Re Data Processing Code of Conduct for Occupational Health and Wellbeing Services – draft for comment

Contents

1. **Introduction** 3
2. **Purpose of processing occupational health data** 3
3. **Application of the Code of Conduct** 5
4. **Fair Processing** 5
5. **Definitions** 6
6. **Roles and Responsibilities** 7
7. **Purpose for processing occupational health data** 8
8. **Consent** 10
9. **Legal Basis for Sharing Data** 13
10. **Data Security** 14
11. **Retention Periods** 17
12 **Transfer of Data** 17
13 **Data Destruction** 19
14 **Data Breach Notification Procedures** 20
15 **Subject Access Requests** 21
16 **Compliance and Monitoring** 23
17 **Monitoring Body** 24

Appendix One – Definitions 26

1. Introduction

1.1. This Code of Conduct is provided by the Society of Occupational Medicine who has appointed and has been approved as a trade sector Code of Conduct by the Information Commissioners Office (ICO) for the provision of occupational health and wellbeing services in the United Kingdom.

1.2. The Code of Conduct is recommended to be used by:

- Commercial occupational health providers who work as an organisation
- Independent sole practitioners providing occupational health services to commercial occupational health providers and their clients.
- In house occupational health services where the clinical and organisational resources are directly employed. (Elements of the Joint Data Controller may not apply to in house operators).
- Buyers (employers) who purchase occupational health and wellbeing services for the management of their employees in the UK.

1.3. The Code of Conduct is recommended to be used by commercial occupational health providers who work as an organisation or as sole practitioners providing occupational health services to clients. The Code of Conduct may also be used by in house occupational health services where clinicians are employed in the same organisation as the employees receiving the services. Elements of the Joint Data Controller may not apply to in house operators.

1.4. The Code of Conduct provides guidance and minimum standards of processing personal and special data in the provision of occupational health services. It places the data security of every Data Subject who engages with occupational health as the first priority and that the occupational health service is transparent in its dealings and processing of data and remains accountable for their actions and controls. The Code of Conduct recognises the unique needs and demands of processing data for the provision of occupational health services and provides service providers, employers, employees and other stakeholders with guidance and minimum standards expected of an occupational health services provider.

1.5. The Code of Conduct is version controlled and will be subject to updates from time to time.

2. Purpose of processing occupational health data

2.1. Occupational health services are the provision of advice, reports and assessments by the occupational health service (OHS) to its Client Data Subject's employer or prospective employer. The primary responsibility of the occupational health service is to provide advice on the impact of work on health and the capability of the health of the Data Subject and their ability to work. In the context of occupational health services, the clinicians providing the advice are not the Data Subject's healthcare provider, they are using their medical knowledge and skill to provide advice to employers.

2.2. This Code of Conduct ensures that all data processing complies with the Data Protection Act (2018) and any recommendations made by the UK regulator the ICO in the best practice and safest practice of managing personal and special data and minimising any risk of harm or loss arising from the processing of data within occupational health services.

2.3. Data is processed by an employer who requires occupational health services to be provided by qualified and authorised healthcare professionals. In order to protect the health and wellbeing of the Data Subject and to allow the Client to organise and meet its legal and morale requirements, it engages an OHS to provide:

2.3.1. Professional management advice
2.3.2. Carry out health assessments and monitoring
2.3.3. Deliver treatments to Data Subjects for the purposes of keeping the Data Subject fit for their contracted duties.

2.4. Clinicians' owe a duty of confidentiality to every Data Subject that they process data for, the obligation is personal and organisational and the Code of Conduct supports and compliments this duty. The Code of Conduct accepts that it professionally and clinically appropriate for clinicians to discuss specific cases that may extend to clinical information with colleagues within the occupational health service. This disclosure may be written or verbal and it is the responsibility of the disclosing clinician only to disclose information on a "need to know basis" and that they are responsible for the method of any communication and the storage of any data that is being processed.

Clinical and professional discussions involving personal and special (health) data should be managed carefully. They are necessary for the best and most appropriate advice to the employer. The Occupational Health Service should ensure that it has put in placed adequate training for its staff on how and when to have these discussions.
Example
Sending an email to a professional colleague maybe high risk if the email contains personal identifying and special health data. The risk is not the transmission of the email but the ongoing processing of the email as it sits in the Sender's outbox and sits in the Receivers in box presenting risks around data storage and management.

2.5. An OHS or it employees should not process personal or special data for any other reason other than for the provision of occupational health and wellbeing services. Data should not be shared with any other party other than the employer without the prior informed consent of the Data Subject.

2.6. Where an OHS uses a Third Party (subcontractor) to provide some of its clinical services (Occupational Medicine, Physiotherapy, Counselling Clinical Assessments), the OHS will have in place:

2.6.1. A documented Agreement with the Third Party that they act as a Data Processor and the OHS is the Data Controller.
2.6.2. That the OHS has carried out an appropriate assessment of the Third Party that they can comply and work to the same levels and standards of data processing and security that the OHS operates within.
2.6.3. That the Third Party has appropriate data protection policies in place and can evidence these for its processing of data security, management and storage of data, technical measures, training of its employees and their third parties and that the Third Party can evidence its compliance through auditing, training and assessment.

It would not be acceptable for an OHS to achieve accreditation and compliance with the Code and then to use a supply chain of Third Parties that do not operate to the same standards. The Code has the objective of raising standards by everyone who processes data and an approved OHS should ensure their supply chain can work within their OHS processes or they meet this Code standards. The OHS should check its supply chain for compliance through audit and encouragement. Within the first 2 years of the Code being approved the goal

would be that all Third Parties who process special data for an accredited OHS should also be accredited to this Code of Conduct.

2.7. Accreditation to this Code of Conduct is voluntary however an OHS that signs up and promotes the Code of Conduct demonstrates to its clients and to the public that it takes data protection seriously and aims to deliver the highest levels of service and best practice.

2.8. A Buyer of Occupational Health services (Employers) must ensure that their supplier have effective data security management processes and capabilities in place. Large employers who are accredited to the Code of Conduct demonstrate their commitment to the importance of processing data for the purpose of occupational health and should select an OHS that can demonstrate that it is accredited to these standards.

3. Application of the Code of Conduct

3.1 The Code of Conduct provides direction and guidance to ensure that data processed for the purposes of occupational health is processed in accordance with UK Legislation and that an OHS can demonstrate their commitment and compliance to complying with privacy and confidentiality.

3.2 The Code of Conduct should be used when drafting Agreements or agreeing ways of working with clients, the Code of Conduct provides the minimum standards of processing and practice that an OHS should commit to with its clients.

An OHS should be alert that it does not compromise its data processing standards and obligations when reaching service Agreements with new clients. Pressure from clients can arise due to their inability to meet the data processing requirements and due to the clients' lack of knowledge and awareness of the unique requirements in processing data for the purposes of occupational medicine.

3.3 The Code of Conduct provides standards and ways of processing that should be communicated to Data Subjects and an OHS should promote that it complies with the Code of Conduct in all of its data processing.

It is appropriate to reference the Code of Conduct and use parts of the code in the OHS Privacy Policy or other policies and public communications making Data Subjects aware of the standards that the OHS complies with.

4. Fair Processing

4.1 An OHS should have a written Agreement with each client setting out the terms and responsibilities that the OHS and the client agree to as part of the service delivery. An OHS and or the client may take specialist legal advice in the drafting of an Agreement the following terms should be referenced.

4.1.1 Purpose for processing data.
4.1.2 Fair processing.
4.1.3 Roles and responsibilities.
4.1.4 Definitions.
4.1.5 Legal basis for sharing data.
4.1.6 Data security and technical measures.
4.1.7 Data retention periods.
4.1.8 Data Transfer into the OHS (Beginning of Contract).
4.1.9 Data transfer from the OHS (End of Contract).
4.1.10 Data Destruction.
4.1.11 Subject Access Requests.
4.1.12 Data Breach notification procedure.
4.1.13 Compliance and monitoring of data processing activities.

4.1.14 Key Contacts for Data Processing purposes.

4.2 An OHS should have documented and public Privacy Policy or policies that explains to Data Subject's:

4.2.1 The identity of the OHS and contact details including ICO registration details if applicable.
4.2.2 Explains the purpose why the OHS processes the data.
4.2.3 Explains what the OHS does with the data that it holds and the services it provides to its clients
4.2.4 Explains how data is processed and where data is stored.
4.2.5 Explains if the data is shared with in any other party who that party is and why the data is shared.
4.2.6 Explains the duty of confidentiality and consent that the OHS undertakes.
4.2.7 Explains the Data Subject's rights.
4.2.8 Explains how a Data Subject can make a complaint and how the OHS will manage complaints with service response times.
4.2.9 Explains how a Data Subject can make a Subject Access Request.
4.2.10 Explains data retention periods and data transfer process.

It is important that the public policies are easy to understand and present the OHS as being open and transparent whilst remaining accountable for the data processing. A well-presented Privacy Policy will give stakeholders confidence in the OHS and can often answer many questions that stakeholders want without incurring the time and resources of the OHS. The Policy should be reviewed on a regular basis and the review time should be stated in the policy. No time period is being recommended by the Code of Conduct except that any review longer than 2 years from publication is likely to be too long and insufficient to meet the OHS monitoring and compliance obligations.

4.3 It is essential that data is only processed for the purposes that it was obtained by an OHS. The OHS must demonstrate that it has appropriate training and communication plans in place to make sure that its employees are aware and comply with this requirement. An OHS may hold significant amounts of personal data including names, addresses date of birth, telephone numbers, email addresses. This personal data must not be used for any other purpose.

The OHS holds special data specifically clinical records this data can include the most personal; and sensitive information about a Data Subject. The OHS must demonstrate to all stakeholders that it can be trusted and that they will only allow access to this data and allow the data to be processed for the purposes it was gathered. The OHS must ensure that it has appropriate security measures that allows authorised Users to be able to access special data. The OHS must ensure that it has appropriate and regular training programmes for all new employees and sub-contractors and can demonstrate that all of its employees have been trained and received refresher training at least annually on the importance of data processing and data security.

4.4 The OHS must have a published Complaints procedure that can be accessed by all stakeholders of the OHS. The complaints procedure should provide an explanation why the OHS processes data and provide 2 levels of dealing with complaints:

4.4.1 Internal procedure where the OHS will respond to and manage any complaints.
4.4.2 External procedure directing the complainer to the Information Commissioners Office where the OHS has been unable to resolve the complaint or the complaint is a breach of the data protection regulations.

5. Definitions

5.1 For the purposes of this specific agreement "Information" shall mean:

a) **Personal data**, to include any person identifiable data such as name, home address postcode, date of birth, gender, title, contact telephone numbers and email addresses, job tittle employer or any other personal data that is held.

b) **Special data** all and any medical forms, clinical notes, appointment details, tests examinations, x-rays, photographs, clinician's names, medical reports or any other person identifiable data held or transferred between the Parties. The examples are not exclusive and may be added too.

5.2 Additionally, there is a supplementary definitions table at Appendix One which defines some of the common terms which may be included in this document.

6. Roles and Responsibilities

6.1 Where the OHS is a commercial and external organisation from its client the relationship between the parties for processing the data will be joint and separate Data Controllers. Each party is responsible for the data that that they process and should have their own measures for ensuring compliance with the UK data protection regulations.

6.2 The client must remain a Data Controller as they require the right to appoint and remove OHS. The Client also provides some of the data such as personal data to the OHS and they have a duty to ensure that this data is accurate and not excessive. The client also has a duty to ensure that any OHS they appoint has the appropriate data protection capabilities and they have satisfied themselves that the OHS has and takes action to process the data.

Occupational health records contain clinical data that is both special and private. These records may have been gathered by healthcare professionals to be used by healthcare professionals for the purposes of occupational medicine therefore the client usually will not have the right to process the data without the specific consent from a Data Subject. Once the services has commenced the OHS will process the data making decisions, gathering more health data and carrying out assessments that the client has no knowledge of or control of. This level of processing is beyond the scope of a Data Processor and the OHS owes a greater duty of care to the Data Subject whose data it processes. Therefore the OHS is a separate Data Controller.

6.3 The OHS who has the main responsibility for the delivery of the occupational health services and who employs the healthcare professional who has ultimate responsibility for the health records must also be a separate Data Controller (Tier 2) They have the same duties to process and protect the data and owe any relevant Data Subject the same duty of care as a Data Controller.

6.4 An OHS who acts as a Data Controller should be registered with eth Information Commissioners Office.

6.5 Any Third Party (Sub-contractor) to the OHS either an organisation or an independent contractor who provides clinical assessment or therapy services is a Data Processor on behalf of the OHS. The OHS should ensure that a written Agreement is in place with each of its Data Processors for how data will be processed and stored. The OHS has a responsibility for their Data Processors and care is necessary to ensure that the

Data Processor is under the control of the OHS and the OHS knows and can decide how data is processed by any Data Processor.

6.6 Occupational Health services are increasingly expanding where an OHS can provide more than advisory and assessment services the table below sets out the definitions and differences in the role that an OHS may operate under:

Service Type	OHS Service Role	Data Transfer at Termination
Occupational Health Advisory Services including management referrals and medical assessments	Data Controller (Tier 2)	Yes
First Day Absence Reporting	Data Controller (Tier 2)	Yes
Physiotherapy treatment services only	Data Controller (Tier1)	No
Counselling treatment services only	Data Controller (Tier1)	No
Employee Assistance Programme	Data Controller (Tier1)	No
Drug & Alcohol Screening Services	Data Processor	Yes

An OHS should take care where it is acting as a reseller of services that are provided solely by a sub-contractor but the OHS invoices its client. In this case the OHS is an agent of the sub-contractor who is required to act as the Data Processor or Data Controller. Acting as a reseller can be problematic as it can be misleading and unclear to the Data Subject who actually has their data and who owes them the duty of care for privacy.

6.7 The Client is a Data Controller as they own the proprietary rights in the data, as they are the employer of the Data Subject they require the data in order for the legal compliance (Health & Safety Regulations (1998) and their obligations under the Equality Act (2010)), they also require the records for the effective management of work on health and health on work. For this reason the Client requires the right to appoint is OHS and to give the instruction that the data be transferred from one OHS to any new OHS.

The OHS is a separate Data Controller due to the manner and extent that it determines how the data is processed. The OHS also has the right to access the data which the Client does not have without the specific consent of the Data Subject. Given the extent that the OHS can process personal and special data it owes the Data Subject a greater duty of care than a Data Processor.

6.8 An OHS who is acting as a Data Controller may need to appoint a Data Protection Officer if it processes data on a large scale and has an obligation to notify the ICO of the DPO name and contact details.

7. Purpose for processing occupational health data

7.1 The purpose of the OHS in processing any Data Subject's personal or special data is for the delivery of services that protect, restore and maintain the employees' health it is necessary to exchange maintain and update the records of employees who are subject to contracts of employment with the Client.

7.2 The OHS is not acting as the Data Subject's health care provider whilst it delivers advisory or assessment services. The purpose of the OHS is to provide advice to the employer in order that the impact of health on work and work on health can be managed.

7.3 The OHS should always obtain a written reason for referral which the Data Subject is aware of and understand the purpose why and which services the OHS is being engaged to provide.

7.4 It is the responsibility of the OHS to obtain informed consent from the Data Subject and that the Data Subject understands their rights that they;

7.4.1 Have the right to refuse consent and if they chose to no medical information will be provided to the employer.

7.4.2 Even after the Data Subject has given consent, they have the right to withdraw their consent up until a report has been sent to their employer.

7.4.3 The Data Subject has the right to have corrected any factual errors in any advice being provided to their employer.

Occupational Health has some unique features as a consequence of processing data the advice provided by a clinician may not always be agreed by the Data Subject where the advice can have an adverse effect on the Data Subject's employment conditions. Clinicians should be open a transparent and explain their opinion and there should be a no surprises and no misleading Data Subject in the content of any advice. A Data Subject rights do not extend to changing the clinician professional opinion they may choose to withdraw their consent and stop any report being provided to their employer however that becomes an employment matter for the employer to deal with.
It is important that Clinicians provide independent medical advice and are not actively involved in employment disputes.

7.5 The OHS should have in place an agreement with its clients that it is the client's responsibility to provide their employee with a copy of any reports provided to the employer by the OHS.

Employers should assess the practicality of an advice provided by clinicians and how and if they intend to adopt the advice provided. Not all advice provided by the OHS is adopted and it becomes a management responsibility for the employer to decide what it intends to do. For this reason it is best practice that the Employer discusses with the Data Subject the contents of the advice and agrees any actions that the employer intends to take. It is best practice that the employer provides the Data Subject with a copy of the report.

7.6 The OHS will share data i.e. provide advice to its clients where the advice includes personal and special data. The OHS should make it clear to all stake holders what data is shared and who it is shared with. This should be further stated when consent is obtained from a Data Subject so that it is clear what the Data Subject is consenting to (See section 8 of the Code of Conducts). Within any contractual Agreement that the OHS enters into with a Client the terms of the data sharing and what is being shared should be clear and form part of their Agreement.

Data sharing is usually between the OHS and the employer; this can be communicated using the OHS Privacy Policy to explain to Data Subjects that reports including data are being sent to employers. It is best practice that the Data Subject is informed of this data sharing within the consent notices that they agree to when the OHS is delivering services. The responsibility is with the OHS to demonstrate that it obtained informed consent i.e. the Data Subject knew what was happening why it was happening and what the OHS was going to do with the data.

Increasingly clients may ask an OHS to share data with a third party, normally an outsourced Human Resources service provider. This is problematic if the OHS is providing the data directly to the third party as the standard data sharing or consent notice may not extend to the sharing with the third party. From the OHS position the easiest way is that the OHS provides the data to the Client it is then the client's responsibility to make its employees aware of any subsequent data sharing.

Where this is not possible the OHS needs to carry out a Data Protection Impact Assessment and design

- **What data is being shared?**
- **Who is the data being shared with?**
- **How is the data being shared?**
- **Why is the data being shared and for what purpose?**
- **How has the OHS made the Data Subject aware of the sharing of the data?**
- **How did the OHS obtain the Data Subject consent to share the data?**

Any DPIA needs to be documented and a detailed account of the risks, justification and accountabilities recorded.

8. Consent

8.1 The Client and the OHS do not rely on consent from Data Subject(s) to process data held for the purposes of occupational medicine. This can include transferring data between OHS providers or an OHS providing an opinion solely based on existing information held. The lawful basis for processing this data is GDPR Article 9(2)(h).

Whilst an employer does not need the consent of their employees when transferring occupational health data between OHS providers; it is best practice that the Employer does communicate the identity of the new OHS before the transfer takes place. The employer should also including what type of data is being transferred and why it is being transferred. The employer should aim to be transparent and inform Data Subjects how they can contact their new OHS as a new Data Controller and where the Data Subjects can obtain more information.

The term Data Subject is expanded here it is possible that an employer could transfer data relating to:

a) **Job applicants (Data Subjects that it has not employed)**
b) **Employees (Data Subjects it currently employs)**
c) **Leavers (Data Subjects who are no longer employed)**

8.2 Notwithstanding any regulatory obligations that clinicians may owe to their respective regulatory bodies; an OHS must ensure that it has sufficient processes and procedures in place to obtain informed consent from a Data Subject when the OHS obtains any new information (verbal) or data (physical or electronic). Informed consent should include:

8.2.1 The reason why the data is required
8.2.2 Who will process the data now and in the future?

8.2.3 How the new data will be used and processed?

8.2.4 Who the data or what data may be shared with another party?

8.2.5 The Data Subject's rights to provide the new data and their rights to withdraw their consent for the processing of the new data.

The OHS must demonstrate transparency i.e. "No Surprises" and that the Data Subject was informed before they provided any new data. This will usually have the relevant consent information in writing as part of their referral documents.
With the increased use of technology e.g. telephone and video consultations it is important that if this consent is being obtained verbally then the OHS has a record of the consent. This may range from the consent being recorded within the clinician's clinical notes to recordings of the consultation. Data Subject's should be advised that once they have given consent they still have the right to withdraw their consent during the consultation until such times as any report has been provided to the employer by the OHS.
Doctors regulated by the General Medical Council currently owe an obligation to the Data Subject to have prior sight of any reports before they are provided to the employer, this still permit the Data Subject to exercise their consent rights.

8.3 An OHS must ensure that it has documented procedures, processes, controls and training for obtaining consent from a Data Subject and that the rights of the Data Subject are respected as best as the can be and always within the law.

Given the extent that an OHS processes data it may not be practical to include all the information it relies on when processing personal and special data. The OHS should have a documented Privacy Policy and it may be beneficial to publish this Policy on its website to allow all stakeholders to be informed into how it processes data and the lawful reasons for processing data that it relies on. This may assist the OHS by including references to the link. An OHS may wish to consider including information on how to obtain its Policies to allow Data Subjects to access more information e.g. "see our Privacy Policy at www.xyzohs.com/privacy Where an OHS does not have a website it should have hard copies of its policy available for Data Subjects to read and retain, this may include written policies in its clinics.

8.4 An OHS must ensure that it has a designed a process that minimises the risk of processing the wrong data, accidental processing of data, any data loss, destruction or theft and only approved personnel have access to data. An OHS must ensure that it has appropriate and effective control and procedures when using Third Parties that they always obtain informed consent when processing new data.

The process should also include how the OHS controls consent and manages consent when it is using a Third Party data processor (sub contractor). The OHS will always remain responsible for how a Data Processor acts on its behalf and it must therefore demonstrate that its processes are designed to manage any sub-contractors. It is best practice that the OHS audits the performance of any sub-contractor to ensure that they are complying with and data processing agreements in place.
Managing Third Parties and ensuring that they obtain the same consent is the responsibility of the OHS. For example a national OHS who uses a network of third party physiotherapists to carry out assessments or treatments as part of the OHS must ensure that at each occasion the Third Party is obtaining the same and appropriate consent from every Data Subject.

8.6 An OHS must have and demonstrate that it has adequate controls to ensure that consent from Data Subjects is always obtained before data is processed and that the consent is appropriate for the use of the data being processed. Control extends to ensure that the OHS must ensure that consent is obtained and recorded and that it regularly monitors and audits how and when control is obtained. The OHS should have in place adequate checks and controls to ensure that its consent is transparent. Controls extend to the OHS employees and any sub-contractors that it uses.

Obtaining appropriate consent must happen on every referral occasion. Whilst IT systems can build in automated check before any process is permitted to continue this may reduce an OHS risk of non-compliance. Where an OHS relies on a paper based systems and relies on the actions of people to comply the OHS must ensure that it has controls that ensure there is no non-compliance.

8.7 The OHS must ensure that it has adequate training of its employees and Third Parties and that it can demonstrate that they have been trained in the procedures, processes and controls relating to its data protection systems. Given that consent to process data is a high volume practice and occurs daily on multiple occasions the OHS must ensure that the training is specific to its practices and that any training is in line with regulatory directions. There is a requirement to ensure that training is continuous and up to date.

The ICO places significant importance in the training of employees and sub-contractors to ensure that all data processing is compliant with the law. Given the risk of harm is high when processing special data (health records) the ICO expects a high level of continuous and effective training to ensure that any human errors are eliminated. The OHS must not only train it people but also demonstrate and record the training. This may include retaining copies of the content of the training materials updating training logs and appraisal documents for people. It may be beneficial for the OHS to introduce testing as part of the training to demonstrate that the training was effective and the people passed to meet the OHS expectations. The OHS must also ensure that all its subcontractors have received the same level of training.

8.8 The Data Protection Act (2018) provides that the processing of data for the purposes of occupational medicine is a lawful reason to process a Data Subject's data. That permits the OHS to process any data that it already has in its storage. An OHS must obtain a Data Subject's consent at each new referral to obtain from them consent to use any new data that the OHS gathers during that engagement. Until any reports have been created by the OHS and shared with the Client the Data Subject has the right to withdraw their consent.

Transparency is the key for the OHS to show that it obtained consent and that it processed the data in line with that consent. Where a Data Subject withdraws consent in the middle of a consultation or withdraws consent to prevent a report being provided to an employer is not the responsibility of the OHS. In these cases the OHS is permitted to process personal data but not special data (health). The OHS can advise the employer that the appointment took place but the employee withdrew consent or failed to give consent therefore no medical advice can be provided. This becomes a management issue for the employer to resolve with the employee. It is important that clinicians do not mistakenly disclose health information in attempts to be helpful.

8.9 Where a clinician requires consent from a Data Subject to obtain information from the Data Subject's healthcare provider then this information is subject to Access to Medical Reports Act (1988) declaration and procedure. The Data Subject should provide written consent to disclosures provided by their healthcare provider and have increased rights to edit or redact information that they do not wish their healthcare provider to disclose. The OHS requires the written AMRA consent declaration to be provided to the healthcare provider. The OHS should also retain a copy of the AMRA consent to demonstrate that the OHS obtained appropriate consent.

8.10 The OHS should enter into a documented agreement with clients or have a standard set of terms and conditions that include the terms of how the OHS will obtain consent, process data and share date.

9. Legal Basis for Sharing Data

9.1 Once an OHS has processed data it usually provides reports containing professional advice to its Client the employer of the Data Subject.

Firstly, in compliance with GDPR A6 (1) (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

Secondly in compliance with GDPR A9 (2) (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment. This processing complies with the UK's legal provision set out in the Data Protection Act (2018) Schedule1 Part 1, Section 1(a).

9.2 The processing of data on behalf of an employer by an OHS also extends to a Data Subject who intends to or has entered into a legal contract with that employer, this may include job applicants subject to pre-employment health screening or assessments and the processing of a Data Subject who has left the employment of the employer "a Leaver".

Article 6(1)(b) of the GDPR gives a lawful basis for processing data where:

"processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

The processing of data is necessary and justified under the Regulation (EU) 2016/679 (General Data Protection Regulation it is applied in the UK by the Data Protection Act (2018) Schedule 1 Part 1 section 2 Data is processed by an occupational health service provider on behalf of a client that relates to a Data Subject where the purpose for processing the data is the provision of occupational medicine.

The processing for the purposes of occupational medicine includes preventive or occupational medicine, the assessment of the working capacity of an employee, the provision of health care or treatment, and the management of health care systems or services or social care systems or services.

"SCHEDULE 1 Special categories of personal data and criminal convictions etc data

PART 1 Conditions relating to employment, health and research etc

Employment, social security and social protection.

1(1) This condition is met if—

Health or social care purposes.

2 (1) This condition is met if the processing is necessary for health or social care purposes.

.

(2) In this paragraph "health or social care purposes" means the purposes of—

(a) preventive or occupational medicine,
(b) the assessment of the working capacity of an employee,
(c) medical diagnosis,
(d) the provision of health care or treatment,"

10. Data Security

10.1 The OHS must ensure that personal data processed for any purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this instance, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

10.2 The risk of harm arising from a data breach to a Data Subject is high therefore the measures taken by the OHS to protect the data and avoid any breach must significant that is adequate to prevent any breach.

It is not the purpose of the Code of Conduct to specify or advise on IT systems that is a decision for the OHS. Many OHS use computers and increasingly mobile devices such as laptops, tablets and mobile phones USB sticks. The OHS must have adequate protection in place that prevents any person accidently or deliberately accessing data using a mobile device. Appropriate measures such as passwords, encryption and data storage should be managed by the OHS.
Ensure passwords are complex or sophisticated and therefore hard to reconstruct, this is more important than insisting that passwords are change regularly. For example words from a favourite song or favourite tv programme would be easier for the OHS employee to remember rather than insisting a password is changed frequently causing the employee to write down or record the password somewhere else and creating a security risk.
Passwords can be made complex by using capital letters randomly, using numbers and keyboard symbols e.g. Elvis Presley expressed as 3Lv!spRe5ley.
It is advised that data and passwords stored is encrypted

The OHS must know where data is being stored and is only stored in authorised places; storing data on laptops and USB presents an ongoing risk that data may be accessed. Also there are significant risks relating to an OHS employee or Third Party using their own personal device when processing data for professional purposes. E.g. using the family PC or ipad to do work and then other family and friends having access to the same device is a risk. The OHS would remain accountable for in the event of a data breach.

10.3 The OHS must ensure that data can only be accessed by authorised personnel and that it has security measures in place. These measures should be audited and reviewed regularly. Data should only be held in the European Economic Area (EEA) unless the OHS has entered into specific alternative arrangements with its clients.

An OHS must design risk out pf data processing as part of the DPIA. Consideration should be given to how and where the OHS stores data:

Cloud Data Storage

Using cloud technology to store data is usually cheaper than dedicated servers however the OHS must ensure that if Cloud technology s use then the data is always retained inside the EEA, Some data storage providers are cheaper because the data is hosted globally.

Email Storage

Transmitting special data via email is not recommended even when passwords are used to protect the health data. Some OHS may only have this method of operation and they must continue to use it, however the OHS should recognise the risks associated with email and start to plan to take measures in the future to provide an alternative method. Some of the risk of using email storage and transmission are:

× A copy of the email and data is held on the sender and the recipient's emails account.
× If an email account is hacked then then any data held in that account is accessible
× The management of old devices may still have data stored in it
× If the email account is hosted e.g., Hotmail, Gmail etc. then the User is not in control of where the data is being stored and may be outside the EEA.

Personal Device Storage

There are inherent risk and poor levels of control where an OHS permits its people employees of sub-contractors to use their own personal devices for the storage or transmission of data. The OHS loses control over the device and any data that is stored in it. The ability of the OHS to adequately provide a Data Subject with their data under a Subject Access Request is restricted.

10.4 An OHS must ensure that it has effective and appropriate data backup procedures and infrastructure. Devices must be backed up to ensure secure copies of personal and special data cannot be accidentally lost due to a single error or failure. The greater the risk of harm from data loss or data breach the greater the data backup procedures that are required to be in place and be effective.

Web based IT Systems should be backed up regularly depending on the size and scale of the system and data being held then this may determine the frequency of backup. Typically backups should be carried out daily but even this may not be enough. The OHS should risk assess the impact of the loss of data and the ability to retrieve data that is backed up, the more data has changed since the last backup may influence the frequency of the backup procedures.
An OHS should take professional technical advice in how it manages and stores backup data. There is no benefit in storing backup data on the same device or in the same place as the main system is e.g. if there was a fire the main system would be lost as would the backup data.

A small OHS may only use one or two devices to operate their entire business. Internet Service Providers and Data Storage providers increasingly offer web based back up services. In these circumstances having a backup of data is safer than losing all data by having no backup data procedures.

Backup data must be encrypted and protected when being held

10.5 Where an OHS uses a website for the processing of data it must ensure that it has adequate cyber security measures in place to protect the website from attack. Adequate protection may include accreditation to the UK cyber security accreditation Cyber Essentials see https://www.cyberessentials.ncsc.gov.uk/. Adequate protection will require the OHS to ensure that appropriate penetration testing of their website is conducted.

10.6 The OHS must ensure that it has in place appropriate technical expertise to manage the technical and cyber security aspects of its infrastructure. This expertise should provide constant surveillance and monitoring of the technical and software

infrastructure to protect any possible attacks. The OHS must ensure that it has appropriate and up to date malware and patches of software fixes in place where it processes data using websites.

10.7 The OHS must ensure that it has appropriate policies and in place for the operations of its IT hardware and software where they are used for processing personal or special data. These policies should be communicated to the OHS employees and be reviewed on an appropriate frequency. It is likely that any review period that is longer than 2 years from the date of the last review is not an appropriate period.

10.8 The OHS must ensure that it has adequate training of its employees and sub-contractors and that it can demonstrate that they have been trained in the procedures, processes and controls relating to the operation of its IT hardware and software. The OHS must ensure that the training is specific to its practices and that any training is in line with its policy directions. There is a requirement to ensure that training is continuous and up to date. Training records should be retained as part of ongoing monitoring.

10.9 The OHS should ensure and demonstrate that it has appropriate procedures for the archiving of personal and special data and that the archiving activity is completed on a regular basis. The OHS will process personal and special data of Data Subjects who are currently employed by its clients "employees". The OHS may also process personal and special data of Data Subjects who are no longer employed by its clients "Leavers"

Subject to a client's data retention periods (see Section 11) the OHS must ensure that it receives regular instructions from its clients on data to be archived as Leavers.

Subject to a client's data retention periods (see Section 11) the OHS must ensure that it receives regular instructions from its clients on data to be destroyed as no longer required to be processed. The OHS must retain copies of the instruction of the data that it has destroyed.

The OHS should have effective risk management strategies in place, where in the event of a data breach it minimises access to the data held. It is recommended that Leavers data is stored separately away from live employee data and that the OHS has effective data management procedures in place that ensure that it regular reviews data being held and can identify expected destruction dates.

The destruction of data is ultimately a decision for the Client however an OHS takes on an avoidable risk allowing clients to provide inadequate instructions as to the data that is to be retained as live or archived. Holding excessive data increases the risk to the OHS and its clients. It is best practice for the OHS to constructively engage with clients to ensure that regular (monthly) and continuous instructions are received by the OHS in respect of data held.

10.10 Where an OHS holds paper records there is a requirement that it has effective data management procedures in place for these records. This will include:

10.9.1 An index of all of the paper records that the OHS processes.
10.9.2 An index of the location of the record being stored this should allow any record to be retrieved with minimum effort.
10.9.3 Each record is classified as to its status Employee or Leaver
10.9.4 Where a record is being held as an archived file then a data retention period should be recorded by the OHS.

10.11 Where data is being stored on paper in bulk storage the OHS must ensure that appropriate security protection is in place where only authorised personnel may

access the data and the storage facility has a sprinkler defence system in place in case of fire.

10.12 Where data is being store on paper in live file storage (cabinets) the OHS must ensure that the cabinets are stored in a room that can be locked and secured by a key or entry mechanism. Each cabinet should be locked and the OHS has in place ways of working that cabinets are only opened as and when needed. Live file storage should only be accessed by authorised personnel.

10.13 The OHS should ensure that all its clients agree that the Occupational Health data and storage are controlled by the Data Protection Regulations The Access to Medical Records Act (1990), The Access to Medical Reports Act(1998) The Electronic Communications Act (2000), The Nursing Midwifery Council Guidance for Record Keeping (2010), the Guidance Issued by the General Medical Council (2006) and this ICO approved Code of Conduct for Data Processing.

11. Retention Periods

11.1 It will be the responsibility of the client of the OHS to determine their data retention policy and when data should be destroyed relevant to the requirements that the Client has obligations to comply with.

11.2 The OHS should ensure that it receives regular instructions from its clients to ensure that the OHS complies with the Data Retention Policy of each client.

The following data retention periods are advisory only and subject to the Client or OHS agreement. The time period is less important however will need to be justified if challenged as being excessive. It is important that the OHS has documented these data retention period and complies with them. Data stored too long is a problem for the client to justify in the event of a breach. Data stored longer than the agreed Data Retention period is a problem for the OHS as they have processed data outside of the agreed terms.

Data Subject Type	Retention Period
A data subject who applied for employment but was never employed by the Client	6 months after application
A Data Subject employed by the Client who has left employment	3 years and 3 months from the date of leaving
A Data Subject employed by the Client who may have a claim subject to the Limitations Act (1980) The Client may determine retention on a case by case basis	Up to 15 years from date of leaving
A Data Subject who has been or may have been subject to risks of industrial disease (Asbestos, Lead, Ionising Radiation, Noise or Chemical Exposure requiring routine monitoring)	40 years from date of leaving
A Data Subject employed by the NHS who has been or may have been subject to risks of industrial disease (Asbestos, Lead, Ionising Radiation, Noise or Chemical Exposure requiring routine monitoring) As required by Records Management Code of Practice for Health and Social Care 2016	50 years from date of leaving or until 75th Birthday whatever is longer.

12 Transfer of Data

12.1 Upon the commencement of a service there may be a requirement for an OHS to take receipt of data held previously on behalf of the new client. This data may include

personal and special data relating to live employees and ex-employees who no longer employed by the client “Leavers”. The data transferred should be under the responsibility of a clinician who has the overriding responsibility for the delivery of occupational health services for that client. A clinician should be a qualified and hold a valid registration with either: General Medical Council, Nursing Midwifery Council or the Health Care Professions Council.

12.2 Before the transfer of data takes place the Client should consult with any affected employees or make employees aware that there is a new OHS taking over the services. There is no longer a requirement to obtain the consent from every Data Subject the Data Protection Act (2018) permits the processing of the data for the purposes of occupational medicine. Communication and advising the employees who the new OHS and how they can be contacted is best practice.

12.3 The Clinician who requires the data to be transferred to their OHS should write to their respective colleague in the incumbent OHS requesting the data is transferred. Clinicians should ensure that the overriding objective during the transfer is the health and wellbeing of the Data Subject, for this reason it may be practical for the OHS’s to agree that some records temporarily remain with the incumbent OHS until advice or services are completed. In any event it is likely that data is transferred on or around the commencement date of the service.

12.4 The OHS’s should act professionally and look to carry out the transfer of the data as efficiently as possible. They should agree which OHS is responsible for the physical transfer of data. Where the data is electronic and being transferred it should be transferred using Secure File Transfer Protocols or if being sent via a CD disk, USB or other storage device. The data should be encrypted or secured via a password. In order to protect the data the password should be transmitted separately from the data being transferred. An index of the files being transferred listing the names or identifiers of each Data Subject should be sent by the transferring OHS to the receiving OHS. There should be consignment documentation confirming the transfer of the number of files and confirming the index is accurate and all files have been received. Confirmation of receipt of the data should be sent back to the transferring OHS.

12.5 Where the data is physical i.e. paper and being transferred it should be securely packed with each parcel referenced and indexed to identify the total number of parcels in the consignment. An index of the files being transferred listing the names or identifiers of each Data Subject should be sent by the transferring OHS to the receiving OHS. There should be consignment documentation confirming the transfer of the number of files and confirming the index is accurate and all files have been received. Confirmation of receipt of the data should be sent back to the transferring OHS.

The OHS should look to transfer data as efficiently and securely as possible. Where paper records are being transferred it is recommended that records are shipped directly from the collection location to the deliver location. There is an increased risk of sending data through parcel companies where the parcels are shipped through central distribution points, this may be unavoidable but if possible this transportation method should be avoided. If this is not possible say a few files being shipped in an envelope then the OHS should alert their client to the increased risk and take action such as recorded or tracked

delivery. The risk of data loss should be a greater priority than the cost of transport.

12.6 All occupational health records should be transferred at the end of a service provision the OHS should not retain copies of the data unless this is agreed as part of risk management procedures before data is transferred. Records will include reports, forms, assessment results, clinical notes, drawings pictures or any other personal or special data. Where data is being retained for risk management reasons the OHS should agree with the client or the other OHS how long it will retain copies of the data.

An OHS must not use data as a hostage for the purposes of payment or due to any dispute with its client there is no right of lien on personal and special data to do so would be a breach of the Data Protection Act as the data would be processed i.e. stored for a reason that it was not collected for.

12.7 Where the OHS provides other treatment services such as counselling, physiotherapy or Employee Assistance Programmes these services would not be included within occupational health services and should not be transferred. In the case where an OHS provides these services it acts as a healthcare provider to the Data Subject and the services provider has the same responsibilities as any other healthcare provider.

13 Data Destruction

13.1 An OHS must only destroy data paper or electronically in line with an instruction from their client acting as a Data Controller or in compliance with the client's data retention periods.

13.2 The any personal or special data held by the OHS is not the property of the relevant Data Subject therefore the Data Subject does not have the right to be forgotten under the Data Protection Act (2018). Where a Data Subject has objections to the client retaining their data, they should discuss this matter directly with the client and it is there decision if and when data is destroyed.

13.3 When an OHS is provided with an instruction to destroy data it must be destroyed irretrievably either in paper or electronic formats. Paper records should be destroyed by an approved contractor who can provide evidence of destruction and a certificate of destruction. The OHS should retain this certificate.

13.4 An OHS must also have secure destruction procedures and processes for any of the devices it won or has used for the storage of data. The OHS should retain evidence of any equipment destruction and the destruction is beyond any prospect of retrieving data stored within the device.

Destruction of data should involve paper shredding or incineration of paper records. Adopting an environmental recycling approach to paper records is a high risk practice and should be avoided.
The OHS must ensure that it completely destroys any equipment that may remotely have data stored within t e.g. laptops, mobile devices desktop processors servers voice recorders. In the past the ICO has taken a punitive approach against Data Controllers who have had inadequate destruction processes resulting in significant fines being applied. The days of donating equipment to charity or allowing employees, friends and family members to use equipment for their personal use are no longer. An OHS has a duty of care to Data Subjects and equipment must be destroyed.

14 Data Breach Notification Procedures

14.1 The Data Protection Act (2018) introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the OHS must also inform those individuals without undue delay.

14.2 An OHS should ensure it has robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not an OHS needs to notify the ICO and the affected individuals. The OHS must also keep a record of any personal data breaches, regardless of whether it is required to notify.

14.3 An OHS should have documented processes and procedures that allow it to prepare for a data breach. These should include the following features:

14.3.1 An OHS and its people knows how to recognise a personal data breach.
14.3.2 An OHS and its people understand that a personal data breach isn't only about loss or theft of personal data.
14.3.3 An OHS has prepared a response plan for addressing any personal data breaches that occur.
14.3.4 An OHS has allocated responsibility for managing breaches to a dedicated person or team
14.3.5 The people who work for an OHS (including employees and sub- contractors) know how to escalate a security incident to the appropriate person or team in the organisation to determine whether a breach has occurred.

14.4 In the event that a Data Breach arises the OHS should have processes and procedures in place that enable it to respond to any personal data breach. These should include the following features:

14.4.1 The OHS has in place a process to assess the likely risk to individuals as a result of a breach.
14.4.2 The OHS has a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
14.4.3 The OHS knows what information it must give the ICO about a breach.
14.4.4 The OHS has a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms. It is important that the OHS must inform affected Data Subjects without undue delay.
14.4.5 The OHS knows what information about a breach it must provide to Data Subjects, and that it should provide advice to help them protect themselves from its effects.

14.5 An OHS must document all breaches, even if they don't all need to be reported.

The OHS should understand the importance of how it manages a data breach. It is important that it acts honestly and transparently and without delay. Notification should be made when the OHS knows data has been breached and it knows the Data Subjects that are affected.

In the event that a breach arises it is important that the OHS notifies the Data Subjects or group of data Subjects affected by the breach and not simply all data subjects.

An OHS may also have contractual agreements with its clients to notify them. It is important that the priority should be notification to the ICO and the data subjects first and not clients; even if there is a contractual obligation to do so. From a practical point the OHS may benefit from notifying the client as they may also have an obligation to notify the same Data Subjects or they wish to manage any crisis management plans.

OHS means employees, workers and sub-contractors the OHS must ensure that its breach management plans are communicated to al and it has retained evidence to prove this.

15 Subject Access Requests

15.1 The right of access, commonly referred to as subject access, gives Data Subjects the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why an OHS is using their data, and check it is being done lawfully.

15.2 Data Subjects have the right to obtain the following from an OHS: confirmation that the OHS is processing their personal data; a copy of their personal data; and other supplementary information – this largely corresponds to the information that you should provide in a Privacy Policy.

15.3 A Data Subject is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that the OHS establishes whether the information requested falls within the definition of personal data.

The OHS has the right to redact certain data even if it is included in the document being provided to a Data Subject under request. The OHS should not provide personal identifying data of a third party e.g. a mobile phone number or email address. This may extend to the name of a person if they were not the clinician who was the author of the report. Where management reports are provided by clinicians the Name and title of the clinician who wrote the report should not be redacted.

15.4 An OHS should ensure that it has appropriate training for its employees who manage and administer SAR's. Within occupational medicine the process is complex and should not be considered as an administration task. The OHS should demonstrate that it has trained its employees and that there is an independent checking and supervision process before SAR data is released

.

15.5 An OHS should recognise that it will have committed a Data Breach if it discloses personal data or wrong data to a Data Subject within a SAR. In this case the OHS should apply its Data Breach Management Plans see section Individuals can make a subject access request verbally or in writing.

Care is required that when dealing with occupational health files in paper or electronic that the file only contains the data of the data subject and that a check has been made to verify this. Dealing with paper files or paper files that have been digitised may result in errors where a file for a Data Subject contains documents relating to another unrelated person.

15.6 Subject Access requests may be made verbally or in writing providing the OHS with the Data Subject contact details and the request. An OHS must ensure that it has adequate communication methods for Data Subjects to make requests. An SAR must be completed within 1 month from the next day following receipt from the Data Subject.

Managing requests can be problematic for an OHS it is not acceptable for an OHS to have poor communication channels therefore it must ensure that it is alert to how a Data Subject can make requests for example in writing may include, letters, emails, completing forms, social media pages, SMS, Website contact pages. The time limit starts when the request was sent not when it was received.
Where a SAR is made verbally the OHS must ensure that its people are alert to such request there is no need for the Data Subject to use any formal words so a simple comment such as "I want a copy of my file" in a consultation appointment is in effect an SAR. Employees must act and make the OHS aware of the request. Where an SAR is made in an appointment it is recommended that this is recorded in the clinical notes.

15.7 An OHS can omit data or redact data that it provides to a Data Subject if in the professional opinion of the OHS the data is likely to cause harm to the Data Subject or another person. The decision to omit or redact data on this basis should be taken by an independent person authorised and competent to make such a decision.

There must be high justification to omit or redact data on the grounds of harm it should not be applied for convenience of the OHS or its clinicians e.g. if the file contains some embarrassing remarks or content for the OHS or its clinicians who may have inadvertently made unprofessional or inaccurate notes.
Where data is being omitted on the basis it is recommended that the data is independently reviewed by a clinician and a risk assessment is made on the likelihood of harm. This assessment should be documented. There is no requirement to notify a data subject that data has been omitted. The OHS should only omit the relevant data that may cause harm and not the whole file or large sections of the file.

15.8 An OHS may seek clarification from a Data Subject on what data they require if the OHS considers the request to be excessive or repetitive. Whilst the clarification will reset the time limit for responding to the SAR to the start date that the clarification is provided by the Data Subject it does not remove the request. The OHS must demonstrate that it had reasonable grounds to seek clarification from a Data Subject on a case by case basis.

An OHS may have grounds to seek clarification from a Data Subject where the request is plainly excessive and where the OHS has a genuine motive to provide the data that the Data Subject needs and not all data. An OHS may also seek clarification where it has recently provided the same data to the same Data Subject and they appear to be acting unreasonably.

There are no grounds to refuse providing a SAR other than there is no data held. The cost time and resources required to provide SAR is not a justifiable reason for not providing the data requested.

15.9 An OHS may extend the time required in responding to a SAR if it can show reasonable and just grounds for being unable to respond to the request. A time limit may be extended for a reasonable time period either by agreeing with the Data Subject when the data will be provided or by explaining to the Data Subject the reason for the delay and providing a revised deadline for delivery of the data.

It is always best to try and agree an extended deadline with the Data Subject, in the event that the OHS cannot provide the data in the time require it should be transparent and advise the Data Subject why it cannot provide the data and when it will provide the data. Providing these reasons are justified the ICO has taken a pragmatic approach to such requests.
Reason for delay may include the resources and time required in retrieving the data or due to some technical reasons if the data is being held electronically say in different legacy systems.
The OHS should be aware that it is a breach of the Data Protection Act (2018) if they do not have adequate data management and retrieval systems in place and the delay is because of its failure to adequately store the data.

15.10 An OHS cannot charge a Data Subject for the provision of an SAR unless the Data Subject is acting unreasonably and has made repeated recent requests for the same data and the OHS has provided this data.

The OHS is a Data Controller and has SAR responsibilities because it has been appointed by the client as the OHS. It has no proprietary ownership of the data and must provide the SAR as an extension of the service. It is not the purpose of the Code of Conduct to advise an OHS on its commercial policy. Medium to large OHS may require to invest significant resources and costs to providing this service and may elect to charge their clients for the service either within their overhead charges or as a transactional cost as and when occurred.

16 Compliance and Monitoring

16.1 Before an OHS may be accredited to this Code of Conduct it is a requirement of the Code that it:

a) Meets the Assessment standards required by the Code before the OHS can be accepted as being accredited.
b) Demonstrates that it has internal monitoring processes and reviews of its data processing and data security practices.
c) Evidences that is conducts regular management reviews of its data processing practices.
d) Has in place an external audit function that at least annually independently reviews its data processing and data security practices

16.2 Where the Code of Conduct uses words such a “must” and “will” these are requirements of the Code of Conduct and the OHS is in breach of the Code of Conduct. Terms such as “should”, “may” and “can” are advisory and unless the OHS has good reason not to comply with the Code.

The Code is the black text. **Guidance and advice is the bold blue boxed text**

16.3 An OHS should carryout continuous surveillance of its data processing activities and any non-compliance (Data Incidents) or breaches of data processing. The management of the OHS should carryout regular reviews of the compliance monitoring with the view to acting and improving its data processing activities whilst complying with the Code of Conduct and its guidance.

The OHS should adopt a continuous improvement approach to its data processing activities. Where an OHS has had a non-compliance or a failure that is not reportable to the ICO but has been a risk then these should be recorded as Data Incidents. An OHS should encourage its people to report Data Incidents to the OHS and the OHS should record and review Data Incidents.

Whist complete compliance is the desire reporting Data Incidents should be encouraged in the OHS organisation on the basis that the more Data Incidents

that are reported the greater visibility of the risks and non-compliance the OHS has of its processing activities. Action can then be taken to deal with Data Incidents therefore the philosophy that a rise in Data Incidents followed by corrective actions should lead to a reduction or elimination of data breaches

16.4 An OHS should carryout audits of its data processing activities and demonstrate that it has in place a continuous improvement philosophy and that the OHS management have reviewed these activities and taken appropriate action. Audits may be conducted as part of any quality management or clinical assessment accreditation. E.g. ISO9001, SEQOHS or RISK Cyber Essentials or by the Code of Conduct monitoring body..

16.5 In order to demonstrate that an OHS has effective data management and processing controls accreditations such as Cyber Essentials, Cyber Essential Plus and ISO 27001 should be considered with accreditation or plans to achieve these accreditations.

16.6 Only an OHS that has been approved by the Code of Conduct may use its accreditation marks and logos. All OHS will be subject to ongoing review and must ensure that they take all and any measures required to ensure that the OHS complies with the Code of Conduct. Failure to comply with the Code of Conduct will mean that the OHS has its accreditation suspended form the Code of Conduct.

16.7 This Code of Conduct will be overseen and reviewed by the Code of Conduct Board which is an independent board acting as an independent function of the Society of Occupational Medicine. The Code of Conduct Board will consist of 7 members made up of the following:

16.7.1 4 members with qualifications in Data Protection or the management of Data Protection in Occupational Health.
16.7.2 2 members with qualifications in occupational health or having responsibility or the clinical management of an OHS
16.7.1 A member of the Society of Occupational Medicine.

16.8 The Code of Conduct Board will be responsible for carrying out Conduct and Suspension panels where the Monitoring Body has carried out appropriate investigations and recommends that an OHS should be subject to a sanction for failure to comply with the Code to Conduct. These sanctions may include a Compliance Order or in serious cases suspension of the accreditation of the OHS from the Code of Conduct

17 Monitoring Body

17.1 It is a requirement of the ICO that a Monitoring Body is created to overseen and manage that accredited OHS comply with the Code of Conduct. This Monitoring body will be formed and approved by the ICO as being Is independent from Code of Conduct Board.

17.2 The Monitoring Body will act freely from sanctions or external influence to ensure that no conflict of interest arises between it and the Code of Conduct Board

17.3 The Monitoring Body will administer applications and carry out assessments of any OHS who applies to be accredited to the Code of Conduct.

17.4 The Monitoring Body will provide accredited OHS with support guidance and training where requested to ensure that it complies with the Code of Conduct.

17.5 The Monitoring Body will publish the Code of Conduct and any updates reviews or guidance approved the Code of Conduct Board. The Monitoring Body will have the necessary

required knowledge and expertise and have established procedures, structures and resources for the monitoring of compliance with the code.

17.6 The Monitoring Body will provided a first line of complaint and support service to enable it to handle any complaints made against an accredited OHS. The Monitoring Body will Has an open and transparent complaints handling process.

- 17.7 The Monitoring Body will communicate to the ICO code member infringements that lead to suspensions or exclusions or Compliance Orders and will hold appropriate legal status.

Appendix One – Definitions

In this Code of Conduct the following words have the following meanings:

Data Protection Act (DPA)	Means the Data Protection Act (2018) and any subsidiary or subordinate legislation as the same may be varied or replaced from time to time.
Data Protection Regulations	Means General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) Data Protection Act (2018) Electronic Privacy Directive (2002) Privacy and Electronic Communication Regulations (2011)
Data Controller	As defined in the Data Protection Act (2018), means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed.
Data Protection Impact Assessment (DPIA)	A privacy impact assessment (PIA) is a process that focuses on identifying the impacts on privacy of any new project, technology, service or programme and, in consultation with stakeholders, taking remedial actions to avoid or mitigate any risks.
Data processor	In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. This means that the person processes data for a purpose and according to a manner determined by the data controller, and makes no independent determination of such matters.
Data Protection Principles	These are set out in the fair processing/ Privacy Policy and are required to be followed to ensure compliance with the Code of Conduct
Subject Access Request (SAR)	A request by a Data Subject to provide a copy of the data that a Data Controller holds about that Data Subject
Data Subject	Data subject means an individual who is the subject of personal data.
OHS	Occupational Health Service the organisation or person who is engaged to provide the services for the client.

Privacy Policy	All Data Controllers must have a Fair Processing Notice (otherwise known as a Privacy Policy), which is available to data subjects. A Fair Processing Notice is intended to make sure that data subjects are aware of how data is collected and used by the data controller. It aims to ensure that data controllers process personal data fairly and lawfully. Fair Processing Notices may be in oral or written form. The DPA sets out that, at a minimum, Fair Processing Notices should contain the following information - who the data controller is, what the data controller intends to do with their information and any other relevant information (e.g. in the context of data sharing who the data will be shared with). Fair Processing Notices may also be used to provide additional information such as informing people about their subject access rights or the data controller's security arrangements.

Personal Data	Personal Data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".
Special data	Personal data means data which relates to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller now or in the future. This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. (a) the racial or ethnic origin of the data subject (b) their political opinions (c) their religious beliefs or other beliefs of a similar nature (d) whether they are a member of a trade union (e) their physical or mental health or condition (f) their sexual life (g) their commission (or alleged commission) of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by the data subject, including the disposal of such proceedings or the sentence of any court in such proceedings For the avoidance of doubt all medical records, forms, notes, recordings assessments reports or emails containing person identifiable data and medical data shall be considered to be special data.