General Osteopathic Council

General Osteopathic Council

Information Governance Assurance Framework

Contents

1. Introduction

The General Osteopathic Council (GOsC) is established under section 1 of the Osteopaths Act 1993 (the Act). The GOsC's statutory duty is to develop and regulate the profession of osteopathy. In common with other statutory regulators of healthcare professionals, the primary aim of the GOsC in the exercise of its function is to ensure the protection of patients and members of the public.

As a public body, and a statutory regulator, the GOsC holds information from various sources. This includes: information about the individuals who are included in the register that the GOsC is required to maintain under section 2(3) of the Act; information about osteopathic educational institutions and the qualifications issued by them, which the GOsC is required recognise under section 14 of the Act; information relating to concerns raised by and queries from members of the public; patient records held as part of investigations by the GOsC into concerns about its registrants; and general regulatory and policy material, including information relating to GOsC stakeholders.

The GOsC considers the information that it holds to be a vital asset and integral part of corporate governance, both in terms of enabling it to fulfil its statutory functions; and to enable it to manage services and resources efficiently.

The purpose of this document is to set out a comprehensive information governance assurance framework for preserving the confidentiality, integrity, security and accessibility of data processing systems and information held by the GOsC; and which maximises the value to the GOsC of the information that it holds.

The framework seeks to ensure that information is:

- obtained fairly and lawful
- recorded accurately and reliably
- held securely and confidentially, for a proportionate period of time
- used effectively
- shared and disclosed appropriately and lawfully
- disposed of securely.

In addition, the framework seeks to ensure that the GOsC complies with relevant legislative and regulatory requirements relating to the handling of information, and with emerging best practice in this area.

The framework also seeks to ensure that staff and non-executives are appropriately trained, and aware of their individual and collective responsibilities in respect of all the information held by the GOsC; and that there are appropriate procedures in place for the investigation and reporting of data breaches.

2. Framework scope

This framework applies to all:

- information, information systems, networks, applications and locations operated or used by the GOsC
- GOsC employees
- members of the GOsC Council, GOsC statutory and non-statutory Committees and working groups
- third parties undertaking work on behalf of the GOsC.

3. Framework principles

The principles underlying this Information Governance Assurance Framework are:

Compliance and accountability

All staff and non-executives should be trained and made aware of legal and regulatory requirements; and should understand their individual and collective responsibilities in relation to information held by the GOsC.

Maintaining information security and preserving the confidentiality of personal and commercially sensitive information should be seen by all staff as an integral part of daily business operations.

Consent to use or disclose information must be obtained where required, particularly in respect of the handling of patient records held by the GOsC.

Openness

An appropriate balance should be maintained between openness and confidentiality in the management and use of information.

Non-confidential information about the GOsC should be made available routinely or on request in a variety of media.

The GOsC should have clear policies and procedures for:

- responding to queries, subject access and freedom of information requests
- handling information relating to concerns raised by members of the public and other healthcare professionals
- publication of material relating to the business of the GOsC's Council, committees and working groups
- publication of material relating to the investigation and determination of concerns about the fitness to practise of persons registered with the GOsC
- liaison with the press and media

- sharing of information with the four UK health departments, other regulatory bodies and law enforcement agencies
- regular sharing of information with osteopathic educational institutions and the Quality Assurance Agency, and partners in the osteopathic development agenda.

Information Security

The GOsC will maintain:

- secure systems for the storage of electronic and paper information
- effective authorisation procedures for the use of, and access to confidential information and records
- effective procedures for the investigation and reporting of data breaches.

Quality Assurance

Wherever possible, information quality should be assured at the point of collection.

The GOsC will maintain effective procedures in relation to:

- audit and data reconciliations
- records management
- version control.

The GOsC will undertake periodic assessments of its policies and procedures against these principles. In particular, the GOsC will ensure that:

- The GOsC maintains an accurate an up-to-date information asset register
- A formal information security risk assessment for key information assets has been undertaken and is reviewed on a periodic basis
- All information assets that hold (or are), personal data are protected by appropriate organisational and technical measures
- Staff employment contracts include requirements to comply with information governance requirements
- Mandatory training or guidance on information governance is provided to all staff and non-executives
- Formal contractual arrangements that include compliance with information governance requirements are in place with non-executives and all third party contractors and organisations with whom information is shared on a regular basis
- Where required, protocols are in place to govern the routine sharing of information with other organisations
- The GOsC has in place documented policies and procedures in respect of:
  - records management (including version control)
  - incident reporting
- The GOsC's Audit Committee receives periodic reports about the operation of the GOsC information risk management policy and risk management strategy and operation of the Information Governance Framework

4. Legislative, regulatory and best practice requirements

The GOsC is required to comply with all relevant UK and European Union legislation including:

- *The General Data protection Regulation (GDPR)*
- *Data Protection Act 2018*
- *The Freedom of Information Act 2000*
- *Data Protection (Processing of Sensitive Personal Data) Order 2000*
- *The Copyright, Designs and Patents Act 1988*
- *The Computer Misuse Act 1990*
- *The Human Rights Act 1998.*

In addition to these statutory requirements, the GOsC is bound by the common law duty of confidentiality.

As a body concerned with the regulation of healthcare professionals, the GOsC may properly take into account the principles set out the NHS Codes of Practice on:

- Confidentiality
- Records Management
- Information Security management.

As the GOsC is often required to obtain patient medical records as part of its fitness to practise investigations and registration assessment processes, the GOsC will also take into account the 'Caldicott principles' set out in Health Service Circular 1999/012, and "The Information Governance Review" undertaken by Dame Fiona Caldicott (published in March 2013)and "A Guide to Confidentiality in Health and Social Care" published by the Health and Social Care Information Centre (September 2013).

As a statutory body operating in the public interest, the GOsC may also take into account best practice guidance issued by the Department of Health (including the NHS Information Governance Toolkit) and the Cabinet Office on Information matters.

In relation to best practice on information security, the GOsC will have regard to:

- ISO/IEC 17799:2000 *Code of Practice for Information Security Management*
- British Standard BS 7799 *Specification for Information Security Management*
- ISO 27001: 2005 *Information and Data Security*

In relation to best practice on information quality assurance, the GOsC will have regard to:

- BSI BIP:0008 *The British Code of Practice for Legal Admissibility and evidential weight of information stored electronically*

5. Accountability and responsibilities

Person	Responsibility
Council	• Council is required to approve the GOsC's policies in respect of information governance and risk management • Council maintains ultimate responsibility for ensuring that the GOsC continues to meets its legal and statutory obligations in respect of information governance • Council delegates this responsibility to the Chief Executive as Data Protection Officer (DPO)
Audit Committee	• The Audit Committee will receive periodic reports on the operation of this policy from the DPO • The Audit Committee will receive and consider individual reports from the DPO about serious adverse events relation to information including data breaches, and make recommendations and take appropriate action where necessary • The Audit Committee will include information governance in the internal audit programme
Individual non-executives	• Non-executives must ensure that they comply with the GOsC's policies in relation to information security, confidentiality, data protection and freedom of information • Non-executives may be required to attend training on the relevant legislation and policies arranged by the GOsC • Non-executives are responsible for the security of any information which they access through any fixed or mobile electronic device, whether or not it is owned by them • Non-executives are responsible for the security of any paper-based information provided to them and to ensure that it is disposed of securely. which they access through any personal device
Chief Executive	• The Chief Executive has delegated responsibility from the Council for ensuring that the GOsC continues to meet its

	legal and statutory obligations in respect of information governance • The Chief Executive is the GOsC's Data Protection Officer (DPO). • As DPO, the Chief Executive is responsible for ensuring that the GOsC has in place an effective information assurance governance framework which shall include information asset ownership, as well as and clearly defined roles, responsibilities and reporting requirements • The DPO is required to report to the Audit Committee and to the Council on the information governance arrangements in place, and the operation of those arrangements • The DPO is required to report serious adverse events relating to information governance, including data breaches to the Audit Committee and, where it is likely to pose a risk to people, to the Information Commissioner
Senior Management Team (SMT) and Heads of Department	• Collectively the members of the SMT will act as the GOsC's Information Governance Committee • The Information Governance Committee will develop and approve policies, standard operating procedures and guidance relating to information governance. • Individual Heads of Department are the Senior Information Asset Owners for all information assets located within their department, and are accountable to the DPO for providing assurance on the security and use of their information assets • The Director of Registration and Resources shall hold the GOsC Information Asset Register • Individual Heads shall ensure that the Information Asset Register is kept up to date and shall review the Register every six months • The Director of Fitness to Practise shall act as 'Caldicott Guardian' in relation to patient records held by the regulation and policy and standards departments
Managers/ Information Asset Owners	• Information Asset Owners (IAOs) are responsible for identifying, understanding and addressing risks to the information assets that they 'own'.

	• IAOs must ensure that the Information Asset Register maintained by the Director of Registration and Resources is kept up to date. • IAO's are accountable to Senior IAOs for providing assurance on the security and use of their information assets • IAOs involved in procurement shall be responsible for identifying circumstances in which potential or actual access to information or data may be required by third parties/service providers. • In such cases, IAOs shall ensure that appropriate information and confidentiality agreements are in place. • The GOsC standard terms and conditions relating to Confidentiality, Data Protection, and Freedom of Information must be included in any contract with a third party/service provider (advice should be sought from the Director of Fitness to Practise if necessary).
Caldicott Guardian	• The Director of Fitness to Practise will act as the GOsC Caldicott Guardian. • The Director of Fitness to Practise will oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies. • The Director of Fitness to Practise shall ensure that contracts are in place with external firms of solicitors and that such contracts comply with the requirements of the GDPR and Data Protection Act 2018. • The Director of Fitness to Practise shall ensure that all non-executives, and agents and contractors who are given access to personal data, such as fitness to practise solicitors are provided with specific guidance around data security and are regularly reminded of the importance of complying with this guidance
Information Governance Manager	• The Director of Fitness to Practise will act as Information Governance Manager • The Information Governance Manager will i. provide legal advice and guidance on information governance

	ii. in conjunction with the DPO and HR manager ensure there is suitable information governance training for all staff and non-executives iii. (together with the Director of Registration and Resources) investigate reported serious adverse events relating to information governance including data breaches iv. Maintain a log of serious adverse events relating to information governance including data breaches and feed back learning from such events to the SMT
IT Services Manager/IT Security Manager	• The Director of Registration and Resources will fulfil this role working with the IT and Business Support • In particular, the Director of Registration and Resources will: i. formulate and implement IT related policies ii. procure expert technical advice on matters of IT security iii. (together with the Information Governance Manager] investigate reported serious adverse events relating to information governance including data breaches and feed back learning from such events to the SMT iv. be responsible for the effective management and security of GOsC IT resources including infrastructure and equipment (including regular audits of equipment) v. require regular assurances from external providers that all firewalls and security protocols in relation to GOsC data and secure access to servers holding GOsC data are maintained and in place at all times vi. act as the IAO with specific accountability for computer and telephone/mobile technology (including laptops, pad and mobile devices, BlackBerries, memory sticks etc.)
HR Manager	The HR Manager is responsible for ensuring that: i. all staff undertake relevant information governance training ii. information governance forms part of induction of new members of staff iii. information governance matters are addressed in staff contracts of employment and disciplinary procedures
All staff	• All GOsC staff are required to comply with the GOsC's policies and procedures in relation to information governance, including data security; data integrity; and confidentiality • In particular, all staff are responsible for ensuring that: i. computer passwords and log in details remain secure

	ii. confidential information and/or sensitive personal data is not left unattended on photocopiers or desks iii. documents and files containing confidential information and sensitive personal data are placed in locked storage at the end of each working day iv. visitors do not gain unattended access to office premises, workstations, or document storage facilities v. the GOsC's archiving and data retention policies are fully complied with • All GOsC staff are required to undertake relevant training on information governance issues • All staff must be aware of the procedures for identifying and reporting data breaches to their line managers and the SMT
Third parties/ contractors	• Where potential or actual access to information assets is identified, third parties/contractors shall be required to provide and comply with appropriate information/ confidentiality agreements

Staff and non-executive training

1. All staff and non-executives will receive appropriate training on information security.

2. The level and type of training will depend on:

    a. an assessment of the types of information to which the individual has access
    b. the types of equipment that they use to access information
    c. the environment in which they work (e.g. office, home, while travelling).

3. Training may include formal individual or group learning sessions, remotely accessed online learning or other online briefing.

4. Where training or briefing is not provided directly by the GOsC, individuals will be asked to make a declaration that they have received and understood what is required of them.

7. Investigation and reporting of serious adverse events relating to information governance including data breaches

Roles and responsibilities

1. The Information Governance Manager (Director of Fitness to Practise) shall be responsible for maintaining a log of all adverse events relating to information governance.

2. The log shall contain details about:
   - the facts surrounding the breach
   - the effects of that breach
   - remedial action taken.

3. When investigating a serious adverse event relating to information governance, the Information Governance Manager should follow the guidance on data security breach management. In addition, the Information Governance Manager should consider using:
   - the Health and Social Care Information Centre document: *Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation* (https://www.igt.hscic.gov.uk/resources/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance.pdf)
   - the NHS Information Governance Toolkit Incident Reporting Tool (https://www.igt.hscic.gov.uk/resources/IG%20Incident%20Reporting%20Tool%20User%20Guide.pdf).

4. When investigating a serious adverse event relating to information governance, the Information Governance Manager must take into account:

   - the type of data involved
   - the sensitivity of the data
   - whether there are any protections in place, such as encryption
   - what has happened to the data-whether it has been lost, stolen or damaged
   - what the data would reveal to a third party about the data subject
   - how many individuals are affected
   - the type of individual (staff, customers, clients or suppliers)
   - the potential harm to individuals because of the incident (risks to physical safety, financial risks, reputational risks, identify fraud etc.)
   - wider consequences, such as public health risks or loss of public confidence.

5. The Information Governance Manager (in consultation with the Data Protection officer) must take a decision as to whether the breach must be reported to the ICO. If it is decided not to report a breach then this decision and the reasons must be recorded in the data breach log.

6. Data security breaches must be reported to the ICO without undue delay and, where feasible, within 72 hours, using the standard template which is available on the ICO website at https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc

7. Data security breach notifications should be emailed to the ICO at casework@ico.org.uk

8. The ICO has produced guidance for organisations on the information it expects to receive as part of a breach notification and on what organisations can expect from the ICO on receipt of their notification. This guidance is available on the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

9. As a minimum, the ICO will expect to receive information about:

    - a description of the nature of the personal data breach including, where possible:
        - the categories and approximate number of individuals concerned
        - the categories and approximate number of personal data records concerned

    - the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained
    - a description of the likely consequences of the personal data breach
    - a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

10. When the personal data breach is likely to result in a high risk to the data subject's rights and freedoms (for example, emotional distress, or physical and material damage) the Information Governance Manager shall communicate the personal data breach to the data subject without undue delay.

11. In addition to the ICO, the Information Governance Manager must also consider whether to notify any other persons, such as the police, insurers or professional bodies.

12. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

13. When informing the media, it is useful to inform them whether the GOsC has have contacted the ICO and what action is being taken. ICO will not

normally tell the media or other third parties about a breach notified to it, but it may advise the GOsC to do so.

8. Monitoring and review

This Framework and associated policies will be monitored by the SMT on an ongoing basis.

The Framework and associated policies will reviewed formally on an annual basis, and in addition will be reviewed upon the following occurring:

- significant legislative changes affecting information governance;
- significant new best practice guidance being issued by the NHS, Department of Health or Cabinet Office
- significant incidents, including data breaches; and
- significant changes to organisational infrastructure of the GOsC.

Version control

Document title	Document author	Version	Date	Detail of amendments
GOsC information governance assurance framework	Tim Walker	V2	25.05.18	Updated for compliance with GDPR

Pro-forma log for notification of data security breaches to the Information Governance Manager (Director of Fitness to Practise)

No	Ref	Date	No. Of people affected	Nature of Breach	Description of breach	How the GOsC became aware of the breach	Description of data	Consequences of the breach	Have all individuals been informed?	Remedial action taken by the GOsC	Have other regulators been informed?	Has the GOsC notified the ICO about this breach separately? If not, why not?

General Osteopathic Council policies annexed to

The Information Governance Assurance Framework

Appendix 1	**Information security policy**
Appendix 2	**Records management policy**
Appendix 3	**Data retention policy**
Appendix 4	**Policy relating to use of GOsC e-mail, use of internet and use of social networks while at work**
Appendix 5	**Policy on disposal of it equipment and confidential waste**
Appendix 6	**Information quality assurance policy**
Appendix 7	**Freedom of information policy**
Appendix 8	**Protocol for handling patient records within the Professional Standards Department**
Appendix 9	**Protocol for handling patient records within the Regulation Department**

Appendix 1

General Osteopathic Council

Information security policy

Purpose

The purpose of this document is to formalise in detail the IT Information Security Policy. It will be used mainly by the IT Department. The information in this document is correct at the time of creation and will be updated on a regular basis. Further documentation can be created based on the items in this document.

Contents

Information Security Policy

1. Introduction

Data stored in information systems represents an extremely valuable asset. The General Osteopathic Council (GOsC) recognises that data used and stored by it on information systems and in other forms is fundamental to its statutory role of regulating osteopaths in the United Kingdom. The GOsC has a responsibility to its stakeholders to ensure that these systems are developed, operated and maintained in a safe and secure fashion. Increased activity in transmitting information across networks of computers and between third party organisations, makes data extremely vulnerable to accidental or deliberate, unauthorised modification or disclosure. The consequences of information security failures can be costly, in both financial and reputational terms, and rectification can be extremely time-consuming.

This outline Information Security Policy sets out appropriate security objectives and responsibilities through which the GOsC will facilitate the secure and reliable flow of information, both within the GOsC and in external communications.

2. Objectives

The objective of this policy is to ensure that all information and information systems upon which the GOsC depends are adequately protected to the appropriate level. This is supported by the Senior Management Team's (SMT) commitment to:

a. view information security as a business critical issue;
b. develop a culture of information security awareness;
c. use established methods for risk assessment, management and acceptance;
d. implement information security controls which are proportionate to risk;
e. requiring individual accountability for compliance with information security policies and supporting procedures.

3. Scope

The scope of this policy extends to all information in all its forms handled by GOsC employees, including temporary staff, as well as contractors, non-executive members (Council, committees etc), GOsC associates, and agents. The information may be on paper, stored electronically or held on film, microfiche or other media. It includes data, text, pictures, audio and video. It covers information transmitted by post, by electronic means and by oral communication, including telephone and voicemail.

This policy applies throughout the lifecycle of the information, from creation through storage and use, to disposal. Appropriate protection is required for all forms of information, to ensure business continuity and to avoid breaches of the law, and to meet statutory, regulatory or contractual obligations. This also includes all GOsC owned/licensed data and software, be they loaded on GOsC or privately/externally

owned systems, and to all data and software provided to the GOsC, by sponsors or external agencies.

The scope of this policy extends to all processing and storage systems used in support of the GOsC's operational activities to store, process and send and receive information.

4. Policy Statement

It is essential that all GOsC information is adequately protected from events which may jeopardise regulatory obligations. These events include accidents as well as behaviour deliberately designed to cause difficulties. The purpose of this policy is to preserve:

a. confidentiality: data access is confined to those with specified authority to view the data
b. integrity: safeguarding the accuracy and completeness of information and processing methods
c. availability: information is delivered to the right person at the right time.

The GOsC will develop, implement and maintain policies, supporting procedures and guidance, to achieve appropriate levels of information security. These will cover the range of elements that need to be addressed in the management of information security.

5. Retention and Disposal of Information

All GOsC employees, including temporary staff, as well as contractors, non-executive members (Council, committee members etc), GOsC associates and other authorised users of GOsC information storage and processing systems, have a responsibility to consider security when creating, using and disposing of information owned by the GOsC. Procedures for the disposal of information (which may involve destruction of the information or the transfer to archival storage) at the end of the retention period, will be documented. Each department will establish procedures appropriate to the information it holds and processes, and ensure that all staff and other users are aware of those procedures.

6. Information Security Incident Reporting

All GOsC employees, including temporary staff, as well as contractors, non-executive members (Council, committee members), GOsC associates and other authorised users of GOsC information storage and processing systems, should report it immediately to the Director of Fitness to Practise, either by email, by telephone, or in person if:

a. any observed or suspected security incidents where a breach of the GOsC's information security policies has or may have occurred; or

b. any information security weaknesses in, or threatens to, information processing or storage systems.

Users and Desktops

7. Password Policy

Each IT System that is accessed by a username requires a password. Each password must contain at least 8 characters and must contain at least three of the following – lowercase letters, uppercase letters, numbers or symbols. Passwords on all systems are set to expire after 30 days. Once the password has expired, the user will have to reset the password before being able to access the system. A password history of 6 months has been applied, meaning that users will not be able to use the same password they have previously used in the past 6 months. The password history is inaccessible to anyone including the Systems Administrator, and is encrypted in the Windows Operating System. Administrator account passwords are set and kept by the IT Department and Director of Registration and Resources.

8. Data Leakage

Data leakage is when secure information enters the public domain, either by accident or on purpose. The GOsC will do what is necessary to minimise the risk of data leaks by complying with the Information Governance Framework, the Staff Handbook and this document. Data leaks can also be minimised by members of staff's due diligence, making sure that they only keep secure information within Sharepoint/OneDrive, on their work computer, keeping data on password protected encrypted USB keys and only for a period that is necessary, and not carrying sensitive information outside of the GOsC Head Office on paper. All staff must complete the Cyber Security Awareness course through iHasco – the IT and HR Departments are responsible for granting access to iHasco.

9. Working Remotely

Any user wishing to work remotely has to ability to use Citrix, which is accessed using any web browser. Citrix provides users a point of entry to the GOsC network and data. It is therefore recommended that anyone accessing Citrix, does so from a device that is sufficiently protected by an Antivirus product and Windows Updates. Users can also access GOsC data using mobile device applications such as Office365. Users are required to enter their username and password to access this information. The GOsC IT Department has the ability to restrict access and remote wipe any GOsC data that is on any device.

10. Secure Bins

Secure bins are located on each floor. They are locked so that once paper has been inserted into the secure bin, it cannot be removed by anyone who doesn't have the key. Secure bins are the responsibility of the Facilities Department.

11. USB Devices

USB Devices are defined as any device that can be plugged into a USB port on any device that is connected to the GOsC network by USB. This includes (but is not limited to):

- USB Keys or Pen Drives
- External USB Hard Drives
- Mobile Phones
- Portable Music Devices
- Tablets/iPads

It is recommended by the IT Department that a USB device has the ability to be password protected or encrypted for the safety of the data on the USB device.

12. Mobile Devices

A mobile device is defined as a device that can be used on the move without needing a permanent desk to work and also has access to the GOsC network. This includes (but is not limited to):

- Laptops
- Mobile Phones
- Tablets/IPads

It is required that a mobile device is password protected using the Password Policy as detailed above or another means of securing the device (fingerprint, 6 digit PIN, etc)

IT Systems and Network

[Confidential]

Patch Management

[Confidential]

Suppliers

[Confidential]

Appendix 1

Version control

Document title	Document author	Version	Date	Detail of amendments
GOsC Information Security Policy	Carl Pattenden	V2.0	25 May 2018	
	Carl Pattenden	V2.1	28 February 2019	Updated to reflect new IT environment and addition of Patch Management

General Osteopathic Council

Records Management Policy

Introduction and definitions

1. Records Management is the process by which an organisation handles records from the process of creation to eventual disposal or permanent archive. It applies to all records, whether generated internally or externally, and in all formats and types of paper or electronic/digital media.

2. The process of records management involves creating a system to direct and control the way records are created and distributed (including file naming conventions and meta data); clearly indicating the version that is being accessed or worked on (version control, editing access rights, access tracking, etc.); filing and storage (folder architecture etc.); and the way in which, and length of time for which, records are retained or disposed.

3. In this policy, the following terms are used:

   Information lifecycle. Process of creating, maintaining, updating, reviewing, archiving and destroying information.

   Metadata. Data describing context, content and structure of records and their management through time.

   Records. Those documents required to facilitate the business carried out by the GOsC and retained for a set period to provide evidence of its transactions or activities. Records may be created, received or maintained in a variety of formats, including paper records, microfiche, audio and video cassettes, CDs, DVDs and computer files.

   Records system. Information system which captures, manages and provides access to records through time.

   Retention schedule. A list of the GOsCs record types covering review, preservation and destruction dates and actions associated with these types. Such dates and actions are usually determined by statute, legal, regulatory or business compliance.

   Restricted data. Restricted data includes but may not be limited to: patient records; information obtained during the investigation of complaints and fitness to practise cases; personal registrant information that does not form part of the statutory register; financial records; information provided to the GOsC that may be commercially confidential; HR records including information relating to both staff and non-executives.

Scope of policy

4. The GOSC's record management policy relates to all records held by the GOsC. This includes:

    - all administrative and corporate records (e.g. personnel, financial and accounting records, papers and minutes of meetings, complaints)
    - records relating to the GOsC Register and applications for registration
    - records (including patient records) relating to investigation of fitness to practise concerns
    - records relating to the recognition of qualifications by the GOsC
    - records relating to registration assessment and return to practice reviews
    - records relating to complaints about students or complaints about osteopathic education institutions.

5. The GOsC's records management policy draws from relevant standards and best practice guidance for records management, in particular:

    - BS ISO 15489-1: 2001 *Information and Documentation – Records Management part 1*
    - BS ISO 15489-2: 2001 *Information and Documentation – Records Management part 2*
    - DISC PD 0025-2: 2002 *Effective Records Management Part 2: Practical implementation of BS ISO 15489-1*
    - the Freedom of Information Act section 46 Code of Practice
    - Cabinet Office requirements regarding information governance and assurance.

Purpose of policy

6. The aims of the GOsC's records management system is to ensure the GOsC will create, use, manage and destroy or preserve its records in accordance with relevant statutory requirements.

7. In particular, the records management system will ensure that GOsC staff and relevant non-executives know:

    - what records are held by the GOsC
    - where the GOsC records are held
    - that the records are stored securely and that only properly authorised persons can access them
    - how to access relevant records when needed
    - what version of the record they are working on
    - who created, last modified or amended, or disposed of a record
    - which records are related to each other
    - whether a record can be trusted
    - that records are only retained for the proper period of time

Responsibilities

8. All GOsC staff must ensure that records are created, captured, maintained, secured and disposed of in a way that complies with legal, administrative, cultural and business requirements.

9. All GOsC staff have a duty to protect records and to ensure that any information that they add to them is accurate, complete and necessary.

10. All GOsC staff have a duty to comply with all relevant policies, standard operating procedures and protocols.

11. The Chief Executive as Data Protection Officer has a duty to ensure that the GOsC complies with the requirements of legislation affecting management of the records and with supporting regulations and codes.

12. Information Asset Owners will be responsible for ensuring that records management operates within their directorate.

13. The Data Protection Officer will have oversight of requests to destroy or transfer GOsC records.

Principles underpinning and informing the policy

14. The following principles will underpin the GOsC's record management policy:
    - all information created by GOsC staff or members during the course of normal GOsC activity is the property of the GOsC
    - information must be managed to support business processes rather than in a hierarchical or organisational structure
    - records must not be retained, distributed or copies unnecessarily
    - a consistent approach should be adopted with regard to the creation, indexing, storage, retrieval, revision, archiving and disposal of records
    - the management of information must be in accordance with security, protection, legal, environmental and cost issues
    - Records deemed to be 'Restricted Data' will require appropriate additional security.

What Records are held by the GOsC and where such records are held

15. The GOsC's preference is to store records as electronic computer files, in so far as this is compliant with codes of practice regarding the evidential weight and legal admissibility of information stored electronically.

16. This ensures that:

    - **The record is present**: the GOsC has the information that is needed to form a reconstruction of activities or transactions that have taken place.
    - **The record can be accessed**: it is possible to locate and access the information and display it in a way consistent with initial use.
    - **The record can be interpreted**: it is possible to establish the context of the record – who created the document, during which business process and how the record is related to other records.
    - **The record 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.
    - **The record can be maintained through time**: the qualities of accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of formats.

17. The GOsC aims to keep the use of physical records to a minimum, and used principally for personal reference purposes.

18. The GOsC Information Asset Register will contain information relating to:

    - the types of record held,
    - the Information Asset Owners,
    - where the records are stored,
    - access rights and security measures for the records,
    - which records contains sensitive personal data, and
    - risks associated with the data in that record.

19. Electronic versions of all physical records should only be stored in designated areas of the hosted IT server and not on local PCs.

20. Records of decisions and contracts and/or committee minutes that require physical signatures should be scanned and stored in designated areas of the hosted IT server and not on local PCs.

21. Documents should be stored in designated areas of the hosted IT server and not on local PCs.

22. Staff must ensure that any restricted data is securely locked away at the end of each working day.

23. Some physical records may be transferred to a third-party organisation when review is triggered by enforcement of the GOsC retention and disposal schedule.

24. No records containing personal data should be destroyed or transferred without the express authorisation of the Data Protection Officer (DPO)

25. DPO approval should also be sought where bulk destruction of records is proposed, regardless of whether these contain personal data or not.

Access to restricted data

26. Access to restricted data, other than by the information asset owner and their team, is limited to those who require it in the course of their normal work. Access at any other time will require the consent of the relevant information asset owner.

27. Requests for extraordinary access will be logged by the information asset owner.

28. Authorised users of restricted data are:

Category of data	**Authorised users**
Patient records	Regulation and Professional Standards departments and associated non-executives
Information obtained during the investigation of complaints and fitness to practise cases	Regulation department and non-executives associated with GOsC statutory committees
Personal registrant information that does not form part of the statutory register	Registration department and Communication department for routine communications only
Financial records	Finance staff
information provided to the GOsC that may be commercially confidential	Professional Standards department and associated non-executives for RQ information, otherwise finance and legal staff only
HR records including information relating to both staff and non-executives.	HR and finance staff only

Review

29. This policy will be reviewed on an annual basis.

30. Ad hoc reviews will take place where relevant primary or secondary UK legislation is introduced, where codes of practice are updated, and where case law requires.

Version control

Document title	**Document author**	**Version**	**Date**	**Detail of amendments**
GOsC records management policy	Tim Walker	V2	25 May 2018	

General Osteopathic Council

Data Retention Policy

This policy covers information acquired and held by the GOsC for the following functions: Registration, Education and Quality Assurance, Fitness to Practise (FtP) and Protection of Title, and Corporate matters. It mainly relates to personal information held about individuals but includes other information such as Council papers and minutes.

The principles governing this policy are that the GOsC should acquire personal information only for a specified purpose or purposes, and only to the extent that it is needed for that purpose or purposes. Having acquired the data, it should be used only for the purpose or purposes for which it was acquired and held for no longer than is necessary.

The schedule below sets out the type of information held by the GOsC and the maximum period for records to be retained. At the end of those periods the information will be securely destroyed. We intend to apply this policy retrospectively to information we already hold.

Please note that our current approach to emails is that they are non-formal records until they are added to our online data storage system either as part of the GOsC's Integra database or otherwise part of our cloud-based storage system. Once added, they are subject to the retention categories above.

A. Registration

We hold personal information relating to initial applications for registration and the annual registration renewal process. For initial applications, this will include a completed application form, certificate of recognised qualification, character and health references, and a criminal records bureau check.

	Category	**Purpose for which information is needed/comments**	**Proposal for retention of data**
CURRENT REGISTRANTS			
1	Initial registration	Needed for administration throughout the individual's registration	As long as registration continues
2	Annual renewal, including CPD submissions	Includes financial information which the GOsC is required to keep for seven years	As long as registration continues
3	Criminal records bureau check	This information is only valid for six months from the date it is processed.	Six months

POTENTIAL REGISTRANTS			
4	Unsuccessful applications for registration	Information needed if the applicant reapplies or for 'protection of title'[1] purposes	Full record for 10 years after the last unsuccessful application. A summary record of applicant's name, date of birth and reasons for unsuccessful application to be kept permanently.
5	a) Incomplete applications b) Incomplete 'new powers'[2] applications	Registration is pending	a) Three years b) 30 years (because they cannot reapply under the 'new powers')
6	Students (who may have graduated but not registered)	Applies principally to students in their final year who start to provide information in anticipation of registering after qualifying (once such applicants are registered, this information will form part of their registration records).	Three years
7	Criminal records bureau check	This information is only valid for six months from the date it is processed.	Six months
FORMER REGISTRANTS			
8	Individuals removed from the Register for reasons not related to fitness to practise matters (e.g. resignation or removal for non-payment of fees, etc.)	Information needed if the individual applies for restoration and for protection of title purpose	Full record for 10 years after the removal. A summary record of registrant's name, registration number, date of birth, start and end dates of registration and reasons for ceasing registration to be kept permanently.

[1] The title 'osteopath' is protected by law. It is against the law for anyone to call themselves an osteopath unless they are registered with the GOsC.
[2] The 'new powers' are those introduced in 2009 in Section 3(6A) of the Osteopaths Act.

9	Retired registrants	To be kept for general administration after retirement. Skeleton record for provision of information to those needing to make contact with registrant	One year for complete registration records. Eight years for skeleton information on database: name, address, gender and period of registration
10	Deceased registrants	General administration after death. Skeleton information for provision of information to those needing to make contact with registrant's estate	One year for registration records. Eight years for skeleton information on database: name, address, gender and period of registration

B. Education and Quality Assurance

We acquire and retain information relating to the provision and quality assurance of osteopathic education. Information about osteopathic schools is generally not 'personal data' (i.e. does not relate to individuals).

	Category	Comments	Recommendation for retention of data
1	Data submitted by and relating to Osteopathic Educational Institutions (OEIs)	The length of a normal accreditation cycle is between three and five years. Seven years allows sufficient time for information from a previous cycle to be fed into a subsequent review.	Seven years
2	Student feedback and complaints	Feedback that may be relevant for accreditation of courses.	Seven years
3	Privy Council orders	It is important that we keep a record of when qualifications become 'recognised' so that we are aware of which qualifications entitle the applicant to apply for registration and which do not. This is information that	Permanently

		only we would hold.	
4	Recognised Qualification (RQ) reports	These reports become redundant once a new Recognised Qualification is put in place (typically every three to five years), but seven years allows a margin for general administration.	Seven years
5	Applications for unaccredited OEIs	Information obtained in this process may be relevant for future applications	Seven years

C. Fitness to practise (FtP) and 'protection of title'

In the area of fitness to practise particularly, we need to balance our duty to protect the public against statutory privacy requirements such as those imposed by the Data Protection Act and Article 8 of the Human Rights Act on the other. . This means that the fitness to practise committees need to have all relevant information when considering complaints against osteopaths, but the length of time for which information is retained should nevertheless be proportionate.

Cases can come to an end at different stages along the fitness to practise process. The information acquired and decisions reached at those different stages may become relevant if a registrant is the subject of a new complaint. The relevant legislation, particularly rules governing the functioning of the Investigating Committee (IC)[3], allows for this.

We have also included in the table below a provisions for information acquired during our 'protection of title' proceedings.

	Category	Comments	Recommendation for retention of data
Fitness to Practise			
1	A concern means any professional conduct communication containing information which is	Information gathered from concerns can prove to be important even if the complaint is not screened in.. This is because	Eight years

[3] Rules 4 and 24 of the General Osteopathic Council (Investigation of Complaints) (Procedure) Rules 1999. When a complaint is made and if we have jurisdiction to deal with it ('screened in') it is investigated and considered by the IC. If the IC finds there is a 'case to answer' the complaint is referred to the Professional Conduct Committee or the Health Committee. If there is no case to answer, the case is closed.

	capable of amounting to an 'allegation' or 'complaint' under the Act.	complainants who may be unwilling to make a formal complaint sometimes say that if others come forward with similar complaints they would be prepared to give witness statements or make their own complaints. Balanced against those reasons for keeping information about concerns for as long as possible, is the fact that memories fade, and so evidence from several years ago may become less valuable, putting into doubt the purpose for which the information is held. The registrant is unlikely to know of the existence of a concern. The recommendation made in relation to concerns seeks to find the right balance. NB there is no time bar on bringing a complaint.	
2	Formal complaint made but screened out under the threshold criteria	This relates to where a complaint has been screened out under the threshold criteria. However a number of complaints against a registrant within a short period of time may be indicative of other problems	Eight years
3	Formal complaint, screened in and considered by IC, but no case to answer found (with or without advice)	Similar arguments apply, though the reason for non referral by the IC may be the quality of evidence. Where a number of complaints have been received against the same registrant within a short time period this may indicate wider fitness to practise concerns. Advice issued to the	Eight years for the full record where case closed without advice. Ten years where case is closed with advice. Record of the IC summary paper and decision and the complainant and witnesses contact

		registrant is designed to ensure future compliance with the *Osteopathic Practice Standards*. Advice issued does not affect a Registrant's registration status and will not be recorded on the Register of Osteopaths as it is not a formal sanction nor would any restrictions be placed on the osteopath's registration. However, the fact that advice was issued will become part of the Registrant's fitness to practise history.	details to be retained permanently.
4	Allegations referred to Professional Conduct Committee (PCC) or Health Committee	Allegations heard by the PCC are in the public domain, while in health cases only the outcome is a matter of public record.	Anything in the public domain should be held permanently (e.g. transcripts in PCC cases, determinations) Unproved cases: underlying information to be held for ten years or up to age 18 where a child is involved. Proved cases: underlying information to be held until death of registrant.
5	Medical records belonging to patients	These are considered to be among the most sensitive types of data.	Patients will be offered the records at the conclusion of the case, which would be after any appeal period has ended; if they are not wanted, they should be destroyed immediately.
Protection of title			
6	'Protection of title' investigations	A cease and desist letter may stop the offending in the short term but we need to keep records to check for reoffending	10 years
7	'Protection of title'	Such prosecutions are a	Permanently

	prosecutions	matter of public record, but likely to be sufficient to keep all the documents associated with the court case (i.e. no need to keep drafts)	
	Appeals, including section 29 Appeals	Where a decision by a Conduct Committee is appealed by the Registrant or the Professional Standards Authority	Ten years from end of legal proceedings including the subsequent appeal.
	Where a decision to close a case is legally challenged i.e. by judicial review	This applies where a decision to close a case is made by a Screener or the Investigating Committee	Extend retention date to cover the duration of such proceedings including time limits for further appeal or renewal of proceedings

D. Corporate matters

Some of the records held in relation to the functioning of our organisation will contain personal data, but not all.

In relation to the documents described in categories 5 and 6 in the table below, we propose also that after the seven years (or whatever appropriate period is agreed) for which they are held by the GOsC, they are transferred to the National Osteopathic Archive; with the caveat that documents containing personal information should not be transferred but be destroyed at that point.

	Category	Comments	Recommendation for retention of data
Corporate matters			
1	Council and committee agendas, papers and minutes, including Annual Reports	Much of the information will be in the public domain. Unlikely to contain personal data and information should be kept for historical and current purposes	Permanently
2	Drafts of documents in 1 above		To be destroyed/ deleted following meeting for which they were prepared.
3	Non FtP complaints, responses and correspondence –	The DH has published guidelines on this	Six years

4	Correspondence with registrants	This is stored on the registrant's entry on the GOsC database	As long as registration records held
5	Other correspondence	For general administration purposes	Seven years
6	Corporate documents (where not maintained as part of Council papers)	Including for example responses to consultations	Seven years
7	Tenders and contracts	For general administration purposes and resolution of disputes	Successful tenders – seven years Unsuccessful tenders – one year after contract award
8	HR documents (executive)	For general administration purposes and provision of references	Unsuccessful applicants applications – six months Basic information for reference purposes – six years after leaving
9	HR documents (non-executive)		Unsuccessful applicants applications – two years Other information – for duration of appointment

Version control

Document title	**Document author**	**Version**	**Date**	**Detail of amendments**
GOsC data retention policy	Tim Walker	V2	25 May 2018	
	Tim Walker		7 January 2019	Amended to clarify storage of emails

General Osteopathic Council

Policy on Use of GOSC Communications systems, and Use of Internet and Social Networks while at Work

1. This policy applies to GOsC Staff, Members of the GOsC Council and non-executives. Any breach of this policy or serious abuse of the GOsC communications systems may be regarded as a serious disciplinary offence.

2. This policy respects and complies with the applicable laws including (but not limited to):

   - *Telecommunications Act 1984*
   - *Copyright, Designs and Patents Act 1988*
   - *Computer Misuse Act 1990*
   - *Data Protection Act 1998*
   - *Freedom of Information Act 2000*
   - *Human Rights Act 1998*
   - *Regulation of Investigator Powers Act 2000*
   - *Lawful Business Practice Regulations*
   - *Electronic Communications Act 2000*

3. The GOsC's communications and IT systems (including email and internet access) are primarily for business use. Occasional personal use is permitted provided that it does not interfere with effective performance of staff duties or GOsC business.

4. A distinction should be maintained between business and person emails by marking personal emails as 'personal'.

5. The GOsC's communications and IT systems (including email and internet access) should not be used for advertising, gambling, selling goods or services for personal gain.

6. The GOsC's communications and IT systems (including email and internet access) should not be used for sending or receiving, accessing or downloading content which may be deemed:
   - defamatory
   - offensive to persons with protected characteristics under the Equalities Act 2010
   - pornographic, indecent or illegal.

7. The GOsC's communications and IT systems (including email and internet) should not be used for
   - harassment or bullying
   - breaching copyright or confidentiality
   - downloading software which breaches the software company's rights or licence agreements

- intentional propagation of viruses
- disrupting or damaging other systems by carrying out acts of a malicious nature
- publishing material that brings the GOsC's reputation into disrepute.

8. In accordance with the Regulation of Investigatory Powers Act and the Lawful Business Practise Regulations, the GOsC reserves the right to monitor (and record) email, internet access and other material on its communication and IT systems from time to time for the purposes of:
   - ensuring compliance with GOSC policies
   - ensuring compliance with the GOsC's legal obligations
   - monitoring standards of service and employee performance
   - training purposes
   - preventing or detecting unauthorised use of GOsC communication systems
   - Identification, detection, quarantine and removal of malware
   - reporting of offensive emails
   - prevention and detection of crime, including terrorism
   - investigating abnormal system behaviour
   - resolving a user problem
   - maintaining or carrying out GOsC business.

9. Any monitoring or recording undertaken by the GOsC will be kept to a reasonable minimum and every care will be taken to comply with all applicable data protection and privacy legislation.

10. However, the Chief Executive may authorise more active monitoring or recording in writing, provided that he has reasonable grounds for doing so, and sets out his reasons.

11. If there is a need to access data held on the GOsC communication systems, the individual will normally be asked for his/her consent; however in certain circumstances it may exceptionally be necessary to obtain access without consent. These include:
    - where urgent access is critically required for operational purposes but the individual is absent and cannot be contacted
    - where there is prima facie evidence that an individual may be misusing facilities to an extent which would be considered serious or gross misconduct or if there is a need to initiate an investigation and there is a serious possibility that evidence might be destroyed.

12. Users should be aware that emails:
    - may have to be disclosed to individuals who make a subject access request under the Data Protection Act 1998
    - may be disclosable in legal proceedings
    - are not inherently a secure form of communication.

13. Emails must not be used to:

- send personal data or sensitive personal data about individuals outside the European Economic area
- send sensitive or confidential information (including material relating to complainants or osteopathic patients), unless that information has been anonymised, password protected or encrypted.

14. Users of the GOsC communications systems (including email and IT systems) must not disclose their personal log-on or access codes to any other user.

15. All emails initiated from the GOsC must contain the GOsC disclaimer.

16. In using any social networking site (such as Twitter and Facebook) or any other online forum or service, staff and non-executives must ensure that they do not:
    - bring the GOsC into disrepute
    - post information which is confidential to the GOsC
    - make comments or post remarks that could be considered to constitute bullying, harassment or unlawful discrimination against any individual.
    - use offensive or intimidating language
    - pursue personal relationships with GOsC stakeholders
    - post inappropriate comments about colleagues or GOsC stakeholders
    - do anything else that in any other way that is unlawful.

17. The requirements relating to social media etc. apply whether or not the individual accesses them via the GOsC communications system.

18. GOsC Staff and members should only access parts of the system for which they are authorised.

19. GOsC staff and members are not permitted to load any computer software onto the GOsC's equipment without authorisation from the Director of Registration and Resources. All software must be properly licensed and checked for viruses before loading.

Version control

Document title	**Document author**	**Version**	**Date**	**Detail of amendments**
GOsC policy in relation to use of GOsC email, and use of Internet and social networks at work	Tim Walker	V2	25 May 2018	

General Osteopathic Council

Policy on disposal of IT equipment and confidential waste

Policy Objectives and scope

1. This policy governs the disposal of any waste material that contains information that would constitute a breach of confidentiality if it became available to unauthorised persons (confidential waste).

2. This policy applies to information held in all formats, including paper, computer, video or audiotape, photographs, film fiche, disks and USB storage devices etc.
3. Therefore, the procedure for the disposal of confidential waste must ensure that:
   - confidential waste is kept secure and protected against accidental loss, damage or unauthorised access up until its final destruction
   - confidentiality is protected throughout the whole process up to and including the final disposal and destruction of the confidential waste.

Roles and responsibilities

4. The Director of Registration and Resources shall be responsible for ensuring that arrangements are in place for the secure storage and disposal of confidential waste.

5. All staff are responsible for ensuring that they identify any waste that may be confidential and ensure that it is disposed of using the facilities provided.

Procedures for destruction of confidential waste

6. Confidential waste must be kept secure and protected against accidental loss, damage or unauthorised access up until its final destruction.

7. The last person leaving a floor at the end of the working day should check the printer and place any documents left on the printer in confidential waste.

8. Confidential waste should be kept separate from other waste material and confidential waste bins used where possible, otherwise waste should be bagged and clearly labelled "confidential waste".

9. Bagged waste awaiting collection must be kept secure at all times.

10. Only authorised GOsC personnel or an approved contractor should handle the waste.

11. If destruction is to take place off site, the waste must be escorted and its destruction witnessed by an authorised member of staff unless the contractor is specialised in the secure destruction of confidential waste and will provide destruction certificates.

12. Where offsite disposal is to be undertaken the company concerned must have the necessary controls in place to prevent the information being mislaid.

13. Paper media intended for confidential disposal must be stored in secure, lockable containers prior to disposal. Containers must be clearly labelled 'Confidential Waste.' On no account should any confidential waste be placed in other types of waste receptacles e.g. those for normal recycling, wheeled bins, skips etc.

Provision for mobile working or staff and non-executives working at home

14. As a general principle, the GOsC will minimise the amount of confidential material sent to or carried by staff and non-executives outside the GOsC offices. Staff and non-executives are also discouraged from printing any confidential material away from the office.

15. Any member of staff or non-executive working from home or away from the GOsC offices must ensure that they have procedures in place to safeguard information effectively. This includes the safe disposal of any confidential waste. In such circumstances, this material should be brought back to the GOsC for secure disposal by shredding or placed in the secure confidential waste containers where available.

16. Confidential information, including that on computers, laptops, PDAs, mobile phones and other storage devices e.g. hard discs, floppy discs, tapes, CDs, DVDs, flash drives etc. must be securely erased prior to disposal.

17. Where appropriate the GOsC can make arrangements for them to be made available for re-use or provide secure means for them to be incinerated or crushed.

Disposal of GOsC IT equipment and associated waste

18. Disposal of surplus IT equipment must only be carried out by individuals authorised by the Director of Registration and Resources.

19. Hard drives and data storage devices must be purged and/or destroyed using where necessary authorised contractors who will provide a certificate of disposal on completion of the work.

20. Destruction of electronic records, storage devices and tape must be by incineration or the use of specialised equipment or software that will destroy the information.

21. Floppy disks and CDs can be cut up and disposed as general non-recyclable waste.

Version control

Appendix 5

Document title	Document author	Version	Date	Detail of amendments
GOsC disposal of IT equipment and confidential waste policy	Tim Walker	V2	25 May 2018	

General Osteopathic Council
Information Quality Assurance Policy

Policy objectives

1. This policy is intended to ensure that key data held by the GOsC and used in the preparation of reports, returns and submissions to stakeholders is of good quality and fit for purpose.

Approach to information quality

2. The GOsC adopts the six Audit Commission recommended data quality dimensions of:

   i. Accuracy

      - data should provide a clear representation of the activity/interaction
      - data should be in sufficient detail
      - data should be captured once only as close to the point of activity as possible

   ii. Validity

      - data should be recorded and used in accordance with agreed requirements, rules and definitions to ensure integrity and consistency

   iii. Reliability

      - data collection processes must be clearly defined and stable to ensure consistency over time, so that data accurately and reliably reflects any changes in performance

   iv. Timeliness

      - data should be collected and recorded as quickly as possible after the event or activity
      - data should remain available for the intended use within a reasonable or agreed time period

   v. Relevance

      - data should be relevant for the purposes for which it is used
      - data requirements should be clearly specified and regularly reviewed to reflect any change in needs
      - the amount of data collected should be proportionate to the value gained from it

   vi. Completeness

      - data should be complete

- data should not contain redundant records

3. Each information Asset Owner will measure and improve the completeness and validity of key data items on their system.

Version control

Document title	**Document author**	**Version**	**Date**	**Detail of amendments**
GOsC information quality assurance policy	Tim Walker	V2	25 May 2018	

General Osteopathic Council

Information Access Policy

1. This policy supports the legislative framework for responding to requests for information under the statutory access regimes established by the Data Protection Act 2018 ('DPA'), the Freedom of Information Act 2000 ('FOIA'), and, the Environmental Information Regulations 2004 ('EIR') and other legislation that provides a right of access to information.

Roles and responsibilities

2. The Director of Fitness to Practise is responsible for co-ordinating all information access requests made to the GOsC.

3. Compliance with this policy is compulsory for all staff employed by the GOsC.

4. Guidance on the Freedom of Information Act can be found on the ICO website at: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

General right of access to information

5. All recorded information, personal and non-personal, held by the GOsC in any format is subject to a statutory access regime under the DPA, the FOIA or EIR. However, access to the information may be subject to certain exemptions under the applicable legislation.

6. The GOsC will endeavour to respond substantive to a request for information within the following timescales:

DPA	FOIA	EIR
Without undue delay, and no longer than one month	As soon as practicable, and in any event, within 20 working days	As soon as practicable, and in any event, Within 20 working days; or Within 40 working days for complex cases

7. Where requests are unclear or too voluminous, the GOsC will contact the applicant in writing in order to help the applicant refine their request.

8. In cases where exemptions under a statutory regime apply and either a request for information has been refused or information has been edited prior to release, the GOsC will explain its decision in writing to the applicant.

9. The GOsC will operate a single complaints procedure in relation to requests for information under DPA, FOIA and EIR.

10. The GOsC will keep a centralised record of all DPA, FOIA and EIR requests and responses. This does not include requests for information publicly available (i.e. readily accessible by other means).

11. The GOsC may publish a summary on its website of a selection of responses that it has issued to requests for information under the FOIA.

12. The GOsC will report periodically on its performance in responding to requests for information.

DPA and Personal Information

13. The DPA aims to secure the right of individuals to privacy by protecting information that is held about them. Individuals have the right to submit a subject access request ('SAR') to data controllers, asking for a description of the personal data held about them and to receive a copy of that information.

14. Requests for access to recorded personal information by the individuals to whom the information relates will be processed by the GOsC as SARs in accordance with the requirements of the GDPR (and DPA).

15. A SAR must be dealt with without delay and no longer than one month after receipt of the request. If the complexity or number of requests received means that additional time is needed or further information then an extension of up to two months may be applied. If an extension is applied, the individual will be informed of this within a month of receipt of the request and reasons will be provided for the delay.

16. Requests may be made informally and may be either verbal, via social media channels or in writing. A request may not make any reference to the GDPR or explicitly identify itself as a SAR. If a SAR is made electronically the information will be provided in electronic format, unless otherwise requested.

17. Once a request is received, if the applicant has not already provided suitable proof of identity, he or she will be asked to provide this.

18. Applicants should not be asked to explain the purpose of their request. However, where we process a large quantity of information about an individual, we may ask the applicant to specify the information the request relates to and so it may be necessary to seek further information from them.

19. The GOsC may refuse to respond to the request where it is unfounded and excessive. Reasons for the refusal must be given to the individual. The individual will also need to be informed of their right to complain to the relevant supervisory authority, the ICO and of their right to a judicial remedy.

20. Both the reasons for refusal and advising of the right to complain will be provided to the individual without undue delay and at the latest within one month of the request.

FOI Requests

21. The Freedom of Information Act 2000 (FOIA) gives the public the right to access information held by public authorities. The Act is intended to improve openness and accountability in the public sector. There is also an underlying intention to improve the quality of information and records held by public authorities.

22. The full text of the FOIA can be found on the Office of Public Sector Information website.

23. The full identity and postal address of the individual or organisation is not relevant under the FOIA regime.

24. However, requests must provide sufficient information for the GOsC to be able to respond to the request.

25. The person who is making a request for information and the reasons why they want that information are not relevant. Applicants must not be asked to explain the purpose of their request, although in the course of clarifying requests and ascertaining exactly what information is being sought it may be necessary to seek further information from the applicant. While clarification is awaited from the applicant the elapsed time for responding to the request is suspended. Once sufficient clarification is received to enable the GOsC to respond, the elapsed time will again begin to count.

26. A request by an individual for information about themselves and requests for environmental information are exempt under the FOIA and will be handled under the DPA and EIR respectively.

27. Information requests may be received in foreign languages or in Braille. The duty to assist may apply in the case of translation, although it would not be unreasonable to ask the applicant to reframe their request in English to avoid unnecessary charges. However, the provision of services to the disabled would fall under the jurisdiction of the Equality Act 2010. Where relevant, the rights of the individual under the Human Rights Act 1998 (HRA) must also be taken into consideration.

28. A request for information about another living individual will be handled under the FOIA, but certain data protection considerations will apply. The GOsC will not provide the information if the disclosure would breach the data protection principles.

29. If the GOsC decides that it will disclose the information, it should notify the third party about whom information will be disclosed.

30. The GOsC will not automatically presume a duty of confidence (absolute exemption) and will, where necessary or appropriate, consult with and seek the views of third parties with regard to the disclosure of requested information. However, the decision as to whether or not to disclose the requested information is a decision for the GOsC.

31. The GOsC has no obligation to provide information if the information sought does not exist in a recorded format and/or is information that is intended for future publication.

32. The GOsC will not generate new, recorded information that it does not currently hold in order to meet a request for information.

33. The GOsC will, however, endeavour to advise the applicant of recorded information that it does hold that is relevant to the request and that goes some way towards meeting it. It will also advise if the requested information is likely to be published in the future and, where possible, when it will be published and how it may be accessed.

34. The GOsC produces a Publication Scheme which can be found at: https://www.osteopathy.org.uk/news-and-resources/publications/publication-scheme/

35. The Publication Scheme sets out the range and type of information the GOsC will routinely publish.

36. Requests for information which fall into any of the classes of information listed in the Publication Scheme will, in most cases, be refused on the basis that the information has already been pro-actively published by the GOsC (i.e. the information is publicly available and therefore 'readily accessible by other means'). Applicants should be referred to the website or other source where the information can be found.

37. Correspondence with an FOI applicant, either delivering requested information or declining an application owing to the enforcement of an exemption or the identification of a vexatious request (see below), must be accompanied by details of the complaints procedures operated by the GOsC and the Information Commissioner.

38. Where information is available in hard copy only, it is acceptable to contact an applicant who has only provided an email address to request details of a street or P.O. Box address to which the information can be mailed.

Requests made under the EIR

39. EIR give rights of access to environmental information, including information relating to health and safety issues and policies.

40. An EIR request does not have to be in writing and can be made orally.

41. The GOsC has to respond to the request within 20 working days (40 working days in the case of complicated requests)

42. A reasonable charge can be made for the information. Exemptions exist in relation to some information (see below).

43. EIR requests are exempt from the FOIA but, as with the DPA, public authorities will have a duty to identify the nature of an information request and respond accordingly.

44. EIR overrides any other enactment or rule of law that would prevent disclosure of information in accordance with the Regulations. Guidance on the GOsC's duties under the EIR can be found in the Code of Practice: http://www.ico.gov.uk/upload/documents/library/environmental_info_reg/detailed_specialist_guides/environmental_information_regulations_code_of_practice.pdfn

Fees and charges

45. Information published under the GOsC's Publication Scheme will, wherever possible, be provided free of charge.

46. To avoid unfair treatment and social exclusion, those applicants that do not have access to electronic facilities will be provided with a paper copy of the information free of charge provided it is readily available from the website or does not fall into the categories identified below.

47. A reasonable charge may be made for expenditure incurred such as photocopying, postage and packaging, providing CDs or DVDs, and the costs associated with viewings made in person.

48. Photocopying of black and white A4 copies may be charged at a rate of 10p per page; any other expenses will be charged at cost. All costs will be made known to the applicant before any information is provided.

49. The GOsC will always take into consideration its obligations under the Equalities Act 2010 when considering any request to produce information in other formats.

Costs under the FOIA

50. In line with the Freedom of Information Fees Regulations, the GOsC will not charge for FOI requests for which the total cost of collating, assessing and releasing information is less than £450.

51. All work by GOsC personnel is charged at a rate of £25 per hour per person.

52. Where the total cost of processing an FOI request exceeds £450, the GOsC may either refuse the request, communicate to the applicant that information which can be found within the cost threshold or, in exceptional circumstances, offer the applicant the choice of paying for the processing of their request in full.

53. Information applicants are required to cover in full the cost of having information communicated to them in their preferred format. This includes the cost of postage, photocopying, printing and media such as CD-ROM.

54. The Regulations distinguish between prescribed costs (the cost to the GOsC of processing an FOI request: determining whether the GOsC holds the information requested; finding and retrieving that information) and disbursements (the cost of informing the applicant whether the GOsC holds the information requested; giving effect to the applicant's format preference for delivering the information; delivering information to the applicant).

55. No charge can be made for applying exemptions and assessing the public Interest test.

Costs under the DPA

56. Requests for the provision of personal information that are made under Section 45 of the Data Protection Act 2018 are free of charge unless the request is considered manifestly unfounded or excessive.

Exemptions and refusal of requests

57. A number of exemptions relating to the disclosure of information are identified in the FOIA. These fall into two categories: Qualified Exemptions, where it is necessary to determine whether the public interest would be best served by the disclosure or withholding of information, and Absolute Exemptions, where the public interest test does not apply.

58. Further guidance on the exemptions can be found on the web sites of the Information Commissioner and the Department for Constitutional Affairs.

59. The GOsC will provide written notice to applicants where a request has been refused in its entirety, or where a part of the request is refused.

60. Such notices will provide details of any exemptions that have been applied and, where the public interest test has been applied under the FOIA resulting in the non-disclosure of information, the reasons for the decision not to disclose.

61. The GOsC is not obliged to confirm or deny the existence of information, or to advise in respect of exemptions applied where to do so would in itself disclose exempt information.

Repeat requests

62. The GOsC is not obliged to comply with repeat requests for information, under the FOIA.

63. In reaching a decision about whether a request for information should be treated as a repeat request the GOsC shall have regard to, among other things:
    - the time that has elapsed since the previous request;
    - whether the request is identical or substantially similar to the previous request;
    - whether any relevant, new information has been generated since the previous request.

64. Where there are valid grounds to refuse to respond to a repeat request, the GOsC may refuse any similar requests made within a period of 60 consecutive days.

65. Where the GOsC receives two or more requests from one person, or different persons who appear to be acting in concert, for the same or similar information and these requests are received within 60 working days of a previous request, the GOsC will aggregate the costs of responding to such requests.

Vexatious requests

66. The GOsC is not obliged to comply with vexatious requests under the FOIA.

67. In determining whether a request should be refused because it is vexatious the GOsC will consider all the circumstances of the request, including among other things:
    - the history of requests submitted by an applicant;
    - the number and frequency of repeat requests submitted by an applicant;
    - whether an applicant is habitually and persistently submitting requests where there appears to be no reasonable grounds for them to do so and where there is a strong likelihood that such requests are being made with the intention to harass, unreasonably and unnecessarily divert resources, or to otherwise disrupt the functioning of the GOsC.

68. In instances where a request is regarded as vexatious, the GOsC will provide the applicant with a written notice stating why the request is deemed to be vexatious.

Complaints

69. Complaints received in respect of the processing of FOI, DPA and EIR requests will be centrally co-ordinated and treated as a request for internal review under the FOIA.

70. Complaints should be directed in the first instance in writing to the Chief Executive.

71. Complaints will be acknowledged in writing within 5 working days.

72. The GOsC will endeavour to respond substantively to all complaints within 20 working days.

73. The GOsC will operate a single tier internal review process.

74. Internal reviews will be dealt with by the Chief Executive. Where the Chief Executive has had involvement in the processing of the request or, if it is considered that he may have a conflict of interest, the complaint should be referred to the Chair of Council.

75. Once the GOsC complaints process has been exhausted, and the complainant is not happy with the result, he or she may refer the matter to the Information Commissioner's Office (ICO):

    First Contact Team
    Information Commissioner
    Wycliffe House
    Water Lane
    Wilmslow
    Cheshire SK9 5AF

    Full contact details are available on the ICO web site. Or by calling 0303 123 1113.

76. Relevant records relating to a complaint regarding the handling of an FOI request should not be destroyed, even if scheduled for disposal, until the time allocated to appeal a decision from the Information Tribunal has expired. The destruction of records subject to an information request is a criminal offence.

Review of this policy

77. This policy will be reviewed on an annual basis.

78. Ad hoc reviews will take place where relevant primary or secondary UK legislation is introduced, where Codes of Practice are updated, and where case law requires.

Copyright

79. Recipients of information gained as a result of FOI requests should note that the GOsC maintains copyright control of all publications produced by the organisation.

Version control

Document title	**Document author**	**Version**	**Date**	**Detail of amendments**
GOsC information access policy	Tim Walker	V2	25 May 2018	

General Osteopathic Council

Information Governance Framework

Protocol for Handling Patient Records within the Registration and Resources Department

Introduction

Patient records are received at two stages of the registration assessment process;

a) for the written assessment stage known as the Further evidence of practice questionnaire (FEP); and

b) the practical assessment known as the Assessment of clinical performance (ACP).

Patient records may contain sensitive personal data about individuals. The purpose of this protocol is to minimise the risk of inadvertently placing sensitive personal data in the public domain.

Further evidence of practice questionnaire

At this stage of assessment, the applicant submits a completed questionnaire which contains answers to questions regarding clinical cases. Patient records and detailed information about specific cases are submitted with the questionnaire.

Before any documents are sent to the GOsC, the applicant must be asked to ensure that all documents to be submitted do they do not contain any identifying information about the patients.

The applicant must also be asked to ensure that he has obtained consent from his or her patients to send any documentation to us.

Sometimes, however, we receive documents that have not been anonymised, or have been partly anonymised and some information has been left in error.

- The questionnaire must therefore be checked thoroughly as there are various parts that could contain personal information, including:

  a. references to patients within the text of the questionnaire
  b. accompanying patient records
  c. other accompanying evidence (i.e. referral letters).

- You must remove any details that identify a patient. These include, but are not limited to, the patient's name and contact details (phone number, address, email etc.). Use the redaction tape to cover these details. The date of birth does not need to be redacted.

- You must also remove the name, contact details and signature of any other healthcare practitioners. This does not include the practitioner's title or role.

- If you are unsure about whether a particular piece of information must be redacted, check with your manager.

- A copy of the redacted questionnaire and accompanying evidence must be checked by another member of staff to ensure it is fully anonymised. The redacted copy is then scanned and saved to the system before being sent to the assessors.

- Copies of the redacted version of the records must only be sent outside the GOsC premises by special delivery or as a password protected attachment (if sent electronically).

- The documents are stored securely and must be destroyed 28 days after any appeal period on a registration decision **or** 28 days after registration following a period of adaptation.

- A note must be placed on the file, confirming that the records have been destroyed.

Assessment of clinical performance

During the ACP, the applicant will treat patients and write patient records. These patient records contain information about patients which should not leave the clinic premises. When the applicant has finished writing up the patient notes, these must be redacted so that the copy taken back to the GOsC contains no personal information identifying the patient.

- Use the redaction tape to cover any identifying details about the patient. the patient's name and contact details must covered. These include, but are not limited to, the patient's name and contact details (phone number, address, email etc.). The date of birth does not need to be redacted.

- Once redacted, the notes must be photocopied twice and checked to ensure that no information regarding the patient's name or contact details can be seen. One redacted copy is given to the applicant for their records.

- A template front sheet must be attached to the redacted records, which confirms the number of pages in the records and the date on which the records were created.

- The applicant must sign the template to confirm that the attached records are a true copy of the records created by him on the specified date..

- The original patient notes are owned by the clinic where the assessment took place, these should be passed to the clinic manager after the moderation meeting with the assessors.

- Only the redacted copy is to be brought back to the GOsC office. This copy must be stored securely.

- Copies of the redacted version of the records must only be sent outside the GOsC premises by special delivery or as a password protected attachment (if sent electronically).

- The GOsC redacted copy must be destroyed 28 days after any appeal period on a registration decision **or** where a period of adaptation has been recommended, 28 days after registration following a period of adaptation.

- A note must be placed on the file confirming that the records have been destroyed.

Version control

Document title	**Document author**	**Version**	**Date**	**Detail of amendments**
GOsC Protocol for Handling Patient Records Within the Professional Standards Department	Meera Burgess	V1	30/5/2014	

General Osteopathic Council

Information Governance Framework

Protocol for Handling Patient Records within the Regulation Department

Introduction

As part of our Fitness to Practise Process, we process personal data (under Article 6) and sensitive data which the GDPR terms as Special Categories (under article 9). Examples include the osteopathic treatment records of a complainant; or the medical records of the complainant or registrant may be required. Such records may form part of the evidence in a case, and may need to be considered by the GOsC caseworkers and the registrant; lawyers representing the GOsC and the registrant; experts; legal and medical assessors, and panel members of the GOsC Fitness to Practise Committees. Anyone who receives information from us is also under a legal duty to keep it confidential.

Any organisation that collects, analyses, publishes or disseminates confidential health and care information must follow the Code of practice on confidential information.

The purpose of this protocol is to minimise the risk of sensitive personal data contained in such records being inadvertently made public.

Protocol

1. Before any osteopathic treatment or medical records are requested, written consent from the patient must first be obtained, using the standard template form.

2. The original signed consent form must be scanned into the electronic case file and the original paper copy placed on the paper file.

3. A copy of the signed consent form must be enclosed with the letter to the practice seeking disclosure of the treatment or medical records.

4. Upon receipt, treatment or medical records must be held in the secure locked cabinets in the locked archive room awaiting redaction.

5. The treatment or medical records must be given a unique identifier linking them to the case (this may be the GOsC case number), and then the name and address of the patient should be redacted.

6. Where other information in the records may otherwise identify the patient, this should be redacted also.

7. However, dates of birth and any clinic identifiers (such as NHS patient numbers) should not generally be redacted. This is so that the parties who need to use the records during the proceedings can be sure that the records that they are

looking at, relate to the complainant bringing the allegation or the registrant whose health is at issue in fitness to practise proceedings.

8. Advice from the Director of Fitness to Practise should be sought if further redactions are considered necessary.

9. The redacted records should be checked by a co-worker to ensure that all identifiable information has been properly redacted.

10. The redacted records should then be scanned into the electronic case file and a hard copy placed on the paper file.

11. The original un-redacted records should not be scanned into the electronic case file.

12. The original un-redacted records should be locked in the archive cupboard until the conclusion of the hearing or appeal.

13. The following persons are only be provided with copies of the redacted version of the records:
    - Screener
    - IC members
    - legal and medical assessors
    - GOsC experts
    - GOsC lawyers
    - Registrant and registrant assessors.

14. Copies of the redacted version of the records must only be sent outside the GOsC premises by uploading to a secure on line portal, special delivery or as a password protected attachment (or encrypted USB stick)).

15. Only the redacted version of the records should be included in the IC Bundle and the PCC Bundle.

16. If a registrant or his representative wishes to view the original un-redacted records, arrangements should be made for the records to be viewed on the GOsC premises.

17. The original un-redacted records should also be available for viewing at the hearing on GOsC premises.

18. The original un-redacted records should not be sent out of the GOsC premises without the explicit approval of the Director of Fitness to Practise (Caldicott Guardian).

19. Where a hearing is to take place outside the GOsC, and it is necessary for the original un-redacted records to be present at that hearing, special arrangements

for the transport of the un-redacted records must be made, and approved by the Director of Fitness to Practise.

20. At the expiry of the appeal period (28 days after the hearing) or the conclusion of any appeal:

    a. the original un-redacted version of the osteopathic treatment records should be returned to the registrant by special delivery;

    b. the original un-redacted version of the medical records should either be sent to the patient by special delivery or placed in the locked confidential waste bin.

21. A note must be placed on the electronic and hard copy case files, confirming that the original un-redacted records have been returned or placed in confidential waste, and the date on which such action was taken.

Version control

Document title	**Document author**	**Version**	**Date**	**Detail of amendments**
GOsC Protocol for Handling Patient Records Within the Regulation Department		V2	25/05/2018	Updated to take account of the Records Management Code of Practice for Health and Social Care 2016 and GDPR