# Information Handling and General Data Protection Regulation (GDPR) Policy

The policy relates to all ICT facilities and services and their use by all at Caius House including members (clients), employees, volunteers, and any other users of IT. We are committed to the highest standards of confidentiality. All Clients and staff information must be processed fairly, lawfully and as transparently as possible.

Deliberate and serious breach of the policy statements in this section may lead to disciplinary measures in accordance with the Disciplinary and Grievance Policy. The organisation maintains the right to monitor the volume of internet and network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

1. **Confidentiality**

All personal information gathered is to be treated with the utmost confidentiality at all times. Data and information shall not be disclosed to any unauthorised third party without the express consent of the client, or where the client does not have the capacity to make such decision, the client’s appropriate representative or advocate. The only exception to this is if there is a considerable risk to the client if the information or data is not shared and time does not allow for the correct permissions to be sought. All clients have a right to privacy and dignity and that this extends to our handling of information about them in ways which cause as little as possible intrusion on those rights.

1. **Data processing**

Organisations that process personal data, have an obligation to deal with the information in a certain way, which protects the individual whose information it is. Under the GDPR, personal information must be:

1. Processed lawfully, fairly and in a transparent manner.

2. Collected for a specific, explicit, and legitimate purpose and not further processed in a manner that is incompatible with those purposes.

3. Adequate, relevant, and limited to what is necessary in relation to the purpose(s) for which they are processed.

4. Accurate and, where necessary, kept up to date – ensuring that every reasonable step is taken to ensure inaccurate personal data is either corrected or erased without delay.

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, aside from archiving purposes in line with defined retention periods and provided appropriate technical and organisational safeguarding measures are employed.

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, against accidental loss, destruction or damage using appropriate technical or organisational measures.

The Data Protection Officer (DPO) has overall responsibility for confidentiality and information handling in the business that is compliant with data protection law and meets the GDPR. They should continually monitor the service regarding data protection and raise awareness with staff, providing suitable training where needed. The DPO must have suitable knowledge and experience of information handling that is proportionate to the data handled in the business and are responsible for seeking specific training and guidance for themselves regarding data handling, where needed.

It is a requirement of GDPR that a written contract is in place with any appointed data processors to address as a minimum:

1. data is only processed on documented instructions form the controller in all respects

2. persons authorised to process personal data are bound by confidentiality

3. no further third-party processors are engaged by the third party without authority from the controller

4. appropriate technological and organisational safeguarding methods are employed

5. assistance is provided to the controller to respond to data subjects’ exercise of any rights

6. at the controller’s discretion, returns or deletes data at the end of the provision of processing services

7. all information is made available to the controller to demonstrate GDPR compliance

1. **Rights of Individuals**

Under the GDPR, individuals are able to exercise a number of rights regarding their personal data including:

• the right to request access to the personal data held about them.

• the right to request an error in their personal data held is corrected; and

• under certain circumstances, the right to request an organisation stops processing their personal data and that all personal data held about them is deleted.

If a member of staff of receives a subject access request, this request must be promptly (and in any case within 24 hours of receipt of the request) forwarded to the appointed Data Protection Officer (DPO). The requestor must provide ID and the timescale for responding to the requestor does not begin until you are satisfied you know the identity of the requestor. You should respond to a to the requestor within one month or receipt of the request.

1. **Privacy**

In compliance with the GDPR organisations have a responsibility to provide all staff members and clients with a privacy statement which explains the following:

• Who we are

• What information we hold about staff and clients

• How we use staff and client’s data

• Who we share data with

• How we keep data secure

• Reasons that we collect data and use personal information

• Peoples rights regarding their data

• Retention of data

We ensure that everyone knows how their data is stored and used through privacy statements which clearly set this out.

1. **Record Keeping**

All records must be stored in accordance with the GDPR and, at the appropriate time, be destroyed via shredding. The time at which they will be destroyed will depend on the nature of the records and will be in accordance with legislation and codes of practice. It is the management teams’ responsibility to ensure that records are kept for the appropriate amount of time.

1. **Electronic Data**

In order to ensure that electronically stored client’s information is secure, it is essential to follow some basic security measures. Electronic data is not just data that is stored on a PC but is also any information stored on a smart phone, tablet or other mobile device or portable media (e.g. usb drives, external hard-drives and mobile phones) and steps should be taken to protect and safeguard information on any such devices that hold sensitive personal data.

These include:

• Ensuring that an up-to-date internet security program, including Anti-Virus and Firewall is installed on all computers.

• Each computer or device is password protected and encrypted, and that passwords are changed regularly.

• Ensure that users do not share passwords.

• Only allow staff to access the information that is needed.

• Computers are protected by having the latest security patches automatically downloaded and installed.

• When disposing of old equipment, make sure that all data stored is securely and irretrievably destroyed, either with software or by physically destroying the hard drive.

• Encrypting documents which contain sensitive information.

• Make secure, regular back-ups of all data stored.

• Mobile devices are not used or shared with staff family members when they contain personal sensitive information used in the provision of care

• Any files stored on mobile devices have adequate security and encryption in place

• Any mobile devices if lost have the appropriate software or app so that they can be blocked or locked remotely to prevent access to personal sensitive data

• Any mobile device has adequate security when connecting to any WIFI or cloud-based networks

• Personal sensitive data will not be transmitted by a mobile device on any unsecure network or WIFI connection

• Being exceptionally careful when using any form of portable media which contains personal data ensuring that password protection and encryption are used to keep this data secure

For more information about the storage of data and use of mobile devices the Information Commissioners website should be referred to for guidance.

1. **IT Systems and Security**

The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents.

Do not attempt to gain unauthorised access to information or facilities.

Do not disclose personal system passwords or other security details to anyone and do not use anyone else's log-in. If someone else gets to know your password, ensure that you change it.

If you intend to leave your laptop, PC or workstation unattended for any reason, you should lock the screen to prevent unauthorised access. If you fail to do this, you will be responsible for any misuse of it while you are away. Logging off is especially important where members of the public have access to the screen in your absence.

If you are recording or obtaining information about individuals, make sure you are not breaking data protection legislation, and are compliant at all times with the requirements of the GDPR and this policy.

Unacceptable behaviour under this policy includes:

* Sending confidential information to external locations without appropriate safeguards in place.
* Distributing, disseminating, or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.
* Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, constitutes a personal attack, is sexist or racist, or might be considered as harassment or bullying.
* Using copyrighted information in a way that violates the copyright.
* Broadcasting unsolicited personal views on social, political, religious or other non-business-related matters.
* Transmitting unsolicited commercial or advertising material.
* Undertaking deliberate activities that waste employees’ or volunteers’ effort or networked resources.
* Deliberately or recklessly introducing any form of computer virus or malware into the corporate network.
* Visiting internet sites that contain obscene, hateful, pornographic, or other illegal material.
* Using the computer to perpetrate any form of fraud, or software, film or music piracy.
* Using the internet to send offensive or harassing material to other users or to send material that may be regarded as party political campaigning.
* Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
* Hacking into unauthorised areas.
* Creating or transmitting defamatory material.

Treat others with respect and in a way in which you would expect to be treated yourself.

1. **Copyright**

Be aware of copyright law when using content, you have found on other organisations’ websites. The law is the same as it is for printed materials. Take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

1. **Reporting Breaches**

Staff have an obligation to immediately report actual or potential data protection compliance failures to the DPO as soon as they are identified so, we can:

• investigate the failure and take remedial steps if necessary; and

• make any applicable reports to the Information Commissioner or affected individuals

May 2022

Review Date: May 2023