change, grow, live (CGL) policy

Data Protection Policy

Version: 3.0

This document should be read and implemented by:

- **Staff in operational services** (Orange)
  - Team leaders
  - Clinicians
  - Pharmacists
  - Nurses
  - Staff working with service users
  - Staff working in criminal justice services
  - Administrative staff
  - Recovery champion
  - Social workers
  - Peer mentors
  - Volunteers
- **Managers in operational services** (Blue)
- **Staff in central support services** (Pink)
- **Managers in central support services** (Purple)
- **Prescribers** (Green)

This document relates to the:

- **Service user journey**
- **Staff journey**

Purpose and intended outcomes:

During the course of our activities we will collect, store and process personal information about our staff, service users, clients, sessional workers, volunteers etc. This policy sets out how we will ensure that we treat this information in an appropriate and lawful manner.

Protecting personal information appropriately will help CGL to build trust with service users and staff.

Reference number:	cgl/ply/002
Owner/author:	Alison Levy
Responsible Director:	Kevin Crowley
Ratified by:	EMT and CPC
Date ratified:	June 2018
Review date:	April 2019

Other documents to be read in conjunction with this policy:

- Data Protection Toolkit

Related audits and compliance:

- Information Security ISO27001
- Care Quality Commission
- Information Commissioner's Office

Document History and Version Control Record

Version:	Version date:	Name of reviewer:	Review date:	Amendment details
3.0	June 2018	Sorrel Grantham	April 2018	References to Data Protection Bill amended to Data Protection Act 2018.

Contents

1.0 Definitions and terms

Data:	Information which is stored electronically, on a computer, or in paper-based filing systems.
Data processing:	Any activity that involves use of the data. It includes obtaining, recording or holding the data. It also includes carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
Data processors:	Contractors or suppliers who handle personal data on the organisation's behalf.
Data subjects:	All individuals about whom an organisation holds personal data. All data subjects have legal rights in relation to their personal data.
Data users:	Employees whose work involves handling personal data.
DPA:	Data Protection Act.
GDPR:	General Data Protection Regulations
Personal data:	Data from which a living individual can be identified. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).
SIRO:	Senior Information Risk Owner. The SIRO determines the purposes for which, and the manner in which, any personal data is processed.

2.0 Scope

2.1 This Data Protection Policy applies to all employees, agency workers, sessional workers, volunteers, students, self-employed staff, consultants and peer mentors, who in the course of their work for, or association with, CGL will come across, handle or manage CGL data or information.

2.2 This policy applies to all personal data held by CGL. 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.

3.0 Responsibility

3.1 The following have responsibilities or duties outlined in this policy:

- EMT are responsible for approving this policy.
- CGL is the Data Controller of all personal data used within the organisation.
- CGL's SIRO is the Executive Director Quality Innovation and Governance.
- CGL's Data Officer is the Head of Legal Services.
- The SIRO and Data Officer are responsible for ensuring compliance with the Data Protection Act and with this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Officer.
- The SIRO is responsible for establishing practices and policies in line with the Data Protection Act.
- All staff are responsible for ensuring that they follow the requirements of this Data Protection Policy. If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager or one of the people listed below:

3.2 Data Officer - Alison Levy, Head of Legal Services
Email: alison.levy@cgl.org.uk Phone: 01273 645077 / 07841 067774

3.3 SIRO – Kevin Crowley, Executive Director
Email: kevin.crowley@cgl.org.uk Phone: 01273 677019 / 07811 964558

3.4 National Information Security Manager – Sorrel Grantham
Email: sorrel.grantham@cgl.org.uk Phone: 0121 392 7395 / 07469 355963

4.0 Policy

4.1 Personal and Sensitive Data

4.1.1 During the course of our activities we will collect, store and process personal information about our staff, service users, clients, sessional workers, volunteers etc, and we recognise the need to treat it in an appropriate and lawful manner.

4.1.2 Personal data can include an individual piece of data that could identify an individual to others, for example, a full name. It could also include separate pieces of data that on their own would not identify an individual, but that would do so when put together, for example, a first name and an address.

4.1.3 CGL may also collect, store and process sensitive data. Sensitive personal data can only be processed under strict conditions. Sensitive personal data includes information about a person's:

- Racial or ethnic origin.
- Political opinions.
- Religious of philosophical beliefs.
- Trade Union membership.
- Physical or mental health or condition.
- Sex life or sexual orientation.
- Genetic data.
- Biometric data.

4.1.4 Where this policy refers to 'personal' data, this will also include 'sensitive' data, unless stated otherwise.

4.1.5 The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, customers and others 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 Data Protection Act 2018 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

4.1.6 Due to the serious nature and impact any breach of this policy may have for CGL, any breach of this policy will be taken seriously and may result in disciplinary action.

4.2 Data Protection Principles

4.2.1 Anyone processing personal data must comply with the six enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Purposes for processing are specified, explicit and legitimate.
- Personal data shall be adequate, relevant and not excessive.
- Personal data shall be accurate and kept up to date.
- Personal data shall be kept for no longer than is necessary.
- Personal data shall be processed in a secure manner.

4.2.2 **Processed fairly and lawfully**

- The Act is not intended 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 informed how the data will be processed.

- For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for law enforcement purposes.

4.2.3 **Purposes for processing are specified, explicit and legitimate**

- 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.

4.2.4 **Personal data shall be adequate, relevant and not excessive**

- Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. No more than the minimum amount of data should be kept for specific processing. Any data which is not necessary for that purpose should not be collected in the first place.

4.2.5 **Personal data shall be accurate and kept up to date**

- Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate. 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.

4.2.6 **Personal data shall be kept for no longer than is necessary**

- Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, see the Records Management Policy or contact CGL's Data Officer.

4.2.7 **Personal data shall be processed in a secure manner**

- Data processes must put measure in place to protect against unauthorised access of personal data, including protection against unlawful processing or accidental loss, destruction or damage.

4.3 CGL's Legal Bases for Processing Data

4.3.1 CGL has identified the legal basis from Article 6 of the GDPR, under which we will process personal data. The legal basis under which we will process data is **legitimate interests.**

- Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

4.3.2 CGL has identified the legal bases from Article 9 of the GDPR, under which we will process sensitive personal data on service users. The legal bases under which we will process data are: **vital interests; data which is manifestly made public; establishment, exercise or defence of legal claims**; **provision of health or social care; public interest in the area of public health** and **scientific or historical research purposes.**

- 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.

- Processing relates to personal data which is manifestly made public by the data subject.

- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. It must be carried out on the basis of EU or member state law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Article 9(3) of the GDPR.

- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, 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.

4.3.3 CGL has identified the legal basis from Article 9 of the GDPR, under which we will process sensitive personal data on employees. The legal basis under which we will process data is **employment and social security and social protection law.**

- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection 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.

4.4 Criminal Convictions

4.4.1 Processing of criminal conviction data is permitted by Article 10 of the GDPR, where this processing is carried out in a professional capacity.

4.4.2 CGL will request DBS checks on applicants for employment with CGL and on volunteers, where they would have direct contact with service users if confirmed in post. The purpose of this processing is to assess a candidate's suitability for a role.

4.4.3 CGL is required to process information on service user criminal convictions in order to fulfil contracts with service commissioners.

4.4.4 We will processes information on service user criminal convictions where this is relevant to the risk assessment process and treatment / support provided by CGL.

4.5 Data on Children

4.5.1 The GDPR states that data for online services can only be held on children aged under 13 if explicit consent has been gained from somebody with parental responsibility for them. There is an exemption from this need to gain this consent for the provision of preventive or counselling services offered directly to the child, such as services offered by CGL.

4.5.2 Services offered to young people aged under 13 will include psychosocial services and treatment for substance use.

4.5.3 CGL does not provide services to young people where treatment is solely provided online. CGL may use online services to support face-to-face treatment provided to young people, which may include online referral forms and communication via social media.

4.5.4 CGL will accept online referrals on and from children aged under 13.

4.5.5 CGL will use the same legal basis to hold data on young people as for adult service users. CGL has identified 'legitimate interests' as the legal basis for processing personal data, as set out in point 4.3 of this policy. The legal grounds for processing sensitive data are set out at point 4.3 of this policy.

4.5.6 However, CGL will assess whether the child is capable of understanding the implications of CGL processing their data before proceeding with any further engagement with the child. If the child is unable to understand the implications of CGL processing their data, we will seek consent from somebody with parental responsibility in order to process this.

4.5.7 Where CGL provides options for service users to communicate with CGL via social media, CGL will take reasonable steps to confirm that any young people using services are aged 13 or over. CGL will ask the young person to confirm that they are aged 13 or over before engaging in online communications. CGL will not respond to or send any communication to young people known to be aged under 13.

4.6 Data Erasure and Amendment

4.6.1 Data subjects can request that personal data held on them is deleted. CGL will need to consider any requests we receive to delete data. This right to erasure is not absolute and can be declined if we are required to keep the data for legal or contractual reasons.

4.6.2 Data subjects can request that inaccurate data about them is rectified. CGL must consider any requests to rectify inaccurate data.

4.6.3 Children have the same rights as adults over their data, including the right to request rectification, object to processing and to have their data erased. This right to erasure is especially relevant where they gave their consent to processing when they were a child.

4.6.4 Please see the Data Erasure and Amendment Policy for further details.

4.7 Data Security

4.7.1 CGL must 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.

4.7.2 The Act 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. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

4.7.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on central computer systems / databases instead of individual PCs, wherever possible.

4.7.4 Security procedures include:

- Entry controls. Any stranger seen in entry-controlled areas should be reported to relevant management team.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal and sensitive information is always considered confidential.)
- Methods of disposal. Paper documents should be put in the confidential shredding bins provided by CGL, when no longer required. Electronic equipment should be physically destroyed when it is no longer required, via CGL's IT team.

- Equipment. Data users should ensure that individual monitors are not overlooked by passers-by. They must also log off from their PC at the end of each working day and lock their screen if they are away from their desks during the working day. (Users can lock their screen either by pressing 'Ctrl', 'Alt' and 'Delete' together at the same time and then selecting 'lock computer', or by pressing the Windows key and 'L' together).

4.8 Dealing with Subject Access Requests

4.8.1 Data subjects are entitled to request copies of the personal information that CGL holds on them, under the Data Protection Act. These requests are known as Subject Access Requests. A formal request from a data subject for information that CGL holds about them must be made in writing (letter or email). Any member of staff who receives a written request should refer to the Data Protection Toolkit for information on handling these types of requests.

4.9 Breach of Policy

4.9.1 It is a legal obligation for CGL to ensure the organisation and everyone working within it complies with the requirements of the Data Protection Act 2018 together with the arrangements set out in this Policy and the Data Protection Toolkit.

4.9.2 As employees, sessional workers, volunteers, consultants, self-employed workers etc of this organisation, it is your duty to ensure that you are fully aware, understand, and at all times follow the requirements and arrangements for data management within CGL, to ensure the confidentiality of data is protected at all times.

4.9.3 Due to the sensitive and confidential nature of the data we handle on a daily basis within our services and functions, any data loss, breach of confidentiality or breach of policy will require the following actions:

- Notification sent to line management and the National Information Security Manager of the data loss or breach of data/confidentiality incident by employee/individual (see the Data Protection Toolkit for process) as soon as possible (within 24 hours of incident occurring).
- Formal investigation carried out to ascertain full extent of incident and facts.
- Findings confirmed.
- Discipline sanctions applied where findings have been evidenced and confirmed as a serious breach of Policy and the Data Protection Act 2018. The seriousness of the findings will determine the level of discipline sanction to apply, however in the most serious of cases dismissal could be considered as an appropriate sanction.

4.9.4 Further details can be found in the Data Protection Toolkit.

5.0 Review

5.1 This policy will be reviewed annually by the Data Protection Officer and SIRO.

6.0 Assessments

6. 1 The following assessments were undertaken with agreed and appropriate measures incorporated into this policy:

- Information security assessment.
- Equality impact assessment.

7.0 Records retention

Appropriate records will be retained in accordance with the Records Management Policy (CGL/PLY/124) – link: http://intranet.cgl.org.uk/policy_library/documents/5521/policy/records_management_policy_cglply124_v11

8.0 Document History

Version:	Version date:	Name of reviewer:	Review date:	Amendment details
2.0	April 2013	Alison Levy	April 2013	Document control information added and recorded in QMS.
2.1	April 2014	Alison Levy	April 2014	Annual Review no changes
2.2	August 2015	Paul O'Neill	August 2015	New Responsible Director assigned & reviewed
2.3	April 2016	Paul O'Neill	April 2016	Re-branded to CGL
2.4	August 2016	Alison Levy	August 2016	Review of document
2.5	August 2017	Alison Levy	August 2017	Annual review – content unchanged. Review and update in line with GDPR requirements to take place by end of December 2017.
2.6	January 2018	Sorrel Grantham	January 2018	Review against GDPR requirements. All content to up updated in line with GDPR by end of May 2018.
2.7	March 2018	Sorrel Grantham	January 2018	Updated to meet the requirements of the Data Protection Bill 2018.
2.8	April 2018	Sorrel Grantham	April 2018	Section 4.3.2 updated to include processing on the grounds of public interest in the area of public health and scientific or historical research purposes.
2.9	May 2018	Sorrel Grantham	April 2018	Section 4.4 on criminal convictions added. Section 4.5 on storing data on young people updated.