The Institute
Training and education for Guernsey's Health & Social Care

Data Protection Policy

Version 2

July 2021

Version	Date	Revisions	Author	Next Review
1	April 2021	First Issue	Samantha Nichols	
2	July 2021	Tracey McClean		July 2022

1. Introduction & objectives of this policy

In order to satisfy its operational and legal obligations, the Institute of Health & Social Care Studies ('IHSCS') is required to process personal data about living individuals. It is essential that personal data is processed in accordance with the requirements laid down in the Data Protection (Bailiwick of Guernsey) Law, 2017 ('the Law').

The Bailiwick of Guernsey is not an EU Member State and therefore the GDPR does not apply here, however, in order to ensure that the same level of protection is provided to Bailiwick residents, and in order to continue to ensure the free flow of personal data outside of the Bailiwick, "adequacy" in the eyes of the EU must be maintained in terms of our data protection regime.

In order to maintain adequacy for the Bailiwick, the Data Protection (Bailiwick of Guernsey) Law, 2017 was drafted which essentially mirrors the provisions of the GDPR. The 2017 Law was approved by the States of Deliberation in November 2017 and is enforceable as of 25 May 2018 which coincides with the enforcement of the GDPR within the EU.

This policy has been created in line with States of Guernsey directives and guidance and takes into consideration guidance from the ICO, ODPA and policies from our partner Universities.

The objectives of this policy are as follows:

To ensure that:

- Proper procedures are in place for the processing and management of personal data;
- There is someone within the organisation who has specific responsibilities for data protection compliance;
- A supportive environment and culture of best practice processing of personal data is provided for staff;
- All staff understand that their responsibilities when processing personal data and that methods of handling that information are clearly understood;
- Individuals wishing to submit a subject access request and exercise any of the other individual rights are fully aware of how to do this and who to contact;
- Staff understand that subject access requests (and other data subject requests) need to be dealt with promptly, courteously and within the legally required timeframe;
- Individuals are assured that their personal data is processed in accordance with the data protection principles, that their data is secure at all times and safe from unauthorised access, alteration, use or loss;
- Other organisations with whom personal data needs to be shared or transferred,

meets compliance requirements; and

- Any new systems being implemented are assessed using a Data Protection Impact Assessment to determine whether they will hold personal data, whether the system presents any privacy risks, damage or impact to individuals' data and that it meets this policy's requirements.

2. Scope and Status of the Policy

All IHSCS staff and students are expected to comply with this policy.

Definitions and terms used in relation to the Data Protection Law and GDPR can be found at: Glossary · ODPA

This policy applies to all personal data and special categories of data (sensitive personal data) collected and processed by IHSCS in the conduct of its operations, in electronic format and in any medium and within structured paper filing systems.

This policy applies to all IHSCS employees (whether permanent, temporary, contractors, or consultants) and students.

Disciplinary action may be taken against staff failing to comply with this policy.

Any member of staff or student who considers that the policy has not been followed in respect of personal data should raise the matter with their Line Manager or their Programme Lead in the first instance, or alternatively, directly with the Data Protection Officer for ESC.

3. The Data Protection Principles

The data protection requirements laid down in the Law are known as the data protection principles, which are essentially rules of good information handling. IHSCS is committed to adhering to these principles and does its utmost to ensure that its employees comply with them.

The principles require that personal data shall:

1. Be processed fairly, lawfully and transparently

2. Be processed for a specified and lawful purpose(s) and must not be further processed in any incompatible manner (Purpose Limitation)

3. Be adequate, relevant and not excessive for those purposes (Minimisation).

4. Be accurate and, where necessary, kept up to date (Accurate)

5. Not be retained for longer than is necessary for the purpose for which it is processed (Storage Limitation)

6. Be processed in a manner that ensures its security appropriately, including

protecting against unauthorised or unlawful processing, loss, destruction or damage (Integrity and Confidentiality)

7. The controller is responsible for ensuring that data is processed in accordance with the rights of individuals and must be able to demonstrate compliance with the data protection principles (Accountability).

These principles align with the data protection principles laid out in Article 5 of the General Data Protection Regulation ('GDPR').

4. Data Subject Rights and requests

The Law also gives individuals certain rights, which are set out in Part III of the Law. These rights are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

For more information on the rights of data subjects, please see www.gov.gg/dp

4.1 Handling a data subject request

The most common data subject requests are:

- **Subject Access Requests -** To request access to personal information, either by viewing it or being provided with a copy of it; is known as a Subject Access Request. For more information on how to handle a Subject Access Request, please see the full guidance provided by the Data Protection Team on the Bridge (click here).

- **Data rectification requests** – Very often, people forget to update their information when they change address, update their contact details, etc. If a data subject requests that their information is updated and/or rectified, you have one calendar month in which to do this.

- **Data deletion/erasure requests –** This is exactly what it sounds like, a request to remove data from our systems and/or to cease processing data.

It is important that staff and students recognise these requests and that there is a one month period in which to fulfil these. Requests may be received in email form, verbally or via the States of Guernsey Data Protection page which has online forms for data subjects to complete. Individuals can exercise this right by making the request in writing or verbally to any member of staff. The data requested must be provided within one calendar month of the request being verified, though in certain circumstances a Controller may request an extension of a further two months to complete this.

The DPO should be informed of all data subject requests as soon as possible. They will log these on a central database and will provide you with full guidance and instruction as to what steps should be followed in order to fulfil the request.

In line with the MoCs in place with our Partnership Universities, it may be necessary to inform the University if/when a data subject request is received. Again, your DPO will advise you on this.

Please note: There are some exceptions to the right of individuals. These exemptions are detailed in full in Schedule 8 of the Law. If you are unsure as to whether a data subject's request can be completed or if their request is exempt, please contact your DPO who will be able to advise you accordingly.

5. Policy Principles

In order to meet the requirements of the data protection principles and individual rights set out in the Law, IHSCS adheres to the following values when processing personal data:

5.1 Fair Collection and Processing

- The specific conditions contained in Part II of the Law regarding the fair collection and use of personal data will be fully complied with.

- Individuals will be made aware that their information has been collected, and the intended use of the data specified either on collection or at the earliest opportunity following collection through relevant Fair Processing Notice, which can be found on IHSCS's website: http://theinstitute.gg/GDPR. A paper copy is also available on request.

- Staff will advise the Data Protection Officer in the event of any intended new purposes for processing personal data. The Data Protection Officer will then arrange for a Data Protection Impact Assessment to be conducted. This is a lawful requirement.

- Personal data will be collected and processed only to the extent that it is needed to fulfil business needs or legal requirements. If IHSCS wishes to process

personal data for any additional purposes then there must be a legal reason to do so, and consent for this may need to be sought from the individuals concerned.

- Personal data held will be kept up to date and accurate, where necessary. Individuals will regularly be given the opportunity to correct /update their information.

- Information will not be retained for no longer than is necessary, i.e. when there is no legal reason for retaining the information it must be disposed of. There may be a legal obligation to retain certain categories of data for a specified period. Retention of personal data will be appraised and risk assessed to determine and meet business needs and legal requirements, with the appropriate retention schedules applied to that data which take into account requirements from Partner Universities, examination boards and Colleges.

- Personal data will be processed in accordance with the rights of the individuals about whom the personal data are held.

- Students and staff at IHSCS must take the appropriate technical and organisational measures to safeguard the security of personal data.

- A lawful basis for processing any personal data will be documented fully both on the organisation's Information Asset Register and on the Fair Processing Notice.

- Staff will advise the Data Protection Officer in the event of any intended new purposes for processing personal data. The Data Protection Officer will then arrange for a Data Protection Impact Assessment to be conducted. This is a lawful requirement.

5.2 Security

- Appropriate technical, organisational and administrative security measures to safeguard personal data will be in place.

- The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage and that both access and disclosure must be restricted.

- Any unauthorised use of corporate email by staff, including sending of sensitive or personal data to unauthorised persons, or use that brings the IHSCS into disrepute will be regarded as a breach of this policy.

- Relevant Data Protection Awareness Training will be provided to staff to keep them better informed of relevant legislation and guidance regarding the processing of personal information. Data protection training will also promote awareness of the IHSCS's data protection and information security policies,

procedures and processes. Staff are strongly encouraged to complete this training during induction and subsequently on an annual basis.

5.3 Sharing and disclosure of personal information

- Regular information sharing with third parties, where there is a valid business reason for sharing information, shall be carried out under a written agreement setting out the scope and limits of sharing. Data Processing Agreements will be applied to all contracts and management agreements where IHSCS is the data controller contracting out services and processing of personal data to third parties (data processors). These agreements will clearly outline the roles and responsibilities of both the data controller and the data processor.

- All data processors shall agree to conform to this policy and the Law and as far as possible, indemnify IHSCS against any prosecution, claim, proceeding, action or payments of compensation or damages without limitation and provide any personal information specified on request to the Data Protection Officer.

- As part of its Fair Processing Notice, IHSCS will inform individuals of the identity of third parties to whom we may share, disclose or be required to pass on information to, whilst accounting for any exemptions which may apply under the Law and other relevant legislation.

- Personal data will not be transferred outside the European Economic Area unless that country or territory can ensure a suitable level of protection for the rights and freedoms of the data subjects in relation to the processing of their personal data.

- Data sharing agreements may exist between some States Committees. A Data Sharing Agreement is designed to provide guidance to members of staff in order to ensure that the sharing of personal data between their areas complies with the requirements of the Data Protection (Bailiwick of Guernsey) Law, 2017 (the Law). A data sharing agreement is a requirement of the Law and is designed to outline the parameters of the lawful sharing of personal data between relevant parties. It is important to note though, that these agreements are **not legally binding** and do not replace the need for a lawful basis when processing data.

If you are unsure whether you need a data sharing agreement to share and process data, speak to your Data Guardian and/or Data Protection Officer.

5.4 Access to data

Members of staff and students will have access to personal data only where it is required as part of their functional remit.

Staff and students are reminded that in the event of a Subject Access Request being received by IHSCS and/or The Partner University, their emails may be searched, and relevant content disclosed, whether marked as personal or not.

6. Personal data breaches and security concerns

A Personal Data Breach is anything that leads to the loss, altering, destruction, unauthorised disclosure of or access to personal data. It is not necessarily the result of a deliberate act: accidents (for example, sending an email containing personal data to the incorrect recipient) are also personal data breaches.

Some common examples are as follows:

- Supplying personal data to an incorrect recipient
- Alteration to or accessing of personal data without permission
- Personal data being stored in areas where the necessary security measures are not in place (e.g. filing cabinets left unlocked or electronic files stored in areas that are not password protected)
- Lost or stolen IT equipment
- Deliberate or accidental loss or destruction of personal data

All breaches must be reported via the Breach Form and submitted to the Data Protection Officer for Education Sport & Culture as soon as they occur. Your DPO will log the breach on a central log and provide you with a reference number. They will also score the breach for severity and will provide you with guidance as to whether further action is required.

The Data Protection (Bailiwick of Guernsey) Law, 2017, makes it mandatory to report any data breaches likely to result in a high risk to the rights and freedoms of individuals to the Data Protection Authority without undue delay and not later than 72 hours after becoming aware of a breach The DPO will advise as to whether the breach needs to be reported to the Office of The Data Protection Authority ('ODPA'). If this is the case, it must be reported to the ODPA within 72 hours of the breach occurring, so **it is imperative that you report any breach as soon as you discover it.** Ignoring or not disclosing a breach could result in IHSCS being investigated and potentially, sanctioned, reprimanded or fined by the ODPA, which has the right to terminate all data processing it deems unlawful.

There will also be circumstances where the impacted individuals must also be notified of the breach.

Breaches should be reported on the Corporate Breach reporting form, which can be found on The Bridge – please click here.

7.0 Roles and responsibilities

Depending on whether you are a staff member or student, you will have different responsibilities under the Law. It is important that you understand these and also that you are aware of the other relevant staff who hold specific roles. Contact details for these key staff are provided in section 8 of this policy.

7.1 The Data Controller

The Law defines a Data Controller as a legal entity that determines what personal information is needed to carry out its functions and has overall responsibility in specifying the manner in which the data is processed.

The Data Controller (Controller) is the organisation, IHSCS, who assumes the responsibility for compliance. The Controller holds ultimate responsibility for compliance with the Law and is responsible for:

- Determining the purposes for which personal data is processed.
- Ensuring appropriate security is in place to protect personal data.
- Ensuring contracts in writing that include security provisions are in place with any Data Processors.

The Head of the Institute is the nominated representative as the Data Controller.

7.2 The Data Protection Officer

The States of Guernsey Corporate Data Protection Team is responsible for advising on the States of Guernsey's compliance with local data protection legislation. The team is made up of eight officers including the Head of Data Protection, two Senior Data Protection Officers who have responsibility for data protection within Health & Social Care and Home Affairs and five Data Protection Officers who together have responsibility for the remaining SoG Committees.

The Data Protection Officer ('DPO') role is set out in the Law (sections 50 and 51). The DPO has responsibility for advising relevant employees of their duties relating to Data Protection and monitoring compliance with the Data Protection (Bailiwick of Guernsey) Law, 2017.

The Data Protection Officer is responsible for:

- Informing and advising staff of their duties under the Law
- Monitoring compliance with the Law and related Policies
- Reviewing data protection procedures on an annual basis
- Ensuring that appropriate records of information assets that contain personal data are held and maintained;
- Advising on the carrying out of Data Protection Impact Assessments for large-scale or high-risk projects that process personal data or change the way personal data is processed and to be the conduit to the Data Protection Authority for consultation;
- Assisting in the process of reviewing contracts or agreements with processors that may process personal data;
- Reviewing the release of information from Subject Access Requests to ensure that exemptions have been appropriately applied;

- Arranging data protection training and awareness for staff;
- Reporting any data protection breaches to the relevant Controller;
- Preparing statistics on breaches, SARs and other data protection matters to the Controller;
- Advising on procedures to reduce the occurrence of data protection breaches; and
- Ensuring that staff are aware of specific Data Protection policies that may exist in their Office or Service Area.

7.3 Data Guardians

The States of Guernsey have appointed Operational Data Guardians with the responsibility for providing support within each area of the Organisation, to ensure compliance with the Data Protection (Bailiwick of Guernsey) Law, 2017. The role of the Data Guardian is to:

- Assist the DPO with reviewing data protection procedures on a regular basis;
- Record information assets that contain personal data;
- Forward data subject requests to the Data Protection Officer;
- Assist the Data Protection Officer to undertake Privacy Impact Assessments on major projects or service changes that require new processing of personal data or change the way personal data is processed;
- Assist the Data Protection Officer in providing data protection advice and training to staff;
- Report data protection breaches to the Data Protection Officer and, when appropriate, the Office of the Data Protection Authority;
- Assist the Data Protection Officer in preparing relevant statistics on breaches, Subject Access Requests and other data protection matters and providing these to the Data Protection Officer and the CIO; and
- Ensure that staff are aware of any specific Data Protection policies that may exist in their Office or Service Area as well as the States of Guernsey Directive on Data Protection.

7.4 All staff

All staff should be adequately trained and are responsible for understanding their contractual requirements, ensuring that: -

- Any personal data which they hold is kept securely; for example:

a. data is protected against being destroyed or corrupted;

b. unauthorised persons cannot read computer screens;
c. passwords are changed on a regular basis;
d. discarded data is disposed of appropriately;
e. appropriate contractual arrangements are in place where processing is carried out by a third party.

- They comply with the ICT Security Directives in respect of personal data and its security by having signed the Acceptable Use Directive;

- Personal information is not disclosed either verbally, in writing or otherwise, to any unauthorised third party;

- They are familiar with and comply with this policy.

- Ensure that information provided in connection with employment is up-to-date and accurate.

- Observe and comply with the data protection principles and individuals' data protection rights.

- Bring queries and issues around data protection to the attention of the Data Protection Officer for ESC.

- Do not attempt to gain access to information that is not necessary to hold, know or process.

- Report all data subject requests and personal data breaches to the Data Protection Officer for ESC as soon as possible.

Note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. It may also result in a personal liability for the staff member as there is provision within the legislation to prosecute individuals for certain offences.

If staff are unsure about any aspect of data protection, they should contact their Data Guardian or Data Protection Officer for advice.

If, as part of their responsibilities, staff collect information about other people, they must comply with the policy. Staff must be made aware of this policy and a record will be kept of the member of staff's verification that they have been made so aware.

7.5 All students

- Be familiar with and the policy and comply where necessary;

- Ensure that personal information provided is up-to-date and accurate;

- Observe and comply with the data protection principles and individuals' data protection rights; and

- Note that unauthorised disclosure of personal data will usually be a disciplinary

matter.

Any questions or concerns about the interpretation or operation of this policy should, in the first instance, be addressed to Course Administrator.
Student guide

8. Key contacts

Role	Contact details
Data Controller for IHSCS	Tracey McClean tracey.mcclean@gov.gg 07781414415
Data Protection Officer for ESC	Samantha Nichols CIPP/E Data.protection@gov.gg 01481 220012
Data Guardian for IHSCS	Samantha Harris Samantha.harris@gov.gg 07781191986

9. Training and resources

- The Data Protection Team has a page on the Bridge which provides guidance materials and instructions on all things data protection. They also produce a regular newsletter which explains how the Data Protection Law works in practise and how it affects you, both as a staff member, student and data subject. The States of Guernsey Data Protection Bridge page can be found here.

- Online Data Protection Training module can be accessed by visiting your MetaCompliance account. If you are not sure of your login details, please speak to InfoSec infosec@gov.gg

- The States of Guernsey Data Protection page (www.gov.gg/dp) provides further information for members of the public requiring assistance with SoG related data protection concerns.

- The Office of The Data Protection Authority website (www.odpa.gg) provides guidance to individuals and businesses. They have podcasts and easy to read guidance which covers lots of different topics.