British Thoracic Society
Information Governance Policy
1 May 2019

V 3.0

Section 1 BTS Information Governance Policy

1.1 Purpose and range of this Policy

The British Thoracic Society (BTS) Information Governance Policy sets out how BTS handles information, including personal data. It brings together the legal requirements, standards and best practice that apply to the handling of information. It allows organisations and individuals to be assured that information is obtained, held, recorded, and shared in a manner that is legal, secure, efficient and effective.

BTS regularly handles data obtained from individuals and from other organisations such as the NHS, including extracts from patient medical records.

Any group or individual who has access to information relating to their involvement with the Society must abide by this Policy. This includes BTS Head Office staff and associates, including companies that supply IT services to BTS, members of BTS committees, Specialist Advisory Groups, Guideline Groups and other groups (including the Clinical Audit Programme, Registry Programme and MDRTB Clinical Advice Service) set up by BTS must abide by this policy in so far as the information in their hands has come through their involvement with BTS. For the purposes of this document the term BTS Staff encompasses BTS Head Office Staff and Associates.

1.2 Definitions

For further information on definitions please see the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Information Governance

Information Governance (IG) ensures necessary safeguards for, and appropriate use of, personal data, including patient identifiable data. It is "a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service" (https://www.england.nhs.uk/wp-content/uploads/2016/12/information-governance-policy-v3-1.pdf).

Patient identifiable data

Patient identifiable information includes: patient's name, address, full post code, date of birth, NHS number, local patient identifiable codes, anything else that may be used to identify a patient directly or indirectly.

Personal data

This includes information about BTS members and other individuals including home address, date of birth and financial information. It is defined as information relating to persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Special categories of personal data

Certain categories of personal data are subject to additional controls. The categories of data that BTS collects that would fall within this are racial or ethnic origin and data concerning health.

Confidential information / data

For the purposes of this policy confidential information/data is regarded to be data that are provided in confidence and are not publicly available.

Data controller: person or entity who determines the purposes for which and manner in which data are processed
Data processor: person or entity who processes the data on behalf of the data controller

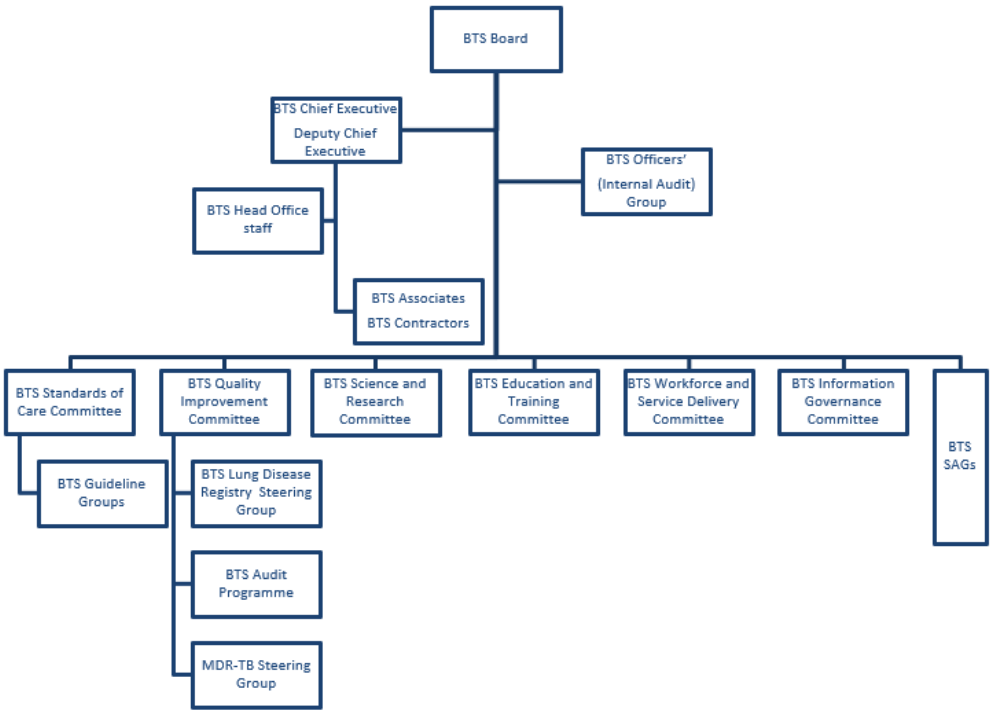
1.3 Information Governance Management Framework

The overall IG Management framework is described below:

Area	Responsibility
Senior Roles	IG Lead: Chief Executive Senior Information Risk Owner: Chief Executive Caldicott Guardian: Chief Executive Data Controller: Chief Executive Data Protection Office: Deputy Chief Executive
Key Policies	BTS IG Policy – which includes: - BTS Confidentiality Policy - BTS Data Protection Policy - BTS Data Security Policy - BTS Information Management and Record Keeping Policy - BTS System Level Security Policy - BTS Incident Reporting Policy - BTS Information Asset Register and Risk Assessment
Key Governance Bodies	BTS Board BTS Officers' (Internal Audit) Group BTS Information Governance Committee
Resources	Key Staff: Chief Executive (see above) Deputy Chief Executive (DPO/Data processor) IT manager (information security) Director of Operations Information Asset Register
Governance framework See flow diagram below	BTS Board (Trustees) BTS Officers' Group BTS Standing Committees including the Information Governance Committee BTS Lung Disease Registry Steering Group BTS MDR-TB Clinical Advice Steering Group BTS Chief Executive/Deputy Chief Executive BTS Head Office Staff and Associates BTS Contractors
Training and Guidance	Annual Data IG Policy training/refresher BTS Staff and Associates Annual performance review for all BTS Staff Induction training for new BTS Staff IG Policy awareness session for BTS Contractors IG Policy awareness as part of the Committee induction process for BTS committee members BTS Board members undertake mandatory IG training via their NHS institution
Incident management	Incident management procedure following policy at Section 7
Approval process	The IG Policy is reviewed at least annually by the BTS Information Governance Committee on behalf of the BTS Board. The Policy is

	presented to the BTS Board of Trustees for approval annually (usually at the June meeting).

BTS Organisational Structure:



1.4 Legal Responsibilities

The relevant legislation includes:

- Common Law – Duty of Confidence
- Data Protection Act 2018, and the General Data Protection Regulation (EU) 2016/679
- Freedom of Information Act 2000 (FIA)

1.5 Duty of Confidence

All NHS bodies and those carrying out functions on behalf of the NHS have a common law duty of confidentiality to patients and a duty to maintain professional ethical standards of confidentiality. Satisfying the Common Law Duty of Confidentially may require a greater level of confidentiality than complying with the Data Protection Act 2018/General Data Protection Regulation.

1.6 Confidentiality

BTS has a Confidentiality Policy which outlines the framework in which BTS staff should work and their responsibilities to ensure standards of confidentiality are maintained (Section 2).

Confidentiality covers all types of information. In addition to legal requirements determined by common law, the Data Protection Act 2018 /General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the Freedom of Information Act 2000, the NHS is required to comply with the NHS Code of Practice for Confidentiality (www.gov.uk/government/publications/confidentiality-nhs-code-of-practice). This outlines seven Caldicott principles relating to collecting, transferring or generally

working with patient identifiable data. The NHS has been advised to ensure that any data stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop, PDA or mobile phone should be encrypted. This is also now a requirement across all public sector organisations set by the Cabinet Secretary. NHS organisations are well within their rights to seek reassurance that BTS operates in line with these requirements.

BTS adheres to the Code of Practice and the Chief Executive is the Caldicott Guardian for the Society.

1.7 Caldicott Principles

A second information governance review by Dame Fiona Caldicott in 2013 updated the original six Caldicott Principles and introduced a seventh:

1) Justify the purpose(s)
2) Don't use personal confidential data unless it is absolutely necessary
3) Use the minimum necessary personal confidential data
4) Access to personal confidential data should be on a strict need-to-know basis
5) Everyone with access to personal confidential data should be aware of their responsibilities
6) Comply with the law
7) The duty to share information can be as important as the duty to protect patient confidentiality

NHS Organisations may require information about the following:

- What data items have been requested
- Name of organisation and person responsible for data
- How the data will be transferred e.g. paper, computer record
- Who will have access to the data
- How service users will be contacted and how consent will be obtained
- Where the data will be stored and how it will be protected
- If data is on a computer if there is access via a network
- How long the data will be stored
- At the end of the period how the data will be disposed & who will be responsible for this

1.8 Data Protection and GDPR

Up until 25 May 2018, all aspects of gathering, using and disposing of personal data (whether in electronic format or on paper) were governed by the Data Protection Act 1998.

Data protection law changed on 25 May 2018. The 2018 Data Protection Act came into force and encompasses the provisions of the General Data Protection Regulation (GDPR), the new, Europe-wide law. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations will need to handle personal data from 25 May 2018.

BTS has a Data Protection Policy outlining how staff must comply with this legislation in all its activities (see Section 3).

GDPR requires that public authorities (and other organisations that carry out certain types of processing) appoint a Data Protection Officer (DPO). Following review in April 2019, BTS confirmed the appointment of a Data Protection Officer (Sally Welham – Deputy Chief Executive). Appointment of the DPO has been registered with the ICO, and responsibilities are outlined here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

1.9 Freedom of Information

As the British Thoracic Society is not a public body, it is not required to comply with the Freedom of Information Act 2000 (FOI). However where the Society acts as a data processor, data may be subject to Freedom of Information. Any requests for information under FOI, should be forwarded to the BTS Chief Executive. Requests should be responded to in a timely manner as responses are required within 20 working days.

1.10 Data Security, Information Management and System Security

Details of the arrangements for data security access, handling, storage and retention/destruction are set out in the BTS Data Security Policy (Section 4), the BTS Information Management and Record Keeping Policy (Section 5) and the BTS System Level Security Policy (Section 6).

These policies have been reviewed in accordance with 'National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs' (recommendations to strengthen security of health and care information and ensure people can make informed choices about how their data is used) produced by the National Data Guardian, published in July 2016.

1.11 Staff Responsibilities and Staff Training

BTS Staff are required to follow the policies set out in this document. Staff contracts contain a confidentiality clause and staff are provided with regular (at least annual) training on data protection and confidentiality policies and procedures to ensure that their working practices comply with stated BTS policy.

1.12 Incident Reporting

BTS Staff should report any incident involving a breach of the policies set out in this document regarding handling of personal data to the Chief Executive without delay. The details of the Incident Reporting process are provided in Section 7.

1.13 Risk Assessment

The Society carries out a Risk Assessment exercise each year and a report is provided to the BTS Trustees for approval. A review of the Information Governance Policy and the Society's adherence to the processes contained within the policy document is an intrinsic part of the annual Risk Assessment exercise. Section 8 provides details of the Information Asset Register and Risk Assessment process.

1.14 Monitoring Compliance

Monitoring compliance with the IG policy and GDPR is the responsibility of the DPO and those working in the organisation, with overall responsibility resting with the Chief Executive and those nominated to act on her behalf in relation to specific projects. Review, monitoring and internal audit takes place through both the BTS Officers' Group and the BTS Information Governance Committee.

1.15 IG Improvement Plan

The Society has set in place a process to ensure that it adheres to all legal responsibilities and that sufficient measures are in place to comply with the NHS Data Security and Protection Toolkit. The Society's Improvement Plan over the coming 5 years comprises:

- Annual IG training for all staff appropriate to their role within the organisation
- Completion of the annual NHS IG assessment process, noting that from 2018/19, the NHS Data Protection and Security Toolkit assessment replaced the previous NHS Toolkit.
- Annual review of the IG policy together with an annual report on information and security risks with details of any incidents or breaches.

- Annual internal audit of IG policies and procedures by the BTS Information Governance Committee.

1.16 Approval and Review

This Policy was been recommended for BTS Board approval by the Information Governance Committee in May 2019, *[Board approval was confirmed in June 2019 and it will be reviewed again in 2020.]*

May 2019

Section 2 BTS Confidentiality Policy

2.1 Scope of Policy

This policy document should be read in conjunction with the BTS Information Governance Policy (Section 1) and the BTS Data Protection Policy (Section 3).

It applies to all staff and associates of the British Thoracic Society. All BTS staff and others who work for BTS must respect the need for confidentiality of information about the Society and its work, particularly where this involves personal data or patient data. This is expected to continue when the individual or staff member no longer works for BTS.

2.2 Information about individuals

BTS is committed to the confidentiality of personal data and patient data. The confidentiality is between the individual and BTS, not the individual and members of BTS staff.

Details of how BTS collects and uses personal data (e.g. BTS member data) are set out in the BTS Privacy Policy (See Appendix 1). BTS will not sell or rent personal data to third parties for marketing purposes. BTS may share information with appropriate third parties in order to improve clinical practice, provide general data about medical training and workforce trends, and our services. For example, BTS, the Royal College of Physicians Workforce Planning Unit and the Joint Royal Colleges Postgraduate Training Board (JRCPTB) share workforce planning data to ensure that records held are accurate and complete. See RCP statement: https://www.rcplondon.ac.uk/terms-and-conditions-and-privacy

Details of how BTS uses patient data are set out in the BTS Clinical Data Policy (https://audits.brit-thoracic.org.uk/WebPages/Help/frmHelpImportant.aspx). Patient data is only collected where this is allowed by law. Data are collected on an anonymous basis unless the collection of patient identifiable data has been specifically approved, for example by the Health Research Authority Confidentiality Advisory Group. Some audit and other projects also require approval from the Research Ethics Committee. BTS will only share data in accordance with these approvals, for example through the BTS MDRTB Clinical Advice Service for the purpose of providing medical advice. Information and reports produced by BTS or individuals working on behalf of BTS, will not contain information that allows the identification of individual patients.

2.3 Limits to confidentiality

In certain circumstances BTS reserves the right to break confidentiality if this is necessary. For example, because BTS is under a duty to share information or because a disclosure is required by law (such as where BTS is made aware that a serious crime has been committed, or where a life is in danger).

The decision on whether to break confidentiality will be decided on a case by case basis and always in conjunction with a senior manager, usually the Chief Executive or Deputy Chief Executive.

2.4 Access to data

BTS staff and others will not usually have access to organisational information or personal data unless it is directly relevant to their work.

Under the Data Protection Act and General Data Protection Regulation, individuals have the right to request access to all information stored about them. Requests should be made in writing to the Chief Executive.

Significant breaches of this Confidentiality Policy by BTS staff will be handled under BTS disciplinary procedures.

Breaches of confidentiality by BTS members in relation to BTS activities will be investigated by the BTS Officers' Group on behalf of the BTS Board (under the arrangements set out in the BTS Complaint Procedures).

2.5 Evaluation and Monitoring

BTS staff will be given a copy of the current Confidentiality Statement (see Appendix 2) when they join BTS and will sign the confidentiality statement to confirm that they will abide by this policy. BTS will ensure that all BTS staff are trained in the application of this policy and all sections of the IG Policy.

May 2019

Section 3 BTS Data Protection Policy

The 2018 Data Protection Act came into force on 25 May 2018, and encompasses the provisions of the General Data Protection Regulation (GDPR), the new, European-wide law and replaces the Data Protection Act 1998 in the UK. It places greater obligations on how organisations handle personal data. The GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

3.1 Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that

(1) personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

3.2 Legal basis for processing

The lawful bases for processing are set out in Article 6(1) of the GDPR. At least one of these must apply whenever personal data is processed:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

3.3 Individual rights

The GDPR provides the following rights for individuals:

i. The right to be informed
ii. The right of access
iii. The right to rectification
iv. The right to erasure
v. The right to restrict processing
vi. The right to data portability
vii. The right to object
viii. Rights in relation to automated decision making and profiling.

3.4 Arrangements for GDPR

BTS took a number of steps to prepare for the introduction of GDPR in May 2018 and these are summarised as follows under the checklist items provided by the ICO: https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

Awareness
All staff and key individuals within the Society (including Trustees) have been made aware of the impact of the new GDPR requirements and a number of key staff have undergone detailed training. Communications have also been issued to the Society's members, users of BTS systems (for example Clinical Audit, Registry and MDRTB CAS systems).

Documenting the information held by the Society
Information on personal contacts is recorded on BTS systems (including the membership databases/CRM, BTS Clinical Audit, Registry systems and the MDRTB CAS system). See Section 8 for the Record of Processing Activity.

Communicating privacy information
An updated BTS Privacy Policy has been developed drawing on advice from BTS lawyers and put in place across the Society and is available on all BTS websites (BTS, Respiratory Futures, audit, registry, MDRTB CAS). BTS has also updated its Cookie Policy which is available on all BTS websites (see Appendix 1). All users of the BTS websites were notified of the new Policies prior to May 2018.

Individual rights
As noted above, GDPR provides a list of explicit rights for individuals. BTS staff have received training as appropriate in the new GDPR requirements and BTS processes have been reviewed to ensure that we can adhere to requests to delete or amend data or to provide access to an individual's data if requested.

Subject access requests
Arrangements have been put in place to ensure that the Society is able to respond to access requests from individuals. In certain areas this involves individuals being able to easily access the information held about them via secure online access.

Lawful basis for processing data (see above)
The Society has identified the lawful basis for processing the data it holds on individuals and this is reflected in the BTS Privacy Policy (Appendix 1).

Consent
The Society has reviewed how it obtains, records and manages consent in relation to the data it holds and has updated its processes accordingly. It has renewed consent from all main groups of contacts and has taken account particularly of the Privacy and Electronic Communications Regulations (PECR) (https://ico.org.uk/for-organisations/guide-to-pecr/).

In summary, PECR restrict unsolicited marketing by phone, fax, email, text, or other electronic message. There are different rules for different types of communication. Specific consent is required to send unsolicited direct marketing.

In view of this, BTS has taken steps to obtain valid consent from its members and other contacts (eg Clinical Audit, Registry, MDRTB CAS) through the explicit tick opt-in boxes on each website so that confirmation has been obtained to contact individuals in future via email. Where this consent has not been obtained, BTS will not contact those individuals by email (for marketing purposes).

The collection of personal data via the BTS registry and MDRTB CAS involves consent by individuals for BTS to hold personal data with the approval of the relevant ethics committee. Fair processing notices outlining use of personal data for the BTS audit, registry and MDRTB CAS sites have been produced.

Children
GDPR has specific requirements for organisations that offer services to and process data from children. BTS does not offer services to children or collect personal data directly from children.
Data collected via the Clinical Audit and MDRTB CAS systems in relation to children falls under the BTS clinical data policy and the appropriate ethical approvals apply.

Data breaches
BTS has arrangements in place for incident reporting which covers the procedures for reporting and investigating a personal data breach (see Section 7).

Data Protection by Design and Data Protection Impact Assessments
GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes 'Data Protection Impact Assessments' referred to as PIAs or DPIAs – mandatory in certain circumstances (where data processing is likely to result in high risk to individuals).

The BTS IG Policy Section 8 relating to risk assessment includes guidance on producing a Privacy Impact Assessment for all new or potentially new information assets.

Data Protection Officers
BTS has reviewed its activities and has appointed a Data Protection Officer (DPO). This position is held by the Deputy Chief Executive who holds responsibility for monitoring compliance for data protection/IG activities working closely with the Chief Executive and others in the BTS staff team. The organisation's structure and governance arrangements are set out in the IG management framework in Section 1).

International
The Society does not operate (i.e. have offices) outside the UK. The BTS Privacy Policy (Appendix 1) outlines how BTS uses and stores personal data noting that on occasion personal data may be processed outside the EEA (for example for credit card payments).

Date of production: May 2019
Date of review: May 2020

Section 4 BTS Data Security Policy

4.1 Scope

This policy provides the basis for all decisions regarding the security, handling of, and access to, personal data held by BTS. It applies to all existing data stored in both physical and electronic form, and to the data for future projects or new aspects of existing projects.

This document is designed to allow a structured approach to decision-making regarding data-related issues and to ensure that we consistently employ “good practice". This practice must comply with the General Data Protection Regulation (GDPR). This policy is applied in conjunction with the BTS Information Governance Policy (section 1). This document contains references to certain legal obligations which arise as a result of the Data Protection Act 2018 and GDPR. Further information on the steps the Society has taken to comply with the GDPR are set out at in Section 3.

BTS obtained accreditation by Cyber Essentials in October 2018. This is a UK government information assurance scheme operated by the National Cyber Security Centre (NCSC) that encourages organisations to adopt good practice in information security.

4.2 Definitions

The following terms are used in this document to describe different types of data.
Please see definitions at section 1.2 and the ICO website: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/.

Personal data includes information relating to persons who:
can be identified or who are identifiable, directly from the information in question; or
who can be indirectly identified from that information in combination with other information.
Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Special categories of personal data: the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Transfer of data to a Third Party: in the context of this document, a transfer of data to a “third party" means supplying a data resource to an individual or organisation outside the Society that is not a contractor or supplier.

Pseudonymised data are personal data that have been processed in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information which is kept separately and securely to ensure that the data are not attributed to an identified or identifiable natural person.

Anonymised data contain no information that can be used to identify a data subject, and unlike pseudonymised data, the data cannot be re-linked with data that would allow identification of data subjects.

Encryption is the process of “scrambling" files on a computer system such that they are completely unreadable. Only the individual or individuals with the appropriate electronic “keys", passwords or

passphrases are able to unscramble (or decrypt) their contents. Encrypting files thus improves security but must be handled carefully. Data encrypted using good encryption techniques is incredibly secure and cannot generally be broken without the appropriate keys or passphrases. Care must be taken not to inadvertently encrypt data that cannot subsequently be decrypted. It is important to understand that encryption is not merely “password protection" and all data processors using encryption need to appreciate the distinction between unencrypted data which requires a password for access and encrypted data which remains secure even if made available.

4.3 Objectives

This policy is designed to ensure that the Society complies with, or exceed, the legal requirements of the GDPR. While the Society does not hold ISO/IEC registration, the policy reflects the best practice set out in ISO/IEC 27001: 2013 (Security techniques – information security management systems).

The policy applies to all work currently undertaken by the Society and to work that may take place in future. The underlying principles are that we must:

- safeguard confidentiality at all times;
- ensure that all data, anonymised or otherwise, is treated with respect and used only for the purposes for which it was collected;
- employ consistent good practice in all aspects of data handling and use and data processor.

The purpose of this document is to ensure that the work of the Society is undertaken effectively and within the requirements of the law and other appropriate guidelines for good practice. Ultimately, the burden of responsibility lies with the data controller.

4.4 Data access

In relation to data access (also refers to obtaining and storing data), the policy provides a framework for determining how rights for access to data in electronic form are assigned and how they are maintained. When changes to access rights are required, or if new data resources become available or are to be created, the policy indicates the procedure that should be followed to ensure that access rights are created and updated appropriately.

The policy will guide data access decision-making and control access to data resources and it ensures that work is carried out within the law, to ensure that access to confidential personal data resources is carefully controlled and restricted to those individuals who need access to such resources for the purpose of their job.

Obtaining information

The amount of personal/patient identifiable/sensitive (special category)/confidential data obtained should be kept to the minimum required. The data should be collected through secure methods such as a secure website (https://). Secure websites encrypt data when it is transferred from the individual/organisation entering the data.

Holding/storing information

All personal identifiable data should be held securely and confidentially. The increasing use of mobile devices such as laptops and memory sticks poses a threat to most organisations, including BTS.

In all instances access to sensitive (special category) data is restricted to the appropriate individuals within BTS Head Office, and the appropriate statisticians, and clinical lead(s).

Physical data

Any documents containing sensitive (special category)/confidential information should be locked in secure storage when not in use. Keys and combination codes required to access personal data stored in physical form (i.e. questionnaires, data stored on physical media such as CD-ROM) should only be made available to appropriate individuals; the data controller or someone working on their behalf, is responsible for deciding which individuals have access to which physical data resources.

In particular, keys or combination codes needed to physically access such personal data should not be made available routinely to all staff.
Access to the keys to secure storage is restricted to individuals specified by the Chief Executive.

Electronic data
Personal identifiable data is stored on a restricted area of the BTS servers.
Sensitive (special category) data will not be stored in any of the following locations:

- In unrestricted areas of the BTS servers
- On the local drives (C://) of BTS computers
- On personal network drives
- On laptops
- On memory sticks

Access rights for each data processor will be assigned based on the specific requirements of their job, allowing no more access than is necessary.
Decisions regarding allocation of access rights will be made and implemented by the data controller or someone authorised to act on their behalf. If appropriate, access to particular resources may be made on a temporary or fixed-term basis.

Access rights should be reviewed regularly by the data controller; if certain resources are no longer required by a user, the rights to access those resources should be revoked.

BTS Servers
Access to the BTS servers is restricted. Measures are taken to prevent unauthorised individuals accessing data stored on BTS servers in line with recognised data security standards.

Information held on the servers can be accessed by the Information Technology (IT) staff working for BTS, or by those employed by the company providing secure server space under written agreement with BTS. Third party System Maintenance and Contractors will only have access to data for the purposes directly associated with the provision and maintenance of the particular service for which they are authorised.

The main BTS server is located in the Head Office building (this hosts office systems, local area network and terminal server for remote access by BTS staff).

The Customer Relationship Management (CRM) database server (which hosts personal information pertaining to BTS members and other individuals, but no patient identifiable data) is hosted by Microsoft under a licensing agreement for Dynamics 365 on servers that are based in Germany.

BTS Head Office is protected by an intruder alarm which is activated when the building is unoccupied. Entry to the Head Office building is monitored by CCTV and access granted to authorised individuals only.

The following systems are hosted on secure servers administered by Westcliff Solutions from 1 February 2012 (and are based outside BTS Head Office):

BTS website, discussion forums
Abstracts system
Elections system
MDRTB advice forum
BTS Clinical Audit system
BTS Registry system
The Audit and Registry systems hold personal identifiable data in encrypted form.
BTS system backups
BTS Secure FTP servers
Declarations of Interest system
BTS MDRTB system

4.5 Hardware, back-up of information, Encryption and Passwords

A back-up of the main BTS server and servers administered by Westcliff Solutions is performed on a regular basis to ensure that should the server fail a recent copy of the content can be recovered.
Offsite automated back-ups of the system are completed on a daily basis via secure FTP and are stored on secure servers provided by Westcliff Solutions. The External servers hosted by Westcliff Solutions are stored in a fireproof location in a building separate from BTS Head Office (see Appendix 4 for details of Westcliff Solutions terms and conditions).

The CRM server hosted by Microsoft Dynamics 365 is backed up under the terms of the licence that BTS holds.

Anti-virus
Industry standard commercial anti-virus and anti-spam software is used to protect the BTS servers and incorporate automatic updates. If a threat is identified BTS IT is notified of virus alerts and outbreak prevention routines are implemented. The anti-virus is multi-level and is installed on desktops, servers (both file- and email-) and email gateways.

Computers and Laptops
Individuals should lock their computers when they leave their desk. All computers used to store or access data are supported by a time-out facility which will lock computers that shall at a minimum lock a terminal after 5 minutes of non-use.
Sensitive (special category)/confidential data are not stored on laptops or desktops. Such data are always saved on restricted areas of the server.

Memory Sticks
Memory sticks are not to be used to hold sensitive (special category) data.

Encryption
BTS uses encryption to secure data fields which contain personal identifiable data (eg name, date of birth) pertaining to the audit and registry systems and the key is available only to individuals authorised by the data controller. BTS uses the Advanced Encryption Standard (AES) method for encryption of its data.

Passwords
BTS requires that complex strong passwords should be used for access to BTS computer systems. These contain:

A “string” – i.e. be of at least 8 characters long, NOT based on readily available information, and using a mixture of numbers , lower and upper case letters and one symbol. Users should avoid

choosing obvious passwords (eg based on names/dates etc or common words). Guidance on selecting secure passwords is available here: https://www.cyberaware.gov.uk/passwords)

Passwords should:

- Not be the same or similar as the User name/ID.
- File passwords should only be disclosed to authorised individuals.
- Not be displayed on screens or reports.
- Be changed regularly

4.6 Data handling

General
All persons who handle personal data, whether in physical or electronic form, have a "duty of confidentiality" towards that data and must ensure that data security arrangements are adhered to in order to prevent breaches of confidentiality.

Personal data in physical form
Personal data stored in physical form, such as questionnaires, printouts and other records, should be stored in a physically secure area while not being used. If such data is to be kept in offices, it should be stored in a locked cabinet or similar. Access to keys for access to store rooms and cabinets should be carefully controlled. It is the responsibility of the data controller to manage access to such keys. Files should be put away in secure storage at the end of the working day, and should not be left on desks overnight.

Personal data in electronic form
Data which is kept in electronic form allows more convenience and flexibility in terms of data handling, but also requires more care to be taken.

Personal data should always be kept on network servers and never on the local hard drives of desktop PCs. Data should not be stored on electronic media such as CD-ROM/DVD or memory sticks.

When working with personal identifiable data in electronic form this should take place in a controlled environment (i.e. in Head Office or other suitable non-public place), following these guidelines:

- Data should be kept on password-protected network systems;
- Sensitive (special category) personal data should be left encrypted between processing sessions;
- Temporary files generated during processing should be deleted as soon as possible after use.

Recording information
Where appropriate, data are subject to validation checks to maximise the integrity of data. All data supplied for clinical audit and registry purposes will be subject to validation checks against criteria specified by the relevant project in order to maintain integrity of the data. Validation checks are instituted on the audit and registry systems which collect and hold the data concerned (for example restrictions on the type of data entered and restricted range criteria are used where appropriate).

Sharing and transferring information
Data should only be shared and transferred if appropriate and lawful to do so. Data are owned by the Society and managed by the BTS Audit and Registry Programme team on behalf of BTS and

authorisation for sharing data should be provided by the Information Governance Committee in line with the BTS Clinical Data Policy.

Before transferring personal data to a Third Party, authorisation must be obtained from the data controller or their nominated deputy.

The data controller must confirm that the organisation with which the information is to be shared has the appropriate Information Governance principles in place (this could include demonstration of compliance with the NHS Data Protection and Security Toolkit for relevant organisations or other forms of assurance for non-NHS bodies).

No more data containing sensitive (special category) personal information should be transferred or received than is necessary for the purpose. Data files can be transferred using the following methods:

- Saving in a restricted access area of the project folder
- Emailing files in an encrypted format
- Uploading via secure ftp (file transfer protocol) in an area that is accessible only using username and password.

Post
Information that contains patient identifiable/ sensitive (special category) or confidential information should be marked as 'Private and Confidential' when posted. Data sent via post should be sent as registered or recorded delivery.

Fax
Patient identifiable, sensitive (special category) or confidential data should not be sent by fax.

Text messages
Patient identifiable, sensitive (special category) or confidential data should not be sent via text message.

NHS Organisations
When sending raw data to an NHS organisation it should only be distributed to authorised hospital staff with an email address ending in ".nhs.uk" or "nhs.net". If an individual without an NHS email address or one that doesn't not belong to the Trust are requesting information details of the request should be forwarded to the hospital for which the data/report is being requested.

In all situations, encryption passwords, passphrases or keys must be communicated to the recipient via an alternative medium to the data itself. Informing a known recipient of a password via telephone is usually considered sufficiently secure for this purpose.

Personal data should not be taken out of the Society's offices or stored on a laptop computer or on physical media in an unencrypted form.

Encryption
In certain specified circumstances it may be necessary to unencrypt data held on the audit and registry systems, for example to allow linkage of data to other records for which specific and appropriate permission has been obtained. The key to the encryption will be made available to specified individuals only.

4.7 Retention and disposal of data

Data will be kept no longer than necessary and in accordance with the GDPR and the BTS Information Management and Record Keeping Policy (see section 5).

Data archival

Personal data that is no longer being used should be physically and electronically archived. This means that data in physical form should be stored in a secure, locked location and all access rights to the data in electronic form should be revoked and ultimately, the electronic data should be archived to a secure server and held in a secure location.

Note that for certain projects data may need to be destroyed rather than archived, upon completion of the project.

Electronic disposal

Computer files deleted from the server are not retained and are no longer available once deleted. Electronic files will be retained and disposed as per the schedule outlined in the BTS Information Management and Record Keeping Policy. Any computer equipment will be disposed of according to current industry standards.

Paper disposal

Personal identifiable / sensitive (special category) and confidential data should be kept in a locked cupboard when not in use. It should be disposed of using facilities provided for the temporary storage of confidential paper until they are removed for shredding. Papers considered "Highly Confidential" e.g. which contain personal identifiers, should be kept for the minimum period necessary and then shredded immediately.

BTS provides a cross-cutting shredder for the onsite disposal of confidential paper material. BTS also uses the services of a waste disposal agency with industry standard secure shredding for bulk confidential waste.

4.8 Handling a breach of confidentiality

In the event of a possible or actual confidentiality breach, all steps must be taken to mitigate exposure of confidential data as soon as possible. The Chief Executive/Deputy Chief Executive should be informed immediately and a report must be prepared in line with the BTS Incident Reporting Policy (Section 7). The Trustees of the Society should be informed and the steps taken to rectify the breach and guard against similar occurrences in future should be fully documented and relayed to the staff concerned.

4.9 Review of data handling procedures

The Chief Executive (or the Deputy Chief Executive acting on her behalf) is responsible for ensuring that procedures for handling data meet the requirements laid out in this document. Procedures are reviewed at least annually under the auspices of the BTS Information Governance Committee.

The impact of procedural changes, with respect to this document, should be assessed prior to any changes being made. If any procedure or procedures are found to be inconsistent with that laid out in this document, immediate steps should be taken to rectify the situation and to attain compliance.

This policy will be reviewed in May 2020.

1 May 2019

Section 5 BTS Information Management and Record Keeping Policy

5.1 Scope and Purpose

The BTS Information Management and Record Keeping Policy outlines the policy and procedures for the management of information held by the Society and the duration of retention and methods of disposal.
The document applies to all BTS staff and associates.

5.2 Definitions

This policy relates to all operational records held in any format by the Society. These include:

- all administrative records (e.g. personnel, estates, financial and accounting records,); and
- all records held on individuals (membership, event booking, audit and registry data, etc.)

The key components of records management are:

- record creation;
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- appraisal;
- archiving; and
- disposal.

The ***Records Life Cycle*** describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

In this policy, ***Records*** are defined as 'recorded information, in any form, created or received and maintained by the Society in the transaction of its business or conduct of affairs and kept as evidence of such activity'.

Information is an asset. The Society's Information assets are recorded on the BTS Information Asset Register.

The aims of the Records Management Policy are to ensure that:

- **records are available when needed**;
- **records can be accessed** - located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
- **records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- **records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;

- **records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- **records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required;
- **records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **staff are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management.

5.3 Responsibilities

The Chief Executive has overall responsibility for Society's records management and is the Data Controller (under the 2018 Data Protection Act/GDPR) and the Caldicott Guardian (with responsibility for the use of patient identifiable information).

All staff, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work and manage those records in keeping with this policy and with any guidance subsequently produced.

The Society will take actions as necessary to comply with the legal and professional obligations set out in:

- The Data Protection Act 2018 and General Data Protection Regulations (GDPR);
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice;
- and any new legislation affecting records management as it arises.

5.4 Retention and Disposal Schedules

It is a fundamental requirement that all of the Society's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the Society's business functions.

The retention periods for different types of record are set out in the Retention Schedule at Appendix 5. The retention schedule will be reviewed annually.

5.5 Records Management Systems Audit

The Society will regularly audit its records management practices for compliance with this framework. The audits will be conducted under the direction of the Chief Executive/Deputy Chief Executive.

The audit will:

- Identify areas of operation that are covered by the Society's policies and identify which procedures and/or guidance should comply to the policy;

- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of audits will be reported to the BTS Board as part of the annual audit and risk assessment cycle.

5.6 Training

All staff will be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes and guidance.

5.7 Review

This policy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are to be introduced).

1 May 2018
Due for review May 2020

Section 6 BTS System Level Security Policy

6.1 Introduction

This document refers to the computer systems owned and used by the British Thoracic Society both within the Society's Head Office building, and under contract or license with other suppliers. The System comprises three elements:

- The main BTS server is located in the Head Office building and hosts the office systems, local area network, the intranet and the remote access (terminal) server. This server holds personal information on BTS staff and BTS members/delegates.

- The Customer Relationship Management (CRM) database server (which hosts personal information pertaining to BTS members and other individuals, but no patient identifiable data) is hosted by Microsoft under a licensing agreement for Dynamics 365 and located on servers held in Germany.

- The following systems are hosted on secure servers administered by Westcliff Solutions from 1 February 2012 (and are based outside BTS Head Office):

  BTS website, discussion forums
  Abstracts system
  Elections system
  BTS Audit system
  BTS Registry system
  The Audit and Registry systems hold personal identifiable data in encrypted form.
  BTS system backups
  BTS Secure FTP servers
  Declarations of Interest system
  BTS MDRTB CAS system

The server provider for the hosted systems listed above, Cogeco Peer 1, adheres to the EU-US Privacy Shield. While the standard terms and conditions for Cogeco Peer 1 (Appendix 4) refer to data transferring outside the EEA – this clause generally applies to managed cloud hosted services and does not apply to the BTS servers which are not cloud hosted and managed only by Westcliff Solutions within the UK.

The Data Controller is the Chief Executive and the responsible IT staff include:

- The BTS IT Manager
- The BTS IT Assistant

6.2 System Security

The BTS computer System operates in accordance with the Information Governance Policy of the Society, reflecting best practice outlined in the NHS Connecting for Health Good practice guideline for web infrastructure and supporting services and the ISO/IEC 27002 (security standard of good practice).

The System incorporates the following security countermeasures:

Physical security measures – Doughty Street Office

- All network equipment (switches, firewalls and routers), servers and other access equipment are stored in secure areas with limited access to authorised personnel only.
- All desktop computers are in lockable office areas which has controlled access via door security into the building.

Logical measure for access control and privilege management –

- All BTS users are required to have login access to desktop computers.
- All BTS users must store data and resources on server drives which are controlled by login and user privilege control.
- All user rights and privileges to network data are approved and authorised by at least two individuals and implemented by the IT manager.
- Records of granted network access are kept and users removed when access is no longer required.
- The network drives are divided into areas requiring stricter control and areas containing less sensitive (special category) data. Access to the secure data network drive is strictly prohibited outside of the network.
- Access to the internal network is restricted to users with logins.

Network security measures –

- A firewall is in place to ensure that the system is not compromised.
- Network Login is controlled by the IT manager and device access is logged as part of the service.
- All external network traffic to and from the servers is digitally signed.
- Firewalls are secured using the latest software and recommended best practices and are intrusion tested on a quarterly basis by a completely external company
- All computers are required to have fully patched operating systems and an up-to-date Anti-virus protection.

Other

- No sensitive (special category) data are allowed to be removed from the BTS servers and all users are required to sign a confidentiality agreement to the effect.
- Access to the remote server is restricted to named and authorised individuals only.

6.3 System Management

The computer System is managed / developed / provided in collaboration with Westcliff Solutions Limited. The services provided by Westcliff Solutions are outlined in Appendix 4.

6.4 System Design

The computer System comprises:

- A fully patched and firewall network
- Unauthorised access to the system will be controlled by the following:
    - Authenticated login access to the network only.
    - Audit of the login authentication via Windows server.
    - Firewalls set at default deny with limited port opening.
    - All ICT equipment, servers, network infrastructure equipment and personal PC's, in secure buildings with controlled access.
    - Sensitive (special category) data are stored on secure servers and access to the data and drive is only permissible using authenticated login only.

Procedures for data collection and storage are outlined in the BTS Data Security Policy (Section 4).

6.5 Disposal

When computer equipment has become redundant or is no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data:

- Disks containing data of a sensitive (special category) nature, that are no longer required, will be wiped using software which meets the 'British Government Enhanced Data Removal' as detailed in document HMG CESG IS5. These will also comply with the 'WEEE' directive (http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx).
- Redundant back-up drives will be destroyed as above.

6.6 Internal Audit

The System shall benefit from the following internal audit arrangements:

- A review of systems to be undertaken once every 12 months.
- Review to be checked by the Chief Executive and form part of the annual Internal Audit process.

The System shall be risk assessed every 12 months using the grid assessment that forms part of the annual BTS Risk Assessment process.

6.7 System Protection

The following measures are in place to address disaster recover/ disruption/total system failure:

- An uninterrupted power supply is in place with 2 hours emergency power to allow planned shut down of services
- Offsite automated back-ups of the system are completed on a daily basis via secure FTP and are stored on secure servers provided by Westcliff Solutions

In the event of a security or confidentiality breach the BTS Incident Reporting Policy should be followed and steps taken to address the breach (see Section 7).

This Policy is reviewed on an annual basis for its completeness and for relevant updates.

The next review will take place in May 2020.

1 May 2019

Section 7 BTS Adverse Incident Reporting and Management Policy

7.1 Scope and Purpose

This policy applies to all staff in the British Thoracic Society. This includes contractors, associates, and temporary staff. The policy should be read in conjunction with the BTS Information Governance Policy, and the Health & Safety Policy.

The aim of adverse incident management is to ensure that systems are in place to secure member, delegate, staff and visitor safety, ensure internal accountability and safeguard BTS assets and reputation. Learning from adverse incidents and near misses enables the Society to reduce risk and improve services proactively. The purpose of this policy is to enable a robust and systematic approach to be consistently applied to the management of all adverse incidents. In so doing, it ensures that BTS meets all relevant statutory responsibilities and reporting requirements; and that the BTS safeguards the wellbeing of its members/delegates, staff and visitors.

7.2 Objectives

- To respond quickly and appropriately to incidents
- To provide a safe environment for members/delegates, staff and visitors.
- To provide information to allow effective evaluation and monitoring of BTS activities, services and procedures
- To provide formal documentation to assist in the management of complaints, claims and investigations
- To provide information to allow effective evaluation and monitoring of BTS activities, services and procedures
- To facilitate organisational learning to reduce subsequent/similar risk
- To provide staff with an opportunity to participate in and effect changes in practice and services to members and the public

The Society recognises that adverse incidents will occur and that it is important to identify causes to ensure lessons are learned to prevent reoccurrence. This policy and its linked procedures will ensure that staff have access to a comprehensive, clear and user-friendly adverse incident reporting system that will encourage the reporting of adverse incidents so that real opportunities for improvement and risk reduction are taken.
Where learning from such adverse incidents is identified the necessary changes will be put in place to improve practice. Learning and sharing from adverse incidents can only take place when they are reported and investigated in a positive, open and structured way.

Crucial to the effectiveness of adverse incident reporting is the Society's wish to promote an open, honest and just culture where all staff can participate in reporting adverse incidents.

All staff must report and manage adverse incidents according to this policy and related procedures for adverse incident reporting. Staff who make a prompt and honest report in relation to an adverse incident or near miss will not be disciplined except under the following circumstances:

- A breach of law
- Willful or gross carelessness or professional misconduct
- Repeated breaches of Society policy and procedure
- Where, in the view of the Society, the action causing the adverse incident is far removed from acceptable practice
- Where there is failure to report a major or catastrophic adverse incident in which a member of staff was involved or about which they were aware.

Completion of an Adverse Incident Reporting form does not discharge staff of the duty of care and their risk management responsibility. The Chief Executive/Deputy Chief Executive will ensure timely and appropriate follow-up of adverse incidents and to identify contributing factors to these events and will ensure that changes are identified to minimise risk.

Appropriate training and guidance will be provided to ensure that all employees understand their responsibilities under this policy and are able to effectively fulfil their obligations to report identified risks and adverse incidents.

Guidance on data security breach management is available on the ICO website at:
https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf
Incident report forms are included at Appendix 5.

7.3 Definitions

Adverse Incident: "Any event or circumstances that could have or did lead to harm, loss or damage to people, property, environment or reputation." (How to Classify Adverse Incidents and Risk, HPSS April 2006)

Harm is defined as "injury (physical or psychological), disease, suffering, disability or death".
A near miss is a situation in which an event or omission, or a sequence of events or omissions, arising during clinical care fails to develop further, whether or not as the result of compensatory action, thus preventing injury to a patient. (Organisation with a memory, Department of Health, 2000) 'Incidents that did not lead to harm but could have are referred to as near misses'. (Doing Less Harm. NHS. National Patient Safety Agency 2001).

7.4 Roles and Responsibilities:

The BTS Board is responsible for the implementation of the Policy for Reporting and Management of Adverse Incidents through the Officers' Group and the Chief Executive, and will:

- Ensure that the organisational arrangements contained within the policy and its associated procedures are implemented;
- Monitor and review the overall reporting performance and receive regular reports from the Chief Executive ;
- Promote an open, honest and just culture for adverse incident reporting;
- Maintain systems for the reporting, recording and analysing of adverse incidents;
- Make arrangements for the investigation of significant adverse incidents;
- Ensure that subsequent learning from adverse incidents is shared across the Society;
- Ensure that the Society has an appropriate risk management training programme which is accessible to relevant staff;
- Disseminate and promote this policy and procedures within their responsibility and ensure its implementation by providing support and advice to staff;
- Ensure reported adverse incidents are investigated appropriately;
- Ensure that adverse incidents are monitored and reviewed and that any recommendations made as a result of investigations are implemented and monitored;
- Take account of relevant adverse incidents when reviewing the Society's Risk Assessment;
- Ensure staff have access to advice and training on adverse incident reporting and management and, where appropriate, investigation and review.

- Ensure that copies of incident forms are retained (see Appendix 5)
- Ensure that their staff are aware of and adhere to this policy and associated procedures.
- Ensure staff are given appropriate support following an adverse incident

In the event of an adverse incident, all Staff have a responsibility to:

- ensure individuals involved (patients, clients, visitors or staff) and the environment / equipment, are made safe
- avoid putting themselves and others in situations of danger
- ensure the Chief Executive/Deputy Chief Executive is informed
- co-operate with the adverse incident investigation process

Education and training will be provided for all staff to ensure that each member of staff is aware of their responsibilities regarding the reporting of adverse incidents and follow-up as required.

This Policy will be reviewed in May 2020.

May 2019

Section 8 BTS Information Asset Register and Risk Assessment

8.1 Purpose

The BTS Information Asset Register is used to record all information assets held by the Society, and as a means of assessing risk. The components of the Information Asset Register (Record of Processing Activity – ROPA) is at Appendix 6.

A Data Privacy Impact Assessment should be carried out for all new or potentially new information assets (Appendix 7). Data Privacy Impact Assessments are a requirement of the General Data Protection Regulation (see Section 3).

8.2 Who is this document for?

This document outlines the policy and procedure for documenting information assets held by the Society and for recording all assessed risks.

The Register and Risk Assessment should be completed by:
Chief Executive, Deputy Chief Executive, Director of Operations, those staff acting on behalf of the CE/DCE.
The document should be read by all staff.

8.3 Definitions

There are various categories of Information Assets including:
Databases: Current and archived.
Paper records: Current and archived.
Software: Applications, programs, systems development tools and utilities.
People: Qualifications, skills and experience.
Policies: Procedures, guidance and training.
Intangibles: Public confidence in the organisation's compliance with the General Data Protection Regulation and Information Governance Policies.

8.4 Information Incident Reporting

All incidents of confidential and/or personal data breaches must be reported to the Chief Executive/Deputy Chief Executive in line with the BTS Information Governance Policy (Section 1) and the BTS Incident Reporting Policy (Section 7).

This policy will be reviewed in May 2020.

1 May 2019

Document control	
Document title: BTS IG Policy	
Version number: 3.0	Author (name, job title): Sally Welham, Deputy Chief Executive
Date approved:	4/6/2019
Effective date:	Approved by: BTS Board
Superseded version: 2.9.1	Date of next review: 2020
Staff members permitted to edit this document: Sheila Edwards, Sally Welham, Maria Loughenbury	

Version control history

Version #	Purpose/change	Author	Date
V1.1	Draft	Sally Welham	30/11/2011
V1.2	Approved by BTS Executive Committee	Sally Welham	2/2/2012
V2.4	Approved by BTS Executive Committee	Sally Welham	19/6/2013
V2.5	Approved by BTS Executive Committee	Sally Welham	23/7/2014
V2.6	Approved by BTS Executive Committee	Sally Welham	24/7/2015
V2.7	Approved by BTS Officers on behalf of Board	Sally Welham	5/9/2016
V2.8	Approved by BTS Officers on behalf of Board	Sally Welham	29/9/2017
V2.9 and V 2.9.1	Review IG Committee Approved by BTS Board June 2018	Sally Welham	1/5/2018
3.0	Review IG Committee Approved by BTS Board June 2019	Sally Welham	1/5/2019

Appendix 1 Privacy Policy – updated May 2019
(Available on the BTS and other websites as listed below)

WHO WE ARE

We are The British Thoracic Society (**BTS**).

BTS is the controller and responsible for this website.

HOW DO YOU USE MY DATA?

When you are involved in the British Thoracic Society, the BTS Lung Disease Registry, the BTS MDR-TB Clinical Advice Service, BTS Clinical Audit or Respiratory Futures programmes.

We have produced specific notices for when you are involved in our clinical advice, registry or clinical audit programmes. Please click here to view the notices that apply to each programme.

How we handle data submitted through one of the BTS websites (BTS/Respiratory Futures/clinical audit/registry/MDRTB CAS) is outlined in the BTS Information Governance Policy and specific information about handling clinical data is outlined in the BTS Clinical Data Policy.

When you become a BTS member

When you become a member of BTS, we will use your personal information to process your membership application and provide you with your membership information and benefits, such as your subscription to our journal or linked membership of the European Respiratory Society. The details we collect from you when you become a member include your name, address, email, telephone numbers, date of birth, employer/academic institution ethnic origin and payment details.

To complete your membership application, we share your personal information with our subcontractors who are involved in the membership application process, such as payment providers, as well as credit reference agencies who we use to assess fraud, credit and/or security risks.

We need to process your personal information in this way to register you as a member and provide the ongoing membership services and benefits to you.

When you attend one of our events

When you attend one of our events (such as our Summer Meeting or a short course), we will collect the following information from you: name, address, email, telephone numbers, employer/academic institution, ethnic origin and payment details. If you are already a member and register to attend an event, we will use the membership details we already hold on file for you to confirm your booking. We need to use your personal information in this way to complete the booking contract between us.

We provide a delegate list to the organisations and other individuals who attend our events. We do this because we have a legitimate interest in wanting to help build and develop the scientific community. You can object to us using your information in this way by contacting us via any of the methods listed on our contact us page.

When you use our website to submit an Abstract for one of our conferences.

We will use your personal information to process your abstract submission and provide you with details about the abstract process including the outcome of the abstract selection process. The details we collect from you when you submit an abstract include your name, address, email, telephone numbers, date of birth and ethnic origin.

When you have asked to receive promotional communications from BTS:

This section applies if you have opted in to receive promotional communications from us. You are not under any obligation to provide us with your personal information for promotional purposes, and you can update your communication preferences at any time by logging into our website or contacting us via any of the methods listed on our contact us page.

We will handle your personal information (such as your name, email address, postal address, telephone number and previous interactions with us) to provide you with promotional communications in line with any preferences you have told us about.

When we send you promotional emails, we rely on your consent to do this. Every email we send to you for promotional purposes will also contain instructions on how to unsubscribe from receiving them

You can tell us that you do not want your personal information to be processed in this way at any time by contacting us via any of the methods listed on our contact us page or, where relevant, by following the unsubscribe link shown in every marketing communication you receive from us.

To make our site better:

We will also use your personal information for the purposes of making our site more secure, to administer our site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes. We process your personal information for this reason because we have a legitimate interest to provide you with the best experience we can, and to ensure that our site is kept secure.

You can prevent us from using your personal information in this way by using the 'do not track' functionality in your internet browser. If you enable do not track functionality, our site may be less tailored to your needs and preferences.

When required by law:

In some circumstances we may also need to share your personal information if we are under a duty to disclose or share it to comply with a legal obligation.

WHAT ABOUT TECHNICAL INFORMATION AND ANALYTICS?

Information we collect about you: When you visit our site we will automatically collect the following information: technical information, including the Internet protocol (IP) address used to connect your computer to the internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, screen resolution, operating system and platform; and information about your visit, including the full Uniform Resource Locators, clickstream to, through and from our site (including date and time), page response times, download errors, length of visits to certain pages, page interaction information (such as

scrolling, clicks, and mouse-overs) and methods used to browse away from the page.

Information we receive from other sources: We are also working with third party analytics providers from whom we may also receive general aggregated anonymous information about you.

We will combine the information you provide to us with information we collect about you. For information about our use of cookies, please see our Cookies Policy.

WHERE IS MY DATA STORED?

Personal information collected by BTS, including clinical data collected through our Audit/Registry and MDR-TB CAS sites, is stored on secure servers based within the EEA.

However, many of the third parties we use to help us run our charity are based outside of the European Economic Area (**EEA**), so their processing of your personal information will involve a transfer of your personal information to a location outside of the EEA.

Whenever we transfer your personal information outside of the EEA, we ensure it is protected by making sure at least one of the following safeguards is in place:

- by transferring your personal information to a country that has been deemed to provide an adequate level of protection by the European Commission;
- by using specific contracts approved by the European Commission which give your personal information the same protection it has inside the EEA; and
- where we use providers based in the US, we may transfer data to them if they are part of the EU – US Privacy Shield which requires the recipient to provide a similar level of protection to your personal information in the US as it has inside the EEA.

To keep this privacy policy as short and easy to understand as possible, we have not set out the specific circumstances when each of these protection measures are used. You can contact us via any of the methods listed on our contact us page for the details as to how we protect specific transfers of your data.

All information you provide to us is stored on our secure servers or those of our third party data storage providers.

HOW LONG DO WE RETAIN YOUR DATA FOR?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting or regulatory requirements.

To determine the appropriate retention period for the personal information we hold, we consider the amount, nature and sensitivity of the personal information, the risk of harm from unauthorised use or disclosure of your personal information, the reasons why we handle your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements.

As outlined in the BTS Information Governance Policy and the BTS Clinical Data Policy, we may anonymise your personal data so that it can no longer be associated with you for research or statistical purposes, in which case we may use this information indefinitely without further

notice to you.

WHAT ARE MY RIGHTS UNDER DATA PROTECTION LAWS?

You have various rights under the data protection laws, which you can exercise rights by contacting us via any of the methods listed on our contact us page. The rights available to you are summarised below:

- **Request access** to your personal information (commonly known as a "subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove your personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your data for direct marketing purposes, research or statistical purposes.
- **Request the restriction** of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

You always have the right to lodge a complaint with us or the Information Commissioner's Office, the data protection authority in England and Wales.

WHAT ABOUT WEBSITES WE LINK TO?

Our site connects you to different websites. If you follow a link to any of these websites or use our services, please note that you have left our site and these websites have their own privacy policies.

We do not accept any responsibility or liability for these policies or websites. Please check their policies before you submit any personal information to them.

WHEN WILL YOU CHANGE YOUR PRIVACY POLICY?

Any changes we make to our privacy policy in the future will be posted on this page and, where appropriate, notified to you by e-mail or post.

Please check back frequently to see any updates or changes to our privacy policy.

HOW DO I CONTACT YOU WITH FEEDBACK?

Your feedback and suggestions on this notice are welcome. If you feel that we have overlooked an important perspective or used language which you think we could improve, please let us know by contacting us via any of the methods listed on our contact us page.

This privacy policy was last updated on 2 May 2019.

BTS Cookie Policy

Like many organisations, the British Thoracic Society (BTS) and Respiratory Futures makes use of cookies on our websites. This includes any address or URL ending in brit-thoracic.org.uk or respiratoryfutures.org.uk ("websites").

Our websites use cookies to distinguish you from other users of our sites. This helps us to provide you with a good experience when you browse our sites and also allows us to improve our sites.

A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer. We only use (and store) non-essential cookies on your computer's browser or hard drive if you provide your consent.

Cookie	**Purpose**	**Expiry**
_ga, _utma,	These cookies are used by Google to collect information about how visitors use our sites. We use the information to create reports which help us improve our sites. They collect information in an anonymised form, such as the number of visitors to our sites, which pages they came from and the pages they visited.	2 years
_utmz		6 months
_gid		1 day
_utmt		1 day
_gat		1 minute
__utmb		1 day
__utmc		End of browser session
_utm.gif		End of browser session
__RequestVerificationToken	This cookie helps prevent Cross-Site Request Forgery (CSRF) attacks.	End of browser session
_atuvc, _atuvs, _loc, _uvc	This cookie enables social media functionality on our site.	End of browser session
_cfduid	This is used by Cloudfare to ensure the traffic visiting our site is genuine.	1 year
ASP.NET_SessionId	This is used to preserves the visitor's session state across page requests.	End of browser session
rc::c	This cookie is used to distinguish between humans and bots.	End of browser session

You can block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our site if the particular settings you have chosen disables functionality our website relies on to display properly.

BTS 15 May 2019

Appendix 2 British Thoracic Society Confidentiality statement for staff, volunteers and associates

When working for BTS, you will often need to have access to confidential information which may include, for example:

- Personal information about individuals who are members or who are otherwise involved in the activities organised by BTS.
- Information about the internal business of BTS.
- Personal information about staff and other individuals working for BTS
- Personal information on other individuals collected in the course of activities conducted by BTS.

BTS is committed to keeping this information confidential, in order to protect people and BTS itself. 'Confidential' means that all access to information must be on a "need to know" basis and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act and General Data Protection Regulation, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by BTS to be made public. Passing information between BTS and an organisation that is a working with BTS under contract, or *vice versa* does not count as making it public, but passing information to an external organisation (that is not a BTS contractor) does count.

You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- not compromise or seek to evade security measures (including computer passwords);
- be particularly careful when sending information to other agencies and organisations;
- not gossip about confidential information, either with colleagues or people outside BTS;
- not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it.

If you are in doubt about whether to disclose information or not, **DO NOT GUESS**. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working or volunteering for BTS.

I have read and understand the above statement and the Confidentiality Policy. I accept my responsibilities regarding confidentiality.

Signed: **Date:**

A**ppendix 3**
BTS Records Retention Schedule

Guiding Principles:-
That documents/records are kept in line with the aims of the BTS policy outlined above, and with due regard to the GDPR.

Category	**Paper (P) Electronic (E) Both (B)**	**Retain number of years**	**Format**	**Method of disposal**	**Lead responsibility**
Operations & Finance					
Financial records - invoices, bank statements, receipts. Includes membership and delegate booking payments.	B	7	B	Archive electronic records, and dispose of paper in confidential bags.	Head of Finance and Events Support
End-of year audit and management accounts	B	7 Trustees' Report and Annual Accounts in perpetuity	B	As above	Chief Executive
Human resources files	B	7, after staff member leaves	B	As above	Chief Executive
Contracts for services and suppliers	B	For life of contract. Then destroy after 3 years.	B	As above.	Executive Assistant
Membership					
Application forms, records of activity (see also Finance)	B	3 categories: When a member dies remove from CRM and destroy paper file at earliest opportunity; If a member retires and indicates that s/he does not wish to remain a member, do the same after a 3 year period; If a member fails to renew, or lapses, retain information for a year beyond	B	In confidential disposal bags As above As above	Membership Manager

		next renewal period, then proceed as above.			
Governance					
Annual Reports & AGM papers	B	In perpetuity	B	N/A	Chief Executive
Standing Committee papers	B	In perpetuity	B	N/A	Chief Executive/Deputy Chief Executive
Returns to Charity Commission & Companies House Office of Scottish Charity Regulator	E	In perpetuity	On-line records will be kept by CC/CH/ OSCR	N/A	Chief Executive
Memorandum & Articles and related correspondence	B	In perpetuity			Chief Executive
Declarations of Interest	E	For length of time a member serves on a Committee, and 2 years beyond. For guideline groups – until the guideline is withdrawn/supercee ded.	E	To be discussed	Chief Executive
Elections	E	*To be discussed*	E	To be discussed	Chief Executive
Programmes & projects					
Thorax contract Thorax	B	For life of contract. Archive all except current issue	B		Chief Executive
RCP London HQIP COPD project	B	Contract/administrat ive documents - For life of project – then as for contracts above	B		Chief Executive/Deputy Chief Executive
Guidelines/ Quality Standards					
Guidelines	B	In perpetuity – for reference	B		Deputy Chief Executive
Quality Standards	B	In perpetuity – for reference	B		Deputy Chief Executive
Audit/Registry data:					
Audit data	E	In perpetuity	E		Deputy Chief Executive

Registry (ILD and MDRTB) data	E	In perpetuity	E		Deputy Chief Executive
Other BTS Reports & Publications					
Other BTS Reports & Publications	B	In perpetuity	B		Chief Executive/Deputy Chief Executive
General enquiries & Correspondence					
Emails	E	3 months	E		Chief Executive/Deputy Chief Executive

1 May 2018

Appendix 4 – Westcliff hosting terms and conditions
See separate document

Appendix 5
BTS Incident Report Forms

Name of person completing form:

Site where incident took place:

Date of incident:

Time of incident:

Nature of incident – please give full details:

Give details of how the incident took place:

All of the above facts are a true and accurate record of the incident.

SIGNED: DATE:

NAME:

Received by Chief Executive/Deputy Chief Executive (date/signature):
_____

Incident Report to the BTS Board - data/security breach

Site where incident took place:

Date of incident:

Time of incident:

Nature of incident – include details of how the incident took place:

What type of data is involved?

How sensitive is it?

What has happened to the data?

Regardless of what has happened to the data, what could the data tell a third party about the individual?

Risk of over-notifying
Decision reached:

Appendix 6

GDPR Information Asset/Audit Table – Record of Processing Activity (ROPA)

This includes details for each use or sharing of personal information undertaken at BTS (including information on data flows, legal bases for processing data, contract dates, the quantity of data involved and other information).

Data items/system	Lawful basis for processing (under GDPR article 6)	Data flow to and from	Consent	Quantity of data (approx. no of individual records)	Supplier contract details	Record review details	Level
BTS members: *Name* *Address* *DOB* *Email* *Telephone* *Financials*	(f) Legitimate interests	From individual to BTS CRM From BTS to BMJ (Thorax) From BTS to ERS (ERS membership)	Opt-in requested for: eBTS News	3,500	Supplier: AMS Start date: 04/06/2018 End date: 03/06/2019	Continuous review by BTS Head Office staff.	Critical to organisation
Contacts on BTS CRM: *Website users (abstracts, online booking)*	(f) Legitimate interests	From individual to BTS CRM From BTS to BMJ (Thorax – Winter Meeting abstracts)	Opt-in confirmed when registering to submit an abstract/book online, etc.	3,500	Supplier: AMS Start date: 04/06/2018 End date: 03/06/2019	Continuous review by BTS Head Office staff.	Critical
Suppliers and contractors	(b) Contract (f) Legitimate interests	From individual to BTS CRM/SAGE	No	200			Critical
BTS Audit system users: *Name* *Address* *Email* *Telephone*	(f) Legitimate interests	From individual to BTS Audit system database	Opt-in when logging in/registering for first time.	4,000 user records	Suppliers: Westcliff Solutions and CTEC Systems Dates: N/A (ongoing)	Continuous review by site users and BTS Head Office staff.	Critical
BTS ILD Registry system users* *Name* *Address*	(f) Legitimate interests **Patient data records covered by ethical*	From individual to BTS ILD Registry system database	Opt-in when logging in/registering for first time.	200 user accounts 2,000 patient records	Suppliers: Westcliff Solutions and CTEC Systems	Continuous review by site users and BTS	Critical

Email *Telephone*	*approval/individual consent*				Dates: N/A (ongoing)	Head Office staff.	
BTS MDR-TB CAS system users** *Name* *Address* *Email* *Telephone*	Legitimate interests ***Patient data records covered by ethical approval/individual consent*	From individual to BTS MDR-TB CAS system database	Opt-in when logging in/registering for first time.	200 user accounts 100 patient records	Suppliers: Westcliff Solutions and CTEC Systems Dates: N/A (ongoing)	Continuous review by site users and BTS Head Office staff.	Critical

Reviewed July 2018 by Sheila Edwards, BTS Chief Executive

Appendix 7 BTS Data Privacy Impact Assessment: Guidance and Template

1 What is a Data Privacy Impact Assessment (DPIA)?

BTS collects and holds personal and organisational information as part of its activities. This process has a number of risks including security, data quality and privacy. The Society has a responsibility to ensure that its activities maintain appropriate privacy for those involved in its activities and other stakeholders.

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. GDPR requires that a DPIA is produced for all processing likely to result in a high risk for individuals. It is also good practice to do a DPIA for any other major pojects.

2. The DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

3. Further guidance on the conduct of a DPIA is available here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

A template DPIA is also available on the ICO website above.

4. Since the introduction of GDPR, BTS has produced a DPIA for the BTS CAP audit 2018/19 in line with the good practice outlined by ICO.

5. BTS will produce a DPIA for any major new project in future in line with ICO guidance.

May 2019