GDPR.

**Data Security and Retention**

Two of the key principles of UK GDPR are data retention and data security.

- Data retention refers to the period for which The Decorum Group keeps the personal data that has been provided by a Data Subject. At a high level, The Decorum Group must only keep personal data for as long as it needs the personal data
- Data security requires The Decorum Group to put in place appropriate measures to keep data secure

These requirements are described in more detail in the policy and procedure entitled Data Security and

Data Retention.

**Website Privacy and Cookies Policy and Procedure**

Where The Decorum Group collects personal data via a website, we understand that we will need a UK GDPR compliant website privacy policy. The privacy policy explains how and why personal data is collected, the purposes for which it is used and how long the personal data is kept. A template website policy is provided.

**Subject Access Requests**

One of the key rights of a Data Subject is to request access to and copies of the personal data held about them by an organisation. Where The Decorum Group receives a Subject Access Request, we understand that we will need to respond to the Subject Access Request in accordance with the requirements of UK GDPR. To help staff at The Decorum Group understand what a Subject Access Request is and how they should deal with a Subject Access Request, a Subject Access Request Policy and Procedure is available to staff. A The Decorum Group process map to follow when responding to a Subject Access Request, as well as a Subject Access Request letter template is also included.

**The Rights of a Data Subject**

In addition to the right to place a Subject Access Request, Data Subjects benefit from several other rights, including the right to be forgotten, the right to object to certain types of processing and the right to request that their personal data be corrected by The Decorum Group. All rights of the Data Subject are covered in detail in the corresponding guidance.

**Breach Notification Under UK GDPR**

We understand, that in certain circumstances, if The Decorum Group breaches UK GDPR, we must notify the ICO and potentially any affected Data Subjects. There are strict timescales in place for making such notifications. A policy and procedure for breach notification that can be circulated to all staff, together with a process map for The Decorum Group to follow if a breach of UK GDPR takes place is available.

We understand that this requirement is likely to have less impact on NHS organisations that are already used to reporting using the NHS reporting tool.

**Fair Processing Notice and Consent Form**

Organisations are required to provide Data Subjects with certain information about the ways in which their personal data is being processed. The easiest way to provide that information is in a Fair Processing Notice. A Fair Processing Notice template is available for The Decorum Group to use and adapt on a case by case basis.

The Fair Processing Notice sits alongside a consent form which can be used to ensure that The Decorum Group obtains appropriate consent, particularly from the Service User, to the various ways in which The Decorum Group uses the personal data. The Consent Form contains advice and additional steps to take if the Service User is a child or lacks capacity.

**Transfer of Data**

If The Decorum Group wishes to transfer personal data to a third party, we understand that we should put in place an agreement to set out how the third party will use the personal data. The transfer would include, for example, using a data centre in a non-EU country. If that third party is based outside the European Economic Area, we recognise that further protection will need to be put in place and other aspects considered before the transfer takes place. Guidance has been produced to explain the implications of transferring personal data in more detail.

**Privacy Impact Assessments**

The Decorum Group must carry out Privacy Impact Assessments each time it processes personal data in a way that presents a “high risk” for the Data Subject. Examples of when a Privacy Impact Assessment should be conducted are provided in the relevant policy and procedure. Given the volume of special categories of data that are frequently processed by organisations in the health and care sector, there are likely to be a number of scenarios which require a Privacy Impact Assessment to be completed.

The Privacy Impact Assessment template may also be used to record any data protection incidents, such as breaches or 'near misses'.

**4.7 Compliance with UK GDPR**

The Decorum Group understands that there are two primary reasons to ensure that compliance with UK GDPR is achieved:

- It promotes high standards of practice and Support, and provides significant benefits for staff and, in particular, Service Users
- Compliance with UK GDPR is overseen in the UK by the ICO. Under UK GDPR, the ICO has the ability to issue a fine of up to 20 million Euros (approximately £17,000,000) or 4% of the worldwide turnover of

an organisation, whichever is higher. The potential consequences are therefore significant.

The Decorum Group appreciates that it is important to remember, however, that the intention of the ICO is to educate and advise, not to punish. The ICO wants organisations to achieve compliance. A one-off, minor breach may not attract the attention of the ICO but if The Decorum Group persistently breaches UK GDPR or commits significant one-off breaches (such as the loss of a large volume of personal data, or the loss of special categories of data), it may be subject to ICO enforcement action. In addition to imposing fines, the ICO also has the power to conduct audits of The Decorum Group and our data protection policies and processes. The Decorum Group realises that the ICO may also require The Decorum Group to stop providing services, or to notify Data Subjects of the breach, delete certain personal data we hold or prohibit certain types of processing.