

**General Data Protection Regulation Policy**

*Adopted: 7th April 2018*

*To be reviewed: March 2019*

**Purpose of the policy and background to the General Data Protection Regulation**

This policy explains to management, staff and the public about GDPR. Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security. This policy updates any previous data protection policy and procedures to include the additional requirements of GDPR which apply in the UK from May 2018. The Government have confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement. This policy explains the duties and responsibilities of the organisation and it identifies the means by which the organisation will meet its obligations.

**Identifying the roles and minimising risk**

GDPR requires that everyone within the organisation must understand the implications of GDPR and that roles and duties must be assigned. Excellent Healthcare Services is the data controller and Director is the Data Protection Officer (DPO). It is the DPO's duty to undertake an information audit and to manage the information collected by the Excellent Healthcare, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information. This will be included in the Job Description of the DPO

Appointing the Director as the DPO must avoid a conflict of interests, in that the DPO should not determine the purposes or manner of processing personal data.

GDPR requires continued care by everyone within the organisation, management and staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the organisation facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as medium risk to the organisation (both financially and reputationally) and one which must be included in the Risk Management Policy of the organisation. Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the organisation undertaking training in data protection awareness.

**Data Breaches**

One of the duties assigned to the DPO is the investigation of any breaches. Personal data breaches should be reported to the DPO for investigation. The DPO will conduct this with the support of the Organisation Management. Investigations must be undertaken within one month of the report of a breach. Procedures are in place to detect, report and investigate a personal data breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will also have to notify those concerned directly.

It is unacceptable for non-authorized users to access IT using employees' log-in passwords or to use equipment while logged on. It is unacceptable for employees, volunteers and members to use IT in any way that may cause problems for the Organisation, for example the discussion of internal organisation matters on social media sites could result in reputational damage for the Organisation and to individuals.

## General Data Protection Regulation Policy

### Privacy Notices

Being transparent and providing accessible information to individuals about how the Organisation uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a organisation does with their personal information. A privacy notice will contain the name and contact details of the data controller and Data Protection Officer, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a privacy notice must be detailed on the Information Audit kept by the organisation. The organisation will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved. All privacy notices must be verifiable.

### Information Audit

The DPO must undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the organisation will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the organisation undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted

### Individuals' Rights

GDPR gives individuals rights with some enhancements to those rights already in place:

the right to be informed

the right of access

the right to rectification

the right to erasure

the right to restrict processing

right to data portability

the right to object

the right not to be subject to automated decision-making including profiling.

The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

If a request is received to delete information, then the DPO must respond to this request within a month. The DPO has the delegated authority from the Organisation to delete information.

If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. The charge will be as detailed in the Organisation's Freedom of Information Publication Scheme. The Management of Organisation will be informed of such requests.

### Children

There is special protection for the personal data of a child. The age when a child can give their own consent is 13. If the organisation requires consent from young people under 13, the organisation must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in language that they will understand.

## General Data Protection Regulation Policy

### Summary

The main actions arising from this policy are:

The Organisation must be registered with the ICO.

A copy of this policy will be available on the Organisation's website. The policy will be considered as a core policy for the Organisation.

The Clerk's Contract and Job Description (if appointed as DPO) will be amended to include additional responsibilities relating to data protection.

An information audit will be conducted and reviewed at least annually or when projects and services change.

Privacy notices must be issued.

Data Protection will be included on the Organisation's Risk Management Policy.

The Management of Organisation will manage the process.

This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.

All employees, volunteers and management are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Organisation.