Information Governance Strategy For GSF Centre CIC

Victoria Mews
8 & 9 St Austin's Friars
Shrewsbury, SY1 1RY

Tel: 01743 291891
Email: info@gsfcentre.co.uk

1 Version Control

This document was prepared for GSF by Professor Alan Gillies, Hope Street Centre CIC

Status:	Final
Created on:	12 July 2011
Last modified:	2 Sept 2011
Version:	1.0
Accepted for implementation by the Board on:	
Signed off as implemented by the Board on:	

2 Table of Contents

3 Introduction

3.1 The Gold Standard for Information Governance

We will seek to meet or exceed all legal, ethical and regulatory requirements in respect of looking after the personal information that we hold on behalf of our clients, staff and the general public.

3.2 The Gold Standard Commitment to Protecting Personal Information

We will:

1. Process all personal data fairly and lawfully

2. Obtain personal data only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

3. Obtain only personal data that is adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

4. Ensure that the personal data we collect and hold will be accurate and, where necessary, kept up to date

5. Not keep the personal data processed for any purpose or purposes for longer than is necessary for that purpose or those purposes

6. Process all personal data in accordance with the rights of data subjects under the Data Protection Act

7. Take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

8. Not transfer personal data outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3.3 Actions to be undertaken

This strategy has been influenced by the fact that GSF is seeking to meet and exceed the expectations of a wide range of clients and regulators, including the NHS, CQC, care home providers patients and carers. Therefore, this strategy is based primarily upon the requirements of the 1998 Data Protection Act with additional requirements when required by the environment in which GSF operates. It uses BS10012 to define its scope.

In support of the main strategy, the document also provides more detailed policies on the following key sections:

- Privacy notice
- Information Security Policy
- Electronic Communication System policies
- Annual audit checklist
- Managing data for ADA
- Implications for other management areas

4 A system to protect the information held by the GSF Centre

The law distinguishes between personal data and data which are not identifiable to a specific individual. It also requires any organisation to identify high risk personally identifiable information and to take specific precautions commensurate with the risk of harm associated with that information. Even information that is not personally identifiable may have significant value to the CIC, such as financial data.

Therefore, GSF undertakes to take all reasonable steps to keep all data private and to ensure that protection measures are commensurate with the value of the information and the risk and extent of harm arising from any potential breach.

GSF has identified 38 requirements to develop a system that could satisfy BS10012:

4.1 Senior management responsibility

A member of the Board has been designated as accountable for the management of personal information within the organisation. Hereafter, they are referred to as the Data Controller in accordance with Information Commissioner Office practice. They will present an annual report to the Board detailing the results of an annual review of information governance carried out in accordance with this policy and the proforma included in the Appendices.

4.2 Responsibility for compliance with the policy on a day to day basis

A member of staff has been designated as responsible for compliance with the policy on a day to day basis. Hereafter, they are referred to as the Data Manager in this policy. They will liaise with the Data Controller and assist them in the preparation of the annual report to the Board and the annual audit of information governance practice.

4.3 Future network of data protection representatives when appropriate

GSF works with a variety of partners to a greater or lesser extent including the regional training centres, care homes, NHS facilities. GSF will maintain a database of designated staff responsible for liaison over information governance issues, and ensure that all these staff have received and acknowledged receipt of this information governance policy.

4.4 Inventory of the categories of personal information

GSF has carried out an audit of the personal information held by the organisation. A list of the types of personal data held by the CIC is held by the Data Manager.

4.5 High-risk categories of personal information

The audit of information revealed that GSF held little high risk personal data beyond that of any business. The one category of data identified as high risk was the data collected and processed for After Death Audits (ADAs). This was the subject of discussion with Prof Gillies

over what was required to take all reasonable steps to protect this information. The results of this discussion and investigation are appended to this document.

4.6 Staff competence

GSF has ensured that all staff have seen and read this document. The implications of this document have been discussed with all staff. GSF is committed to ongoing staff training to ensure that all staff are aware of their obligations and are competent to carry them out. This policy forms part of the staff handbook which will be given to all new and existing staff when published.

4.7 Risk assessment

GSF has considered the level of risk associated with the types of information it uses and the purposes for which they are used. This risk assessment informs this document, and will be reviewed annually or sooner if significant changes occur which affect the type of information held, the purpose for which it is used or the manner in which it is stored, processed or distributed.

4.8 Updating compliance with the data protection legislation and good practice

GSF uses advice from sector bodies such as Forum of Private Business to advise of legislative changes which relate directly to information e.g. 2011 changes to rules regarding the disclosure and consent to the use of cookies, or legislation with implications for information eg 2010 Equality Act. In addition to ongoing monitoring, the annual review will specifically check for relevant changes.

4.9 Notification procedure

GSF has been registered with the Information Commissioner's Office since 09/02/2011. At the introduction of this policy, the scope and timeliness of this registration has been checked, and will be reviewed annually or sooner if significant changes occur which affect the type of information held, the purpose for which it is used or the manner in which it is stored, processed or distributed.

4.10 Procedures to ensure that the organisation processes personal information fairly and lawfully

GSF is committed to ensuring that all personal information is processed fairly and lawfully: this is to be achieved through:

- Implementation of this strategy and its associated policies;
- Dissemination to all new and existing staff of their obligations and responsibilities;
- Explicit contractual obligations in staff employment contacts to conform to information governance processes

- Annual review of all procedures, adverse events and near misses, and changes to the legislative and operating environment which might impact on information governance; and
- Clear responsibility for information governance lodged with the Data Controller and signed off by the Board of Trustees.

4.11 Records of privacy notices and online privacy statements

The Data Manager will keep records of the content, revisions and location of privacy notices and online privacy statements and act on any user feedback over their availability and accessibility.

The privacy notice will include information about the use of tracking of usage through devices such as cookies to meet the latest legislative requirements. A privacy notice is appended to this document which meets these requirements at the present time, and will be reviewed annually or sooner if significant changes occur which affect the type of information held, the purpose for which it is used or the manner in which it is stored, processed or distributed.

4.12 Privacy notice or online privacy statements availability

GSF will provide privacy notices where personal information is collected and also on the website. All GSF emails will carry a link to the privacy notice in their signatures. In addition, any person submitting personal information to GSF on paper will receive a copy of the privacy notice.

4.13 Privacy notice or online privacy statements accessibility

GSF will seek to ensure that the privacy notice is written in plain English and is jargon-free. Where the privacy notice is made available online, it will conform to the same accessibility standards as the main website.

Where GSF receives a specific request for a privacy notice in another language or format, it will do so provided that this can be achieved without excessive cost, taking all reasonable steps as defined in equality and disability legislation.

4.14 Collection from third parties

GSF will seek to ensure that all personal data collected from third parties, is collected in a manner consistent with GSF's own information governance procedures, and therefore in accordance with legislation. Where GSF enters into a contractual relationship with a third party, this will be written into any contractual agreement.

4.15 Check for breaches or potential breaches of any legal obligations

The Data Manager will regularly check for breaches or potential breaches of any legal obligations. In particular, they will check all contractual agreements conform to GSF's own information governance policy and do not compromise GSF in any way.

As part of the annual review, they will record any breaches or near-misses and what has been done in response. Staff are encouraged to raise any issues or concerns they may have with the Data Manager before acting in a manner which may compromise GSF's commitment to the highest standards of information governance.

4.16 Consent for new purposes

Where information is to be used for a new purpose, the purpose will first be considered to establish whether there is a reasonable expectation of use for that purpose based on existing usage. The Information Commissioner provides the following additional guidance on this area.[1]

Where there is doubt about whether a new purpose is a related purpose for which prior consent exists, GSF will seek new consent before proceeding.

---

[1] *It depends on whether it would be fair to do so. You should explain why you want to use an individual's personal data at the outset, based on your intentions at the time you collect it. If over time you devise new ways of using that information, perhaps because of changes in technology, you will be able to use their personal data for the new purpose if it is fair to do so.*

Example

A mail-order book and record seller has had some customers for many years and has regularly sent them catalogues of books and records. After a while the company also started selling audio tapes, CDs and DVDs. It is likely to be fair to start sending catalogues advertising DVDs to long-established customers, who are unlikely to be surprised that the company has diversified. However, customers are less likely to consider it reasonable if the company uses the interests they have shown by their purchases to promote another company's themed holidays (for example, holidays in Salzburg for opera buffs). Passing details of customers and their interests to other companies for marketing is likely to be unfair unless they have agreed to this.

Example

A bank records information about some of the individuals who are shareholders of its corporate account holders. It collects and holds this information to comply with its duties under anti-money laundering regulations. Unless the bank had obtained their prior consent, it would be unfair to use this information to send marketing material to the individuals concerned inviting them to open personal accounts with the bank.

4.17 Sharing personal information with another organisation

GSF does not sell personal data. In some limited cases, information may be shared with third parties for specified legitimate purposes. Where this occurs, it will be made explicit at the time of collection so that individuals concerned can be treated fairly, and can choose whether or not to enter into a relationship with the organisation sharing it.

Data is not deemed to have been shared or transferred where it is simply being stored or processed remotely by GSF employees, although in such cases, GSF will ensure that the security arrangements comply with GSF governance standards.

4.18 Matching with other personal information to create an enhanced profile

From its own investigations, GSF has identified that specific data items collected under ADA could result in information becoming personally identifiable by combining different fields. This is not required by the ADA process and therefore, GSF takes the following steps to prevent inappropriate disclosure.

Externally, no third party will be supplied with a combination of data sufficient to identify an individual.

Internally to GSF, a single designated individual has access to this combination of data and they are not authorised to combine data in this way. Details of how GSF protects its ADA data are appended to this document.

4.19 Personal information is adequate for the organisation's purposes

GSF has reviewed the information it holds to ensure that it is sufficient for the organisation's purposes and will be reviewed annually or sooner if significant changes occur which affect the type of information held, the purposes for which it is used or the manner in which it is stored, processed or distributed.

4.20 Minimum amount of personal information processed

As part of establishing this strategy, GSF considered the personal information it holds. Recommendations were made in those areas where the information held did not need to be personally identifiable, and will be reviewed annually or sooner if significant changes occur which affect the type of information held, the purposes for which it is used or the manner in which it is stored, processed or distributed.

4.21 Maintenance of the integrity and accuracy of personal information being processed

The data held by GSF is not rapidly changing, but some will change over time. GSF will contact those people whose email addresses it holds with consent annually to ensure that they still wish GSF to retain this data and to check that the information is still accurate.

Where the data subject objects or the email is no longer current, the email details will be deleted, otherwise the details will be retained.

Data relating to accreditation will be re-examined at re-accreditation to ensure its continuing accuracy.

GSF undertakes to update personal information promptly when the subject of that information informs them that the data is inaccurate or out-of-date.

4.22 Retention schedules for personal information

Data will only be held as long as is needed.

Portfolios of evidence for accreditation will be stored for 3 years and destroyed/returned to the home.

Information regarding job applications will not normally be retained for unsuccessful applicants, and information from successful applicants will be transferred to personnel records. In exceptional cases, information from an unsuccessful candidate with rare expertise may be retained, provided specific consent is obtained from the candidate.

4.23 Respecting individuals' rights in relation to their personal information

Individuals have the right to query whether GSF holds any personal information regarding them, and no personal data will be collected without the subject of that data being informed that the data is being collected.

GSF makes only very limited use of cookies, and does not actively analyse data from cookies other than for the smooth running of the website. Requests or complaints from individuals will be dealt with promptly and courteously. Requests and complaints will be reviewed annually.

4.24 Complaints procedure about the processing of personal information

The GSF website and privacy notice provide information about how individuals can request information or complain about the personal information held about them.

GSF will:

- Request sufficient information to reasonably verify that the contacting person is the subject of the data request
- Will aim to confirm receipt and verification of identity to the contacting person within 48 hours
- Will aim to deal with the request and inform the data subject within two weeks of the original request

The Data Manager will annually monitor the number of requests, the actions taken and the performance in terms of meeting the targets for a timely response.

4.25 Security Controls

GSF has developed specific security controls appropriate to the type of personal information being processed; and to the risk of damage or distress to the individuals if the information is compromised.

Details are provided in the appended security policy which forms part of the staff handbook for existing staff and induction for new staff.

The security controls and the policy which describes their use will be reviewed annually or sooner if significant changes occur which affect the type of information held, the purposes for which it is used or the manner in which it is stored, processed or distributed. It will also be reviewed in the event of security breaches or reported “near misses”.

4.26 Personal information is stored and handled securely

GSF recognises that secure information handling and storage is not just about systems and security measures, it is also about staff behaviours and their appreciation of the implications and risks associated with those behaviours.

GSF is seeking to establish a culture in which personal information is stored and handled securely as a routine part of the way that GSF operates.

This will be encouraged through training and by the management demonstrating good practice in this area.

4.27 Secure transmission of data

Where data is transmitted, GSF will take steps to ensure its security and privacy.

GSF will:

- Not use faxes or SMS text to transmit personal or sensitive data
- Where files are transmitted over email, they will be password protected and the password sent in a separate email
- Where the file contains high risk data, the password will be transmitted via a different media, typically SMS text or voice call. The password communication should not contain any other information, and if SMS text is used, prior consent should be obtained from the recipient

The security of data transmissions will be reviewed annually or sooner if significant changes occur which affect the type of information held, the purposes for which it is used or the

manner in which it is stored, processed or distributed. It will also be reviewed in the event of security breaches or reported “near misses”.

4.28 Access restricted to those workers who require such access as part of their role

GSF only provides access to staff requiring that information for their role.

In particular, access to high risk potentially personally identifiable combinations of data within ADA is restricted to a designated individual.

In addition, due to the physical layout of the GSF office being open plan, GSF policy is, for staff who will be away from their work stations for more than 5 minutes, to log out of their workstations.

After 10 minutes of inactivity, workstations will lock users out until their password is entered, to prevent inappropriate access to data.

Role-based access rights and the restriction of unattended workstations will be reviewed annually or sooner if significant changes occur which affect the type of information held, the purposes for which it is used or the manner in which it is stored, processed or distributed. They will also be reviewed in the event of security breaches or reported “near misses”.

4.29 Routine review of security controls

All security controls will be reviewed annually or sooner if significant changes occur which affect the type of information held, the purposes for which it is used or the manner in which it is stored, processed or distributed.

4.30 Management of security incidents involving personal information

All security breaches or reported near misses will be investigated by the Data Manager, and reported to the Data Controller. Remedial action will be taken as required. Minor incidents without serious repercussions will be reported as part of the annual review: more major breaches will be reported to the Board at the first opportunity.

4.31 Transfer of personal information outside the EEA

Currently GSF does not transfer personally identifiable data outside the EEA. Should this become a business requirement in the future, and if the intended destination is outside the EEA or the list of allowed countries (see appended list), then explicit consent would be sought.

If the transfer is inside the EEA or to a country on the list, then standard governance processes for third party transfers will be used.

4.32 Third parties' evidence of their right to access personal information

GSF has a responsibility not to disclose to people personal information, unless they are the subject of that data. Therefore, personal information will not be given out without suitable verification of identity.

The nature of GSF business is such that personal information is not normally required to be given out over the telephone, and should be limited to:

- Basic non-critical information such as diary information where the recipient is known to the organisation

Email addresses provide a degree of confidence about the identity of the recipient but fax and SMS text numbers cannot be assumed as evidence of identity as they are often in open environments. A signed letter offers a degree of legal protection, and is the preferred method of communication in terms of confirming identity of the person requesting the information.

Personal information will not be given out to relatives or carers of data subjects without signed written permission from the subject themselves

4.33 Selection of providers that meet the requirements of the organisation

GSF will ensure that, where information is processed on its behalf by another organisation(s), they select only providers that can provide technical, physical and organisation security which meet the requirements of the GSF's own governance procedures.

Contractual arrangements will explicitly state that providers understand GSF's governance procedures, and can deliver within those procedures.

Provider relationships will be reviewed annually or sooner if significant changes occur which affect the type of information held, the purposes for which it is used or the manner in which it is stored, processed or distributed. They will also be reviewed in the event of security breaches or reported "near misses".

4.34 Maintenance of procedures and technology components

GSF will ensure that procedures and technology components are maintained to ensure their correct and appropriate functioning, and that such maintenance is planned and performed on a regular, scheduled basis.

Following the annual review and report to the Board, GSF will implement any required changes unless changes are required sooner in the light of security breaches or reported "near misses".

4.35 Audit programme for the processing of personal information

GSF will conduct an annual review of its governance arrangements in respect of the processing of personal information to cover the aspects outlined in this strategy document; a summary proforma is appended to this document.

The review will be carried out by the Data Manager.

4.36 Objectivity and the impartiality of the audit program

In respect of the annual review of the processing of personal information, the Data Controller is responsible for ensuring its objectivity and the impartiality on behalf of the Board of Trustees. This will be achieved through scrutiny of the audit itself and the audit process.

4.37 External audits of the processing of personal information

At this stage and given the limited nature of the processing of personal information carried out by GSF, and the external input into this strategy, external audits are not deemed to be necessary on a regular basis at this stage.

In the future, should GSF consider applying for ISO9001 certification, then GSF will consider dual certification for BS10012 at that stage. This would require additional monitoring processes and would benefit from external audit prior to applying for BS10012 certification. Should certification be achieved, then external audits would be needed on a regular basis to maintain the certification status.

4.38 Management review

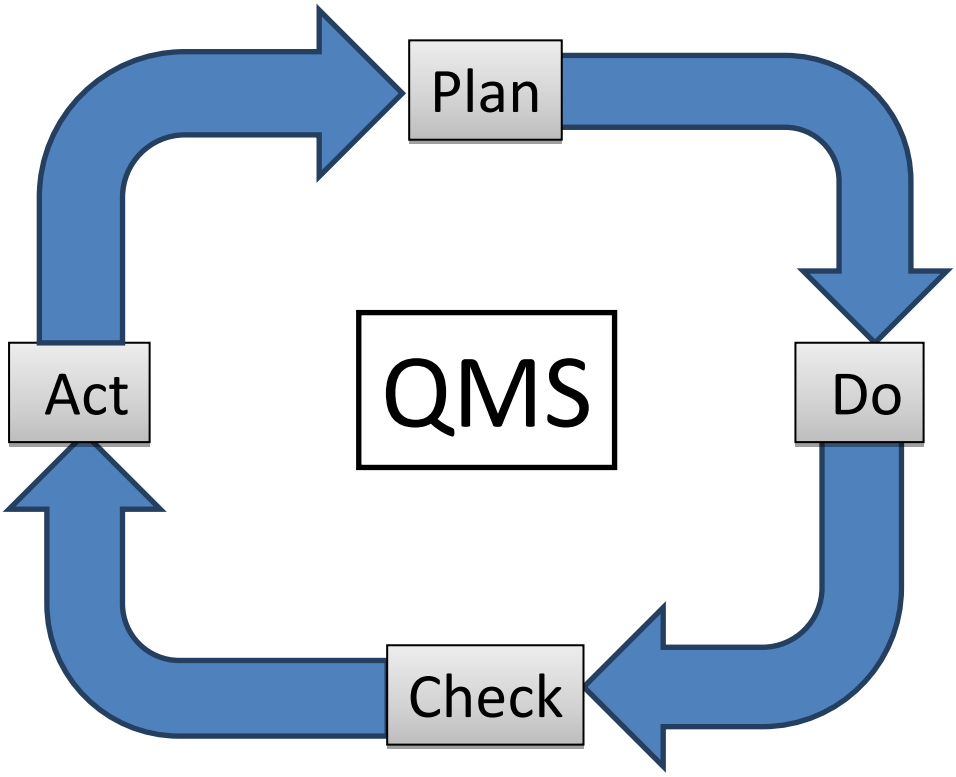
The Board is responsible for reviewing the governance arrangements for personal and other sensitive information. The Board and their designated representatives will use a Plan Do Check Act cycle to ensure proper review:

Plan: This strategy represents the Planning stage of the cycle

Do: Ensure that all aspects of the strategy are implemented

Check: Review the procedures focusing on where they are not working, breaches, near misses and changes to the environment which mean they are no longer fit for purpose

Act: Revise the procedures focusing on actions to learn from errors, near misses or breaches and changes required to adapt to changes to the environment which mean they are no longer fit for purpose. Revise the strategy and return to step 1.



Plan-DoCheckAct cycle

5 Freedom of Information

As a Community Interest Company no longer operating under the NHS and not providing primary medical services, dental services or ophthalmic services[2], GSF is not required to reveal information under the Freedom of Information Act, nor are GSF required to produce a publication scheme.

As a voluntary commitment to the goals of the Freedom of Information, GSF will publish the widest possible range of information on its website. However, GSF will never publish:

- Personally identifiable information
- Commercially sensitive information

which is outside the scope of the Freedom of Information Act and would place us in breach of the Data Protection Act.

[2] Source: Freedom of Information Act, Freedom of Information Act 2000, SCHEDULE 1, Section 3(1)(a)(i)

6 Appendices

6.1 Privacy notice

What GSF does with information given to us

This privacy notice sets out how GSF uses and protects any personal information that you give us.

GSF is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using this website, then you can be assured that it will only be used in accordance with this privacy statement.

GSF may change this policy from time to time by updating this notice. This policy is effective from August 1st 2011.

What we collect

We may collect the following information:

- Name and job title
- Contact information such as address postcode, telephone numbers and email address
- Other information relevant to customer surveys and/or offers

What we do with the information we gather

We require this information for

- The provision of information and services including training
- Internal record keeping
- If you highlight a deficiency in how we do things at the moment, we may use the information to improve things
- We may periodically send you emails about new information and services which we think you may find interesting using the email address which you have provided

We will never share your information with a third party without your additional explicit consent, unless ordered to do so by a legal authority.

Security

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

How we use cookies

A cookie is a small file which asks permission to be placed on your computer's hard drive. GSF makes only very limited use of cookies, and does not actively analyse data from cookies other than for the smooth running of the website.

Once you agree to a cookie being added, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about webpage traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

Links to other websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Controlling your personal information

You may choose to restrict the collection or use of your personal information in the following ways:

- Whenever you are asked to fill in a form on the website, look for the box that you can click to indicate that you do not want the information to be used by GSF for marketing purposes (we will never share or sell your data to a third party for this purpose): if you have previously agreed to us using your personal information for marketing purposes,

you may change your mind at any time by writing to or emailing us at info@gsfcentre.co.uk

You may request details of personal information which we hold about you under the Data Protection Act 1998. A small fee will be payable. If you would like a copy of the information held on you please write to the address below.

If you believe that any information we are holding on you is incorrect or incomplete, please write to or email us as soon as possible, at the address below. We will promptly correct any information found to be incorrect.

Thank you

The Gold Standards Framework Centre CIC
The Coach House,
Crescent Lane,
Shrewsbury, SY1 1TR
Tel 01743 291891
Email: info@gsfcentre.co.uk

6.2 Information Security Policy

Information Security

Information security is vital in order to ensure the confidentiality, availability and integrity of data, which are defined as:

- Data Confidentiality: confidential information needs to be accessible only to those authorised to have access to it. This normally means staff that need to process data in the scope of the care programme or processing derived from it
- Data Availability: information and assets must be available to those who are authorised to have access to it when required
- Data Integrity: information needs to have integrity: to be accurate and complete and resistant to unauthorised modification or destruction

Whose data is it?

All data processed on computers, electronic devices or storage media or held on paper are the property of GSF and not personal property unless this can be adequately demonstrated.

Breaches of Security

In the event of theft of any equipment or any unauthorised use of equipment and access to data, this should be treated as a significant event and reported and investigated as such. All breaches (actual or potential) should be reported to the Data Manager as soon as possible. (Throughout this policy, if the Data Manager is unavailable and the matter requires urgent attention, it should be referred to the Data Controller). Dependent upon the breach scenario, investigations may be carried out jointly with the Data Controller.

Authorisation

Access to information systems is restricted to authorised personnel and to other persons only under the supervision of an authorised person. It must only be granted on the basis of a sound and justifiable need. Access to the information held on such equipment must be authorised by the Data Manager.

Unless specifically authorised, staff are not permitted to do any:

- Processing of data such as deletion, modification or destruction
- Sharing or distributing, by any means, of any confidential data without authorisation. If doubt arises about what is confidential (including 'commercial in confidence') then the Data Manager must be consulted

Staff must be authorised to access and/or operate information systems. Access to information systems will only be granted on a basis of 'justifiable need'

For business continuity, access may be granted to any computer, device or file on site. This must be authorised. If there is any doubt as to whether a member of staff has the necessary authority to access information or a system then they must be sure to clarify this with their line management first.

Investigative access must be requested by the manager leading the investigation and conducted by appointed staff. An investigation order must be signed by the Data Manager prior to commencement.

Staff must have their own unique computer account and only login to systems or applications that they have been granted access to (unless there are exceptional circumstances which would be approved by a Board member).

If data or a system is accidentally accessed that should not be then staff are obliged to maintain its confidentiality, integrity and availability and also to report the fact immediately to the Data Manager. Where such access is suspected of being confidential or sensitive then an investigation may be required – the Data Manager will make this decision.

Access controls must take account of security requirements of the business application and permit access to be granted only on approval by the system administrator in consultation with the appropriate senior manager where there is any concern or doubt.

No individual should be given access to a live system unless the relevant forms have first been completed and they are aware of their security responsibilities as outlined in this policy and the Information Governance Strategy and its related policies.

Employees will normally be granted access only to such information that is required to perform their work duties. If they are erroneously granted any other access, then this fact must be reported to their line manager immediately as it may become construed as unauthorised access.

When information is copied between systems within the network, then employees should ensure that any confidential information remains secure and that the recipient system has the same or greater standard of security protection as the sender.

Access for Visitors/Contractors

This may include an engineer or contractor, auditor or researcher. Visitors must check in and out with an allocated supervisor. This supervisor must know the reason for the visit and any agreements that have been made.

Visitors must be supervised and only approved systems engineers may be allowed access to hardware or software.

On completion of work visitors must complete 'sign off' sheet or 'statement of work'

No data should be removed from the system without prior consent.

New Users

The Data Manager will complete all processes needed to initiate registration for new employees, and close down accounts when staff leave the company. Each user will be provided with a unique user account and ID. Any requests for changes to the account must be made in writing.

Revoking User Accounts

A user account can be revoked by the System Administrator when a user no longer requires access. A user account must be revoked when a user is not granted access to a system. During an investigation a user's account must be suspended or revoked to prevent access, with approval from the Data Manager. Access to a user account may be required to access mail if the member of staff is unexpectedly on long-term sick leave

Systematic Review of Accounts

At the time of the annual information governance review, the Data Manager will

- Generate a list of users by (profile, application etc)
- Confirm that all users identified are authorised to use the system or application
- Confirm that all user's access is appropriate

Any user not confirmed or with inappropriate access will have his/her access either removed or revoked, pending investigation.

Data Manager will maintain a file of account details with access levels, and a record of any action taken against unauthorised uses or users.

Physical Security

Staff must :

- Report problems with IT and information systems including unsafe or unsatisfactory equipment to the Data manager. In general, the more serious the fault or incident (or potential for one to occur) the sooner it must be reported
- Report any deficiencies in security, for example, equipment must be sited in order to avoid computer screens being able to be read by unauthorised staff or the public. If this is not the case it should be reported
- Ensure doors and windows are closed and locked correctly when vacating the premises

- Report improper use of equipment or damage to the Data Manager

Staff must not:

- Cause deliberate damage to a computer, information system, application, data or storage
- media (this includes unauthorised installation or distribution of software, computer viruses or malicious code.)
- Deliberately disrupt a computer or information system
- Deliberately exploit any vulnerability
- Deploy security without approval – Such measures must only be deployed on approval of the senior management in scope and by staff qualified to do so
- Move computers, printers or other desktop equipment without permission
- Allow computers, electronic media (e.g. floppy disks, CD disks, USB pen drives) to be exposed to extreme temperatures, fluids or corrosive substances
- Connect unapproved, un-configured computers to the network
- Eating, and especially drink, in the vicinity of computers and related equipment. Eating and drinking is forbidden in areas where there are important computers such as fileservers

Computer hardware and software protection

Environmental controls must be installed for key computer equipment where extreme temperatures may adversely affect their operation. Key equipment must be covered by maintenance agreements with trusted service providers who can demonstrably meet GSF information governance and health and safety requirements.

Precautions should be taken against theft, especially equipment that is portable and desirable like laptops and mobile phones:

- Personal computers should only be placed in locations with lockable doors and windows
- Curtains/blinds must be closed when possible and doors and windows locked when the office is vacated
- Wherever possible computer equipment must be kept 'out of view' and 'out of reach', particularly in public areas
- Master copies of software must be stored in lockable cabinets

Transporting Equipment

Equipment must not be 'on display' in a vehicle but put into the boot or equivalent and covered up, especially if the vehicle is left unattended. Equipment should not be taken home unless it has been authorised and has appropriate security

Data Backup

Files must be stored on a user's network drive. This will mean they are then saved onto a secure and resilient file server. This is not the same as saving data onto a computer hard drive. For instance a laptop would have to be plugged into the network to do this. Any computer that stands alone does not backup onto a file server.

The Data Manager will ensure that there is a regular and comprehensive backup schedule in place. Where this includes data held on servers on site, backup tapes and media must be stored safely and securely off site. Where data is held on behalf of GSF by third party hosting organisations, their backup and security arrangements must meet or exceed GSF standards

- Confidential or business critical information must not be stored on individual computer hard drives. The data manager has the right to check all local PC drives for data held in this way
- Data located upon critical network servers must be backed up in accordance with IT backup procedures to provide at least one month of information retention. Such information will be stored at another site to facilitate a maximum loss of one calendar week of information destroyed as a result of local building or system damage
- All back-up media must be maintained securely and only erased when no longer required in compliance with legislation and/ or policy

Clear Desk & Screen

Confidential (including 'commercially confidential') information (paper, computer media (floppy disks, CDs etc) must be stored in suitable locked cabinets and desks when not in use.

All GSF computers must require a username and password to be entered into the login screen before being used

Computers that may be left unattended, even for short periods, should be screen-locked or shut down. All GSF PCs will be set to automatically display a password protected screensaver after 10 minutes' inactivity.

Printers used for printing confidential or business critical data must be cleared of such data regularly and when left unattended. If confidential printed material appears in a printer and it is not local to the department it must be destroyed or the owner contacted.

Expectations of Staff

In essence, all staff are required to use company resources and information appropriately and professionally, and not take any action that could bring the company or themselves into

disrepute.

Compliance with the policies of GSF is a condition of employment and hence breach of a policy may result in disciplinary action being taken.

All staff and personnel employed or hired by GSF have a duty to ensure and maintain confidentiality and security of data.

Where there is evidence that any staff member has purposefully or negligently not adhered to this policy, disciplinary or legal action may be taken which may lead to termination of work contract.

E-mail

E-mail is a business tool that should be treated like any other tool in the workplace. E-mail is robust, cost-effective and fairly secure but should not be used as a replacement for face-to-face contact. Professional standards of behaviour apply to the use of etiquette and all staff are asked to work within the general guidance following this policy.

There are specific legal issues to remember with regard to email:

- Don't pretend you are someone else when sending mail this is misrepresentation
- Don't send frivolous, abusive or defamatory messages. Apart from being discourteous or offensive, they may break the law
- Remember that there are various Laws relating to written communication and they apply equally to e-mail messages, these include laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information, and wrongful discrimination. This list is not exhaustive
- Your use of the company's IT facilities and networks is restricted to bona fide purposes only, i.e. those which are consequent to the Company's provision of healthcare, related study, research, support services, administration or related activity occasioned by employment with the Company
- Remember that sending e-mail from your company account is similar to sending a letter on letter headed paper, so don't say anything that might discredit or bring embarrassment to the Company

Due to the insecure nature of Internet mail, users must consider Internet e-mail to be public information. Internet and email users must be aware that the system is inherently insecure. No service user identifiable information or other company confidential information or government classified information should be transmitted over the Internet without appropriate security measures, which may include encryption or other forms of password protection.

Monitoring

GSF reserves the right, consistent with UK law, to monitor any of its computers, computer networks, data processing/storage facilities and information systems. This includes e-mail. Members of staff should not consider information sent/received or stored on company systems as his/her private information.

Malware and Viruses

GSF will run and update anti-virus software automatically on your computer without your intervention. Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

Delete spam, chain, and other junk email without forwarding it in line with this policy. Never download files from unknown or suspicious sources.

New viruses are discovered almost every day. If in doubt contact the Data Manager and periodically check your email for virus warnings.

Acceptable Internet Usage

GSF recognises that many staff regularly access the internet in the course of their duties. As an unregulated facility, safeguards are in place that must be considered to protect the information security of the company.

It is acceptable to use the internet to access information and information systems relevant to your work, or work related research material

Limited personal use is permitted, provided this does not interfere with the performance of staff work. Some Internet access is acceptable before the individual's working hours, during lunch hour and after work hours as long as it complies with the rest of this policy.

Unacceptable Internet Usage

It is unacceptable to overuse the Internet for personal purposes. The individual's company e-mail address should never be used to register on any non-work related sites.

GSF staff are not permitted to create, download or transmit:

- Any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material, or any material considered to be unlawful any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material
- Any material that is designed to annoy, harass, bully, inconvenience or cause needless

anxiety to other people

- data or material that is created for the purpose of corrupting , destroying or accessing GSF data or hardware, such as viruses
- "junk-mail" or "spam". (eg unsolicited commercial webmail, chain letters or advertisements)
- information to conduct private business or participate in on line gambling or game playing
- streamed video or audio content for entertainment purposes;
- contributions in on line chat rooms, other than GSF chat rooms as a part of their role

GSF staff must not present views in media statements or social forums on the Internet on behalf of GSF, or relating to GSF unless specifically authorised by a senior manager, or make statements about people or organisations on any web pages you are including on the company website without verifying their basis in fact.

GSF staff must proactively seek to avoid any use of the Internet that might be considered harassment or bullying, for example by displaying particular web sites that others may consider offensive or threatening.

This list cannot be exhaustive and merely indicative of the type of content that deviates from the professional standards expected by all staff at GSF; where staff are believed to be using the Internet inappropriately, this would be fully investigated within the Grievance and Disciplinary Policy (and may result in dismissal).

Accidental Access of Inappropriate Material

If staff accidentally access inappropriate material of the type referred to above, or other material which they feel may be considered of an offensive nature, they should note the time and web site address and exit from the site and then inform the Data Manager.

Where a doubt arises about whether it is appropriate to access a site, then approval should be obtained from the Data Manager.

Social media

All staff should be aware that any postings to any of the social media sites that may relate to their personal lives may also impact on their professional lives. Any material posted on social media sites which brings the organisation into disrepute may be considered under the Grievance and Disciplinary Policy.

Moreover, no information relating to their role or any aspect of service that GSF provides may be posted onto such sites. Staff are asked to exercise caution in the sharing of any data or information that may be accessed by the general public, and therefore includes all service

users.

Removable Media

This includes the use of Removable Media such as: Floppy Disks, CD-R: CD-R, CD-RW, Memory Sticks, Flash Drives, Flash Disks, PDA Memory Cards etc.

Removable media can be classified as any portable device that can be used to store and/or move data. Media devices traditionally can come in various shapes and forms, including Universal Serial Bus (USB) memory sticks, floppy disks, read/write compact disks (CD), PDA storage cards, magnetic tapes and cassettes. Essentially anything you can copy, save and/or write data to which can then be taken away and restored on another computer.

Because they are portable, Removable Media create their own security vulnerabilities; they provide the means to conveniently transport up to several gigabytes of data from one computer or network to another.

GSF staff should carefully consider the use of removable media within the office and avoid it whenever possible.

GSF staff may NOT remove any removable media from the GSF Centre office without prior written or email permission from the Data Manager. Requests for permission should be made by email and include the reason why removal is necessary, the information to be removed and the purpose to which the information will be put externally.

Passwords

Staff should be aware of how to select strong passwords and avoid the use of weak passwords, considered to be

- Those with less than eight characters
- A word found in a dictionary (English or foreign)
- Birthdays of people known to anyone coming into contact with the GSF office
- Other personal information such as current or recent addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- USB sticks: files should be password protected or encrypted

Strong passwords have the following characteristics:

- They contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

- Are at least eight alphanumeric characters long
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on computer unless encrypted. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. Alternatively, use a variation on an old telephone number such as one not used by you in the last ten years and use letters to represent the dialling code eg Man7455128, is derived from an 0161 number.

GSF expects staff to take passwords seriously. Therefore, staff should not:

- × Use the same password for all accounts
- × Share passwords with anyone unless this has been authorised. All passwords are to be treated as confidential information
- × Reveal a password over the phone to anyone
- × Reveal a password in an email message, unless for a specific purpose where it is not used in any other context
- × Talk about a password in front of others
- × Hint at the format of a password (e.g., "my family name")
- × Reveal a password on questionnaires or security forms
- × Share a password with family members
- × Reveal a password to co-workers unless authorised to do so
- × Use the "Remember Password" feature of applications (e.g.Outlook, Internet Explorer etc) in the communal office
- × Write passwords down and store them anywhere in your office
- × Store passwords in a file on ANY computer system without encryption

You will be prompted to change passwords at regular intervals. However, GSF recognises that it is difficult to keep track of passwords, so will not ask you to change it too often.

If an account or password is suspected to have been compromised, report it to the Data Manager and change all passwords.

Password guessing may be performed on a periodic or random basis by the Data Manager or delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Disposal

Disposal poses a major threat to information security.

All waste paper should be shredded unless it can be shown to contain no sensitive or personal information: the presumption should be if in doubt, shred!

All electronic equipment capable of holding information including PCs, phones, removable media such as CDs, DVDs and USB sticks must be disposed of using procedures guaranteed to strip out all personal and/or sensitive data.

All furniture, (desks cabinets etc) must be searched before disposal to prevent accidental removal of paper or electronic media containing personal or sensitive data.

6.3 General Guidance on the use of Email

Messages should be concise and to the point. As people receive many e-mail messages it is important that a subject is added to the e-mail in order that the recipient can see clearly what the e-mail is about. Many Email systems will reject or divert messages without a subject. E-mails can be marked for importance and sensitivity, such as urgent or private and confidential.

It is not uncommon for GSF e-mail users to send and/or receive quite a few e-mail messages per day. To ensure that e-mail is used efficiently and effectively, an understanding of good practice, e-mail etiquette and policy that applies to its use are required.

Log in at least twice a day and respond to requests promptly. Check your e-mail regularly; to ignore a message may be discourteous and confuse the sender. Reply, even if a brief acknowledgement is all you can manage.

Advise people when you are not available. When out of the office and not able to log into your email account, use the tools within your system to notify others of your inability to read your mail.

Other issues to consider:

- Be selective about who receives your emails, especially when using “Reply to All”.
- Consider - do all recipients need to see the reply?
- Use distribution lists with care – is it important that all addressees receive this email?
- Use organisation-wide distribution lists only to communicate important business information that has genuine site-wide value
- Check that e-mails are addressed to the correct recipient when using a Global Address Book
- Check the e-mail before despatch. Once you have clicked the SEND button the email cannot usually be retrieved
- Use discretion when forwarding a long email message to group addresses or distribution lists
- Print only essential messages
- Keep messages concise and to the point. Try to keep your messages to one or two screens-full maximum. Most people prefer not to use a computer screen to read text on in preference to a printed document, and it can get very tiring for some users
- Mark e-mails for importance and sensitivity if you need to, such as urgent or private and confidential
- Be careful how you express yourself. E-mail lacks the cues that convey the way you want your message to be taken, and may convey a wrong impression

Do NOT:

- Get caught out by the speed of e-mail. Do not act impetuously. Is your first reaction the one you want the recipient to receive?
- Share your e-mail password or use other people's account to send your messages.
- Send a mass mailing circular via the email
- Send e-mail that may be misconstrued by the recipients. Be aware that the recipient of your e-mail message may be a person whose culture, language, and humour have very different points of reference from your own. Avoid sarcasm. Also bear in mind that date formats, measurements, and idioms may not travel well
- Verbally attack someone in electronic form
- Send e-mail in upper case, this is the equivalent of shouting in someone's ear.
- Send large attachments by e-mail. If you believe that most recipients will print the document, try to use another method of sending the hard copy
- Send computer program files as attachments unless essential – some Emails prohibit downloading them and it is poor etiquette to expose the recipient to a potential risk
- Send or forward chain e-mail – this will be considered a waste of company resources and may lead to disciplinary action
- Extract and use text from someone else's message without acknowledgement. If you wouldn't do this with conventional mail, don't let the ease of being able to do it with e-mail lead you into bad habits
- Make changes to someone else's message and pass it on without making it clear where you have made the changes. This could be misrepresentation
- Continue to include people in cc's if the messages have become a two-way conversation. Limit cc's to those with a need to know. Watch cc's when replying

E-mail Etiquette

Always sign off with your name, the name of the company and address, and telephone number. This is more important when sending outside the organisation. There are facilities within the software which allow you to automate this process saving time re-keying this each time you send mail.

Use the 'subject' field with a few short descriptive words to indicate the contents when sending e-mails. It will assist the recipient in prioritising opening of email and aids future retrieval of opened messages.

When using the 'reply' option, ensure that the subject field (usually filled in for you in this circumstance) still accurately reflects the content of your message. It is a good idea to check all your mail subjects before responding to a message as sometimes a person who asks you for help or clarification will send another message which effectively says "It's ok now".

Type your messages in lower case - using capital letters is considered aggressive. Be careful about content. E-mail is easily forwarded. Do not write something in an email that you would not write in a letter or say to someone face to face. Maintain the conventions normally used in sending a letter by post. If you usually address someone as “Dr. Smith”, do the same in e-mail. E-mails carry the same etiquette as traditional communication, they also carry the authority of the sender!

Always ensure that the correct address has been entered before sending your email message especially if it contains information of a confidential nature. Be careful as there may be addresses that go to a group although the address appears just like it is one person.

Where practical, restrict yourself to one subject per message. Sending multiple messages if you have multiple subjects helps recipients to use the 'subject' field to manage the messages they have received.

Don’t assume that because you have sent a message, it has been read. It is easy to overlook an e-mail message. Reply as promptly as you can as e-mail systems do not have a conventional 'pending' tray.

Be tolerant of others' mistakes. Some people are new to this medium, and may not be good typists, or they may accidentally delete your message and ask you to re-send it.

E-mail Housekeeping

Ensure that when the size of a mailbox reaches the maximum storage limit set on your server, items are moved to a personal folder. Keep the amount of e-mail in your Inbox to a minimum. Delete e-mails after reading, response, or action. Saving messages uses valuable disk space. Review saved e-mails every month and delete the ones no longer required. If there is an e-mail that may be required in the future, it should be archived.

Regard the security of e-mail messages as about equivalent to a message on a postcard and recognise that anyone along the chain of distribution could get to see what you have said. It might end up in someone else's hands by being forwarded or even by accident. If you have sensitive messages to send you may need to use some other more secure medium.

Develop an orderly filing system for those e-mail messages you wish to retain.

The e-mail may have an attachment containing a virus so if in doubt do not open it. Check that any message you respond to was directed to you. You might be copied (cc) rather than the primary recipient.

6.4 Electronic Communication System policies

This policy and the information governance strategy supersedes any previous Electronic Communication System policy

6.5 Annual audit checklist

At the annual review, the Data Manager will prepare an audit report for the scrutiny of the Data Controller and the Board of Trustees. It will cover any changes, or non-conformances identified and consequential actions taken in respect of:

- Updates to the risk assessment in the last 12 months
- Updates to data protection and other relevant legislation
- Required updates to the notification to the Information Commissioner's Office
- Staff training in respect of information governance
- Breaches of confidentiality
- Requirements for privacy notices
- Contractual arrangements with third parties in respect of information governance
- The purposes for which personal information is used
- The adequacy of personal information stored
- Deletion of personal information in accordance with retention schedules
- Requests or complaints from individuals about personal information held about them
- Security controls, their operation and adoption by staff including disposal, use of passwords, emails and other security measures
- The security of data transmissions
- Restriction of access to those needing it
- Transfer of personally identifiable data outside the EEA
- Verifying the identity of subjects seeking information
- Selection of providers of information processing services that meet GSF standards
- Maintenance of procedures and technology components

6.6 Managing data for ADA

In establishing this strategy, GSF identified ADA data as “high risk” in terms of the Data Protection Act and a review was carried out.

It was suggested that the demographic data should no longer be collected routinely, as it had no specific purpose and was readily identifiable.

It was identified that the diagnosis and place of death could in combination lead to identification. As this data was needed for analysis, it was resolved that these data would not be presented externally in combination.

Internally, the following protection measures are taken:

The following processes have been put in place to protect any data entered:

- Individual log in details for each facility with a request to change their password as soon as they log in and not to share that information with anyone else
- If they enter the incorrect password four times they get locked out the account and have to contact GSF to unlock the account
- Only one person at GSF has day-to-day access to ADA and the data entered. When the main person is unavailable, a backup administrator takes over. Only the staff who entered the data will know the identity of the patients for whom they entered data. Each ADA record is given a unique numeric value which they must record locally against a local patient identifier or NHS number. There is no way from within the system to identify record X as belonging to a specific patient
- All data is partitioned such the user X can only ever access the data they entered
- There is no search facility to 'browse for records'
- We have a SSL certificate so all data in encrypted
- Log in details are encrypted
- When running the data and sending to evaluation teams GSF take out any information that would connect patients to certain facilities. Facility names will not be sent out on the same spread sheet as the patient information unless specific to that particular evaluation
- If there is a need to store ADA data from previous systems etc. all spread sheets are password protected with only one person knowing the password
- MARACIS is already compliant with the NHS IG toolkit. This is a prerequisite for the N3 connection held by GSF

- Only the account (system administrator) has permission to cross the data boundaries which segregate the data of facility A from facility B. When a user from facility A logs in they can only ever access / report on facility A's data
- As far as MARACIS development staff are concerned all work is done against their development environment which holds dummy data. When a modification is ready to be released into the test or live environments it is done so automatically (no human intervention) and the designated GSF staff member then checks that it works correctly before releasing it to the wider user population

6.7 Implications for other management areas

This strategy impacts on other key GSF strategies. When changes are made to this or any other strategy, GSF will consider their implications for all other strategies

6.8 List of countries approved for personal information transfers using standard GSF protocols

GSF may transfer personal information transfers using standard GSF protocols without further explicit consent to the following countries

EEA Countries	Other approved countries
• Austria • Belgium • Bulgaria • Cyprus • Czech Republic • Denmark • Estonia • Finland • France • Germany • Greece • Hungary • Iceland • Ireland • Italy • Latvia • Liechtenstein • Lithuania • Luxembourg • Malta • Netherlands • Norway • Poland • Portugal • Romania • Slovakia • Slovenia • Spain • Sweden	• Andorra • Argentina • Canada • Faroe Islands • Guernsey • Isle of Man • Israel • Jersey • Switzerland

6.9 Sources and other useful documents

1. The Web site of Information Commissioner's Office (www.ico.gov.uk)

2. Information Commissioner's Office (2011) Advice on changes to the rules on using cookies and similar technologies for storing information, available on line at http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf
3. Gillies, Alan (2011)Data Protection for Small Business (Kommon Sense Guides for Kindle) [Kindle Edition], downloadable from http://www.amazon.co.uk/Protection-Business-Kommon-Guides-ebook/dp/B004QOA1AA