WARWICKSHIRE POLICE	**POLICY**

Security Classification	Official	
Disclosable under Freedom of Information Act 2000	Yes	

POLICY TITLE	**Occupational Health Records Management**
REFERENCE NUMBER	**WP122**
Version	**1.1**

POLICY OWNERSHIP	
DIRECTORATE	ENABLING SERVICES
BUSINESS AREA	HUMAN RESOURCES

INITIAL IMPLEMENTATION DATE	**September 2022**
NEXT REVIEW DATE:	**December 2018**
RISK RATING	**MEDIUM**
EQUALITY ANALYSIS	**HIGH**
TIER	**2**

Warwickshire Police welcome comments and suggestions from the public and staff about the contents and implementation of this policy. Please e-mail policiesandprocedures@warwickshire.police.uk

Contents

1.0 POLICY OUTLINE

This policy provides a structure and framework to ensure all processes and procedures relating to the management of health records can be followed and adapted to meet changing requirements in respect of storage, accessibility, disposal and information needs.

Warwickshire Police will hold a range of health records, in hard copy and electronically, and on G2 (specialist OH software system) each category of which carries different requirements under legislative requirements and professional guidelines. In all cases this policy covers:

- the control of records
- the transferring of records
- the transportation of records
- audit trails of access
- retention and disposal of records

2.0 PURPOSE OF POLICY

The aims of this policy are to provide:

- a systematic and planned approach to occupational health (OH) records management with regards to retention and disposal
- an awareness of the need for responsibility and accountability at all levels, when dealing with the management of clinical information.

3.0 IMPLICATIONS OF THE POLICY

This policy is to ensure that all Occupational health records held by Warwickshire Police Occupational Health department (OHU) are treated in accordance with legal obligations and statutory requirements and provides guidance for all users of health records.

Health records are valuable because of the information they contain and the information is only usable if it is correctly and legibly recorded, kept up-to-date and is available when required. All users must ensure records are used and kept in accordance with the principles of:

- The General Data Protection Regulations (retained from EU) 2016
- The Data Protection Act 2018
- The Human Rights Act 1998 (HRA)
- The Management of Police Information (MoPI) Code of Practice 2005
- Warwickshire Police's Information Management and Security Policies
- The Access to Medica Records Act 1988

- The Health and Safety At Work Act 1974
- The Management of Health and Safety at Work Act 1999
- The Records Management Code of Practice for Health and Social Care 2016 (Information Governance Alliance)
- The Nursing and Midwifery Council Record Keeping Guidance for nurses and midwives
- Warwickshire Police Records Management Policy

In terms of GDPR requirements, the legal basis for processing this data is necessary for the employer's legitimate interests, for example in managing sickness absence; or that it is necessary for compliance with a legal obligation, such as the duty to make reasonable adjustments.

Under GDPR health information is a special category of data, and therefore requires a relevant condition allowing the processing of the data. Depending on the specified purpose of the report this is likely to be one of the following:

- the assessment of the working capacity of the employee or
- for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the employer in connection with employment, (e.g. health and safety obligations and the obligation to make reasonable adjustments); and/or
- for the establishment, exercise or defence of legal claims.

Compliance with the legal requirements and guidance requires that not only are records stored securely and access controlled but also that they are accurate and fit for purpose, with the following key elements:

- All staff receive training to ensure the General Data Protection Regulations (EU) 2016 and Data Protection Act 2018 is adhered to
- The information held is accurate, needed and we know the reason for holding such data
- The individuals concerned know we hold information on them and the purpose for holding the data
- Staff are aware of under what circumstances they can pass on data
- The data stored on individuals is relevant, complete, kept up-to-date and accessed by those on a 'need to know' basis
- The data stored on individuals is held in a secure environment, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- The data stored on individuals is deleted or destroyed as soon as it becomes obsolete and there is process for secure shredding of confidential data
- Where an external agency is used to dispose of or destroy confidential data, they comply with the General Data Protection Regulations (EU) 2016 and Data Protection Act 2018 requirements

4.0 ROLES AND RESPONSIBILITIES

4.1 The OH Manager has operational responsibility for this policy and for ensuring this policy complies with legal and regulatory edicts. They are responsible for:

- Ensuring records are stored securely and access to them is controlled
- Providing learning and development with key learning points from this policy
- For monitoring the policy to assess its overall effectiveness

4.2 The OH Manager is the Nominated Information Asset Owner for OH records and is responsible for ensuring the asset they 'own' is managed in accordance with this policy, and maintaining adequate records within the context, both legal and regulatory, of the business area the asset operates, e.g. maintaining an Information Asset Register for the records held.

4.3 All staff are responsible for keeping a record of any significant processes conducted as part of their duties with OHU. The record should be saved appropriately, a retention period assigned and access controls applied as necessary. A GDPR Checklist (see appendix F) will be completed to ensure that records are only kept for the relevant length of time. Should it be required a GDPR Decision Sheet (see Appendix G) will also be completed.

5.0 PROCEDURE

5.1 Types of Records held by Occupational Health

Health Records – these are records of individuals who have undergone some form of health surveillance and will include personal details, details of the health surveillance checks carried out and the OH assessment of fitness for role. They should not contain any confidential medical information.

Medical records are compiled by a doctor or nurse and may contain information obtained from the individual during the course of health surveillance. This information may include clinical notes, biological results and other information related to health issues not associated with work. This information is confidential and should not be disclosed without the consent of the individual.

Medical reports are those prepared by a medical practitioner who is or has been responsible for the clinical care of the individual, e.g. GP or consultant's reports – OH reports completed by an OH nurse or physician (i.e. FMA, SMP and IRMP) will not normally be considered to be a medical report. The requesting and use of these reports is specifically covered within the Access to Medical Records Act.

Management reports can include management referral forms submitted to OH, fitness to work and case management reports completed by OH professionals and shared where consent is given by the individual. These reports may contain confidential medical information and will also be retained in HR files where the same standards for record management must be applied.

Clinical notes from the in house couselling team will be held securely within the OH records management system G2. Where specialist or outsourced therapy is provided through OH these records will not be held by the OH and will be held by individual therapists who are required to comply with all relevant standards as part of their professional registration.

5.2 Records Storage

All newly created OH records will be stored within the dedicated secure OH software system, G2. There will be a gradual migration of existing paper and electronic files to G2. The G2 system will ensure all records are securely backed up and have robust audit trails associated with them. Use of the G2 system will reduce the risks associated with data storage and transfer, it will allow managers and employee to communicate, send and receive confidential information through the system, significantly reducing to use of email and other less secure methods.

Historic electronic records will be retained within the shared network drive folder allocated to OH awaiting migration to G2, and access to this will be restricted to OH staff. Electronic records must be held within shared drives rather than on individuals' drives and staff should not use home email accounts or private computers to hold or store any sensitive records or information relating to the business activities of OH. Regular back-up copies will be scheduled and undertaken according to digital services policies and procedures. Back up should provide a reliable copy of the record, which is easily accessible.

Third party providers hold electronic records on their proprietary systems, which are accessed by OH staff.

The Origin HR system will be used to record basic details of OH activity, e.g. the date a referral was made, whether an officer has been placed on restricted duties, but no confidential medical information will be added to origin by OH.

Hard copy records are retained in locked filing cabinets within the OH office, which is itself within an area to which access can only be gained via a keypad operated door lock. Access levels are maintained through the force's Axiom system and restricted to OH and authorised facilities staff. Keys to confidential filing cabinets are housed in a secure code box which only OH staff have access to.

Records containing personal or sensitive data must not be left unattended in offices or areas accessible to the members of the public and staff should ensure that personal or sensitive data is not displayed on computer screens visible to passers-by.

All desks must be left clear at the end of the day or when leaving desks and when non OH staff may be present in the department.

5.3 Transfer of Records

There will be limited occasions where the physical transfer of a full OH file is required with the introduction of the G2 Occupational Health system.

Where information is sent by email, it should be sent solely using the secure force email system. Where OH send information or reports to any non force secure email (for example if an individual is having any difficulties accessing the G2 system and reports have to be emailed), consent from the individual, outlining the risks or using a non secure email provider should be obtained and documented first.

Where such records have to be transferred outside of the force email system e.g. as part of legal proceedings, or in response to a Subject Access Request, records will either be posted in hard copy using recorded delivery or emailed in a password protected format with the password sent in a separate email. Where records are transferred to the SMP, where possible this shall be completed using the G2 system.

Where an officer has successfully applied to transfer to another police force, their OH records will be provided, with their consent, at the point at which the OH unit is informed that their transfer has been confirmed.

Where an officer is applying to transfer to Warwickshire Police, at the point at which a conditional offer of transfer is made OH will request their records from their current force, with their consent.

Should the OH Practitioner feel further information is required from the OHU at the candidate's current force, they should obtain the candidate's informed consent and request a bespoke report relating to the relevant medical condition.

Where there is a change of third party provider, the transfer of relevant medical records will be undertaken during the implementation phase of the new contract. Individuals will be notified of this transfer and given the opportunity to object to the transfer.

5.4 Transportation of OH Files

Due to the personal, sensitive and confidential information in clients' health records, care must be taken when transporting them within or outside the OH unit. Paper files should not be moved from the OH office unless it is for archiving purposes, in which case they will be transferred using the agreed force transport arrangements.

5.5 Record Audit Trails

Records stored on G2 are supported by audit trails, which record details of all additions, changes, deletions and viewings. Typically, the audit trail will include information on:

- who – identification of the person creating, changing or viewing the record;
- what – details of the data entry or what was viewed;
- when – date and time of the data entry or viewing; and

Audit trails are important for medico-legal purposes as they enable the reconstruction of records at a point in time. Without the associated audit trail, there is no reliable way of confirming if an entry is a true record of an event or intervention. Regular audits should be conducted, and recorded, to check through the records held, to ensure personal and sensitive data is not kept for too long and / or needs to be archived or deleted.

5.6 Missing Records

This will be minimised by:

- Ensuring the OH Team minimises the places where manual records may be kept
- Keeping a register of records transfers (e.g. sent to elsewhere) to facilitate location.

In the rare event a file is temporarily missing, a record of missing / lost files with as much of the information as possible listed is to be kept by the OH Manager. They will conduct a further risk assessment and take necessary steps to minimise risk to those involved in the event records are mislaid, as well as reporting the potential loss to the force Information Security Officer. Should a new set of medical records have to be made, this will be marked 'Temporary File' and merged with the original when possible.

5.7 Retention of Records

Personal data and sensitive data must not be kept longer than is necessary or relevant for the purposes for which it was collected. However Occupational health records may be crucial in legal proceedings, which can take place years after the employee has left the company.

Clinical information contained from management referrals will be retained for at least 6 years after the employee has left unless deemed of medical importance to retain.

Records from health surveillance should be kept for a minimum of 40 years after the date of the last entry, or longer if required by law e.g. under the Control of Asbestos at Work Regulations 1987 and the Control of Substances Hazardous to Health Regulations 1988.

The continued storage of and controlled access to information held for a policing and / or medical purpose, will be maintained as per the guidance at Appendix A and the following points outline the key aspects of record retention.

5.7.1 Records of Leavers should be archived and registered on the force's archive record system before being transferred to the records archive.

5.7.2 Records where legal cases are on-going records will be retained and identified 'Retain Required for Legal Purposes'. Records may only be sent to archive once the case is concluded or settled, even if the employee has left employment.

5.7.3 Where there is a statutory requirement for record retention, these records will be retained for the required period and so marked. Should medical records be transferred to a new OH provider, the details should be recorded and a register maintained.

5.7.4 Where personal and sensitive data is shared between organisations, those organisations should agree what to do once they no longer need to share the information, e.g. return it to the supplier, without keeping copies or all the organisations involved delete their copies of the information.

5.7.5 Records identified as having a long-term or historical value or which need to be kept permanently, should be retained in the section which created them or transferred to the force's archive.

5.8 Deceased Persons

OH staff will release medical records about deceased persons in accordance with the Access to Health Records Act 1990 and only upon receipt of a valid written consent from the next of kin or other *bona fide* authority with the authority of the Head of Human Resources if required.

5.9 Clinical Records Disposal

On notification that a staff member has left the organisation, the OH administrator is required to check the contents of the OH file for the individual and complete a GDPR Checklist and Decision Log shown at Appendix B. Should the administrator identify that any of the documents from the checklist are present, the file will be passed to the OHA to identify the destruction date and complete the GDPR Checklist and Decision Log.

Clinical records not selected for archiving and which have reached the end of their administrative life will be disposed of. Personal information should be removed from documents before being disposed of as per the agreed process at the end of their retention period. Disposal will be carried out in line with ISO 27002 standards, and in accordance with MoPI 2010 (section 7.8).

All procedures relating to the disposal of records must be followed by trained staff to provide safeguards against accidental loss or disclosure of the contents of the records.

The Freedom of Information Act 2000 requires us to maintain a list (electronically) of records which have been disposed of and who authorised their disposal (see Appendix D template). Members of staff should record:

- File reference (or other unique identifier)
- File title (or brief description)
- Number of files
- The name of the authorising officer
- Date of disposal

If a record due for disposal is known to be the subject of a request for information or potential legal action **the records must not be destroyed.**

5.10 Certificate of Destruction

Under the terms of the General Data Protection Regulations (EU) 2016 (retained from EU Regulation 2016/679 EU) and Data Protection Act 2018 data must be disposed of securely and confidentially, whether done internally or by an external agency. Detailed records should be kept of the disposal or destruction of medical records and a sample form for internal use is shown at Appendix D.

6.0 MONITORING AND REVIEW OF POLICY

This policy is to be monitored in order to:

- Ensure it has been put into practice and if the policy is effective
- Verify it is being applied and complied with
- Check all elements are operating properly and the information is up-to-date
- Ensure the aims are being achieved
- Review the policy and its contents initially every two years

7.0 DOCUMENT HISTORY

Date	Author / Reviewer	Amendment(s) & Rationale	Date of Approval / Adoption
Feb 2022	Alison Hall & Rachel House	First version	
October 2025	Rachel House	Review and minor amends to incorporate introduction of G2 electronic records system and change to in-house counselling service (5.1-5.3)	Published 18/12/25

8.0 CONSULTATION

Consultation has taken place with Unison, the Federation and the Superintendents Association as the 3 main bodies representing staff and officers in the force.

Consultation has also taken place with the Information Security Manager and the Head of Legal Services to ensure all relevant legislative requirements and force policies with regard to information assurance have been taken account of.

(above consultation to be completed through circulation to the Critical Friends Group).

Appendix A

Retention Periods

The General Data Protection Regulations (EU) 2016 and Data Protection Act 2018 do not set out any specific minimum or maximum periods for retaining personal data. Instead, it says: 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'

The exact minimum retention period varies with the specific data type, and should be based on individual business needs. A judgment must be made about:-

- the current and future value of the information;
- the costs, risks and liabilities associated with retaining the information; and
- the ease or difficulty of making sure it remains accurate and up-to-date.

The table below gives an outline of documents and their period of retention.

Type of Data	Maximum retention period	Reason for length of period
Occupational Health Medical Records unrelated to a specific Health & Safety Regulation.	Keep until 6 years after the staff member leaves or 75th birthday whichever is sooner	The Records Management Code of Practice for Health and Social Care 2016 (Information Governance Alliance)
Medical records kept by the reason of COSHH	40 years from the date of the last entry	Control of Substances Hazardous to Health (COSHH) Regulations 2002
Immunisation and vaccination records	40 years from the date of the last entry	Control of Substances Hazardous to Health (COSHH) Regulations 2002
Records/documents related to any litigation	Review all records 10 years after file is closed and liaise with Legal Services on a case by case basis	The Records Management Code of Practice for Health and Social Care 2016.(Information Governance Alliance)
Scanned records relating to client care	Providing the scanning process and procedures are legally compliant* once the case notes have been scanned the paper records can be destroyed under confidential conditions	* BSI's BIP:0008 – Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically Fifth edition 2014, and The Records Management Code of Practice for Health and Social Care 2016.(Information Governance Alliance)
Equipment / instruments maintenance logs, records of service inspections	11 years after decommissioning of equipment	COSHH Regulations 2002
Complaints	Review 10 years after closure of incident (contact Legal Services for advice on a case by case basis)	The National Archives Records Management retention scheduling: Complaints records (Crown copyright 2012) The incident is not closed until all subsequent processes have ceased including litigation. The complaint must not be kept on the client's OH records. A separate file must always be maintained

Type of Data	Maximum retention period	Reason for length of period
Pre-Employment Medical Health Questionnaires including bespoke GP/Specialist reports & clinical information gathered	Form part of the Occupational Health file and retention will remain as per the entry above regarding Occupational Health Medical Records	Reference may need to be made to information disclosed on the questionnaire during the course of an individual's employment and for a period of time after employment has ceased
GP Records required for decisions relating to employment/Ill Health Retirement/H1 considerations	To be kept until the purpose for which they were required is complete	Access to the GP records may be required whilst the purpose for which they were requested is ongoing
Ill Health Retirement/H1 records	Review file 6 years after staff member leaves	The decision to keep the information for longer depends on the following : • Legal requirement; Ionising Radiation 2017/ COSHH-40yr rule/Asbestos Regs 2012/Lead at Work Regs 2002/Compressed Air Regs 1996 etc.. • Used for research • OH or Organisation defending an allegation in court
Injury Award Medical Files	The Occupational Health file will be retained whilst the individual remains in receipt of the award. GP records will be destroyed once the purpose for which they were obtained is complete	Should there be a requirement for the injury award to be reviewed; reference to the information would be required to provide an understanding as to how the original decision had been reached. Should GP records be required again at a later date, consent would be obtained to request up to date GP records
Pre-employment records for candidates who do not take up post	1 year from when Occupational Health receive notification the individual will not be taking up post	British Medical Association (BMA) 2015

Appendix B

GDPR Checklist & Decision sheet

Destruction Date
Last day of _____ 20_____

Name on File	DOB or Collar No:
Start Date	Leaving Date:
Date of last entry in notes	

OH Administrator - Please check files against the below criteria and tick the relevant boxes in the table below if **any** of the documents listed are present in the file.

		Admin Notes - initial and date	**OHA Notes**
☐	Health Records – to be retained for 6yrs or until the individual reaches the age of 75yrs (whichever date is first) **unless it contains records related to the elements marked with an*below**		
☐	* Health Surveillance (H/S) to be retained for 75yrs – NB enter date of last H/S: _____ Audio/noise exposure (**not pre-emp**), skin check, spiro/lung function print outs/results, blood lead, asbestos, radiation.		
☐	*Any Vaccination 40yrs – enter date of last vaccination administered: _____ (Retain BBV records, plus Extradition officers and DVI officers)		
☐	*Ill Health Retirement/Retirement under H1 regulation – Aged 75yrs unless in receipt of an injury award. (Check – legal advice - IOD files only retained, H1s not specified separately)		
☐	*Other – risk of litigation – Accident Form on file / request for copy of OH records in the future. Determine based on risk - minor injuries delete. Retain records of 'traumatic' or severe accidents / incidents / BBVs.		
☐	*Deceased officers and staff – delete file at 6+ years after date of death. No docs to be retained.		

OHA signature:	**Date**