Lawrence Hill Health Centre

Information Governance, Data Protection and Confidentiality Policy

Version	Date	Author	Distribution	Review date
Version 1	May 2018	E Cameron	All Staff	November 2018

Contents

1. Overview

Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. All records should meet legal and regulatory compliance and professional practice recommendations.

Health organisations need to have policies and procedures in place that ensure health records are created, managed, handled and stored securely. Lawrence Hill Health Centre endeavours to have such policies and procedures that adhere to the HORUS model:

- **Holding** information securely and confidentially
- **Obtaining** information fairly and efficiently
- **Recording** information accurately and reliably
- **Using** information effectively and ethically
- **Sharing** information appropriately and lawfully

In committing to these, Lawrence Hill Health Centre will ensure that anyone processing personal data in relation to the organisation will comply with the eight enforceable principles of good practice as indicated in the Caldicott Principles and the Data Protection Act 1998:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than necessary
6. Processed in accordance with the data subject's rights
7. Secure
8. Not transferred to countries without adequate protection

We will ensure that:

- Records are created, maintained and stored to standards which meet legal and regulatory compliance and professional practice recommendations; and
- Patients can be assured of appropriately completed health records and that all information is managed within the regulated body to ensure patient confidentiality. Information will be made available on how to access records and issues governing consent.

Everyone needs to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

The principle behind this code is that no-one shall misuse any information or allow others to.

This policy has been written to meet legal requirements and best practice guidance including:

- Data Protection Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- The Protection and Use of Patient Information (HSG 96 18)
- Caldicott Report on the Use of Patient Identifiable Information (1997)
- Freedom of Information Act 2000
- The Department of Health's guidance 'Confidentiality – NHS Code of Practice, Nov 2003

- Privacy and Electronic Communications Regulations
- Environmental Information Regulations

2. Records Management

Patient Information

Identifiable patient information is only recorded where:

- Necessary for the delivery of high quality medical care to patients either from The Old School Surgery or from other medical organisations; or
- Record retention is a regulatory requirement.

Identifiable patient data should not be used in any way to support alternative objectives such as supporting the delivery of contacts with NHS organisations, other than by way of a requirement under law to release such information.

Non-identifiable patient data, including statistics, should be used only where it has the potential to improve patient care; or is required to be released by law.

Patient information should be held in either paper or electronic form as appropriate.

The term 'Patient information' applies to all personal information about members of the public held by The Old School Surgery or a provider of services on its behalf. This includes medical records as well as 'non health' information.

Staff Information

Staff information is retained for HR purposes in both paper and electronic form.

3. Data Retention and Destruction of Records

The current recommendations from the Department of Health are contained in (HSC 1998/217: Preservation, Retention and Destruction of GP General Medical Services records relating to patients). It recommends that medical records should be retained for the following periods:

- Maternity records – 25 years.
- Records relating to children and young people (including paediatric, vaccination and community child health records) – until the patient's 25th birthday or 26th if an entry was made when the young person was 17; or 10 years after death of a patient if sooner.
- Records relating to persons receiving treatment for a mental disorder within the meaning of the Mental Health Act 1983 – 20 years after no further treatment considered necessary; or 10 years after patient's death if sooner.
- Records relating to those serving HM Armed Forces – not to be destroyed.
- Records relating to those serving a prison sentence – not to be destroyed.
- All other personal health records – 10 years after conclusion of treatment, the patient's death or after the patient has permanently left the country.

Where records are to be destroyed it should be done using a safe and reputable source and written confirmation of the destruction should be obtained and retained.

4. Access to Records – information for patients

This policy details the rights of patients to have access to their medical records. It explains the procedure for patients who request access, their rights and the action to be taken by the practice.

How requests for information should be made

Any request by an individual for access to information that we hold about them is allowable and under the new GDPR laws must be made available in 30days. Requests can be made by individuals acting on behalf of the patient, but they must declare why they have this entitlement and provide proof if required. This is generally where they have parental responsibility for a child. It may also be where an individual has been legally appointed by a Court of Protection or Guardianship order – in such circumstances seek further advice about the purpose and the details of what should be released.

The request must contain sufficient information to enable Lawrence Hill Health Centre to undertake the search required (e.g. Name, Address and Date of Birth). Lawrence Hill Health Centre is not obliged to comply with individuals' request until the requester has given you adequate information. You may wish to verify a person's identity by asking them to confirm their NHS number (if known). Further checks can be undertaken by asking the individual to produce a copy of their driving licence or credit card.

In cases where the information requested is deemed to be excessive (GDPR law makes no distinction for this so the Practice Manager will be responsible for making the decision) then a nominal fee may be charged.

The Patient's Rights

Lawrence Hill Health Centre will comply with an individual's request within calendar 30 days of receipt of the request (and the fee, if copies of the record are required). Once received, the individual is entitled to:

- Access to personal data about themselves that is held in either computerised or manual forms, from whenever the record was compiled. People have right of access to all records irrespective of when they were created, unless where permitting access to the data would be likely to cause serious harm to the physical or mental health or condition of the data subject or another person (e.g. health professional).
- A description of the data held, why the data is being processed and who has access to it (the leaflet "Your Medical Records, Protecting your Information" should be offered to explain this to patients). If more information is requested, the practice policy is to arrange for the individual to have an appointment with their GP or the practice manager.
- Lawrence Hill Health Centre will endeavour to explain data that is not intelligible. (Explanation of codes and abbreviations).
- Any information Lawrence Hill Health Centre may hold as to the source of the data if held. If information is requested by a patient, and this identifies an individual as the source of the information (e.g. a relative has provided certain information), this can only be released if that individual consents to the release, or where it is seen as reasonable to comply to the request without that individuals consent (questions regarding the duty of confidence owed to the individual must be taken into consideration).
- If the requestor is not the patient, and has an enduring power of attorney registered with the Court of Protection, they may be allowed access to information in respect of making

or processing a compensation claim. The power does not give them a general right to any information.

- Information must be supplied in a permanent form, unless this causes disproportionate effort by Lawrence Hill Health Centre or the requester agrees to the information being supplied in another form. This might apply if the printed version is very lengthy or is held in a remote archive.
- An individual who suffers damage or distress as the result of any contravention to the Act is entitled to compensation. They also have a right to ask for data to be rectified, blocked, erased or destroyed if the Courts find this data held is inaccurate.

Withholding Information
Information can be withheld, if it may cause the subject undue harm or distress if it is disclosed to them. For example where a patient is unaware of a suspected diagnosis, then they should not learn of this by reading their notes. In practical terms it will be very difficult to withhold information that might cause harm, without it being obvious that information is being withheld, which itself may well cause distress and concern. It is advised that if information that may cause harm/distress is identified, then discussion with the patient should take place about this prior to, or as part of disclosure.

Information that identifies another individual can also be withheld. If the individual is a professional involved with the patient's treatment, then this should normally be disclosed, unless to do so would put the individual at significant risk of harm. If the individual is a third party, then their identity should be protected unless they have consented to its release, or there is an overriding justification to release it without their consent. In such cases names could be blanked or substituted. Note however identity can be implied from comments or situations

If in any doubt about withholding information, please seek further support.

Special conditions
Once the request has been received you must not make any amendments or deletions to the data that would not have otherwise been made. The data must not be tampered with in order to make it acceptable.

Lawrence Hill Health Centre does not have to comply with a request where it has already complied with an identical or similar request by the same individual, unless a reasonable interval has elapsed. In deciding what a reasonable interval is you must take into consideration the nature of the data, why the data is used and the frequency with which the data is altered.

Request Form
Patients requesting information should be supplied with the Request Form below to initiate the request.

5. Information Asset Register

Lawrence Hill Health Centre maintains an Information Asset Register that identifies all types of patient and staff data this is retained and identifies how it is kept secure.

6. Data Protection

Data Protection Registration
Lawrence Hill Health Centre is registered with the Information Commissioners Office.

Data Security
Storage and Backup
Any data stored on a computer hard drive is vulnerable to the following:

- Loss due to a computer virus.
- Physical loss or damage of the computer e.g. Theft, Water damage, Fire or physical destruction, Faulty components, Software.

In particular, there is a risk of breach of confidentiality where a computer is stolen or otherwise falls into unauthorised hands.

Precautions to be taken include:

- Servers should not be used as regular workstations for any application.
- Access to servers should be authorised by senior personnel.
- A full backup must be taken every working day.
- At least 2 revolving backups with a copy taken off site at least weekly.
- Servers should be sited away from risk of accidental knocking, spillage of drinks, leaking pipes, overheating due to radiators and be inaccessible to the public.
- All computers (but not server) are to be completely shut down at the end of the working day.
- All users are allocated a system security level appropriate to their needs.
- Where a PC is standalone, ensure that important data on the hard drive is backed up regularly and any confidential data is password protected.

Protection against Viruses
Data is vulnerable to loss or corruption caused by viruses. Viruses may be introduced from CDROM/DVDROM, other storage media and by direct links via e-mail and web browsing.

Precautions to be taken include:

- Ensure virus protection software is installed on ALL computer equipment.
- Anyone discovering a virus must report this to the Senior Partner.
- All software must be purchased, installed and configured by the specialist Outsourced Provider. This includes all software packages, software upgrades and add-ons – however minor. It also includes shareware, freeware and any items downloaded from the internet.
- No document or file from any source outside the organisation can be used unless it has been scanned for viruses using the virus scanning software.
- Staff should treat email attachments that they are not expecting with extreme caution – especially if the sender is unknown. Viruses are often sent this way. If unsure what an attachment is for, or why someone has sent it, this should not be opened.
- Staff should note that intentionally introducing files which cause computer problems could result in prosecution under the Computer Misuse Act 1990.
- Staff must not violate licence agreements by making illegal copies of software. It is not permissible to download software from the internet or install from CD or disc without prior authorisation. Software licensing will be arranged and recorded as part of the

procurement and/or installation process. Any unlicensed software found on a practice PC must be deleted or disabled.

Installation of Software
Software purchases will be authorised by the Senior Partner and the specialist Outsourced Provider will supervise the loading of the software onto the system or individual PCs in accordance with the software licence.

Staff are prohibited from:

- Installing or upgrading personal or purchased software without permission.
- Staff are prohibited from downloading software, upgrades or add-ins from the internet without permission.

Internet and Email Use
All staff must use the Internet and email in a responsible manner. Inappropriate use may be subject to disciplinary or legal action.

Protection against Physical Hazards
Staff must be aware of and comply with the following:

Water

- Ensure that the PC or server is not at risk of pipes and radiators which, if damaged, could allow water onto the equipment.
- Do not place PCs near to taps/ sinks.
- Do not place PCs close to windows subject to condensation and water collection on windowsills.
- Ensure that the PC is not kept in a damp or steamy environment.

Fire / Heat

- Computers generate quite a bit of heat and should be used in a well-ventilated environment. Overheating can cause malfunction, as well as creating a fire hazard.
- Try to place the PC away from direct sunlight and as far as possible from radiators or other sources of heat.
- Normal health and safety protection of the building against fire, such as smoke alarms and CO2 fire extinguishers should be sufficient for computers. If backup tapes are kept on the premises they must be protected against fire in a fireproof safe.
- Have the wiring and plugs checked annually.
- Ensure that ventilators on computers are kept clear.
- Do not stack paper on or near computers.

Environmental Hazards

- Computers are vulnerable to malfunction due to poor air quality, dust, smoke, humidity and grease. A normal working environment should not affect safe running of the computer, but if any of the above are present consider having an air filter. Ensure that the environment is generally clean and free from dust.
- Power Supply - Protect against power surges by having an uninterrupted power supply fitted to the server.

Protection against Theft or Vandalism via Access to the Building
In addition, the following precautions should be considered to protect the building, such as:

- Burglar alarm with intruder monitor in the building.
- Appropriate locks or keypad access only, on all doors.
- Ensure any keys stored on site are not in an obvious place and any instructions regarding key locations or keypad codes are not easily accessible.
- Ensure that there is appropriate insurance cover where applicable.
- Maintain a separate record of hardware specifications of every PC in the office
- Specific precautions relating to IT hardware are:
    - Locate PCs as far away from windows as possible.
    - Clearly 'security mark' all PCs and all parts of PCs i.e. screen, monitor, keypad.
    - Have an asset register for all computer equipment, which includes serial numbers.
    - Ensure every PC is password protected.

Mobile Computing
Laptops and any other portable devices are more vulnerable than PCs, because they are easier to pick up and remove and therefore more desirable to the opportunist thief. It is also less likely, in some circumstances, that their loss will be noticed immediately. However, because of their size, it is possible to provide extra protection:

- When the device is not in use, it should be stored in a secure location.
- Where it is left on the premises overnight, it should be stored in a locked cupboard or drawer.
- Where the device is shared, have a mechanism for recording who is responsible for it at any particular time.

Computers should not be left unattended in cars. Where this is unavoidable ensure that the car is locked and the computer is out of site in the boot or at least covered up if there isn't a boot. The responsible staff member should take the device with them if leaving the vehicle for any length of time.

Where a device is being used in a Public Place it should remain with the member of staff at all times, and care should be taken to ensure that confidential data cannot be overlooked by members of the public, e.g. on public transport.

Confidentiality
Overview
This Code is intended as an overview of the issues that staff need to be aware of when using patient information within the organisation. It has been designed on advice from the Department of Health. It aims to give a brief, easy to understand advice on a very complex issue.

Everyone needs to be aware of the importance of confidentiality. This Code should help staff and providers of services on behalf of Lawrence Hill Health Centre to be aware of what is required of them.

Any personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider of the information. This is usually the patient but sometimes another person may be the source (e.g. relative or carer).

All NHS Staff are under a duty of confidence and this has long been established as common law. With the correct safeguards it need not be interpreted so strictly that, when applied there is a risk of it operating to a patient's disadvantage. This applies to those performing services on behalf of Lawrence Hill Health Centre.

Transfer of records

Overview

Patient identifiable information can be transferred by the following means:

- Post - either internal NHS or Royal Mail or other reputable 3rd party carrier;
- Fax - to and from Safe Haven fax facilities;
- N3 email - to and from .nhs.net email addresses;
- EMIS Web (which operates via secure N3 connections).

In exceptional circumstances, data may be transferred via encrypted data stick subject to the following:

- Data sticks are only to be used following explicit written consent from the Caldicott Guardian;
- Only encrypted data sticks are to be used (regardless of the purpose);
- Only the Caldicott Guardian can approve the purchase of data sticks for use.

As such, it will continue to be the case that it is not standard practice to take transfer patient or any other data away from our office on data sticks.

In order to support the safe transfer of records, Lawrence Hill Health Centre maintains the following:

- An Information Mapping Document that sets out how confidential information can be communicated either between different sites within Lawrence Hill Health Centre organisation or to third party organisation; and
- A log of all data sticks to ensure that they are all accounted for at any one time.

Breach of these policies is a serious matter and could give rise to disciplinary action being taken.

Patient Consent/Justification for Transfer

Information may be passed on where the patient has consented or where the following circumstances apply:

- If the recipient needs the information because they are concerned with the patients' care or the use can be justified for the purposes described below:
  - Assuring and improving the quality of care and treatment.
  - Monitoring and protecting public health.
  - Co-ordinating care with other agencies (e.g. local authority).
  - Effective healthcare administration (e.g. managing and planning services).
  - Auditing accounts (auditors).
  - Risk Management (e.g. health and safety).
  - Investigating complaints and legal claims.
  - Teaching.
  - Statistical analysis or research (specific consent should be sought to any activity relating to teaching or research that will involve people personally).
  - Whistle blowing.

- Statute or court order requires the information.
- Passing on information can be justified for other reasons (protection of the public).

Responsibility for Passing on Information
Individuals are responsible for their decision to pass on information. If unsure whether to pass on information ask the health professional responsible for the patient's care or a nominated senior manager.

The unauthorised passing on of patient information by any member of staff is a serious matter and may result in disciplinary action and possible legal action.

Non-identifiable Information (Anonymised)
Where anonymised information would be sufficient, identifiable information should be omitted where possible. Patient identifiable information should not be used unless it is essential for the purpose.

Interpretation
An explanation concerning the interpretation or relevance of this code should be sought from a clinical supervisor or from a Senior Manager.

Non-Compliance
Non-compliance with this code of conduct by any person employed by The Old School Surgery may result in disciplinary action being taken.

Glossary
This defines the terms used within this Confidentiality section.

Anonymised data: Data from which the recipient of the information cannot identify the patient.

Consent: Any freely given specific and informed indication of wishes by which the patient signifies their agreement to personal data relating to them being used.

Identifiable data: Data from which the patient can be identified by using any one of the following data items:
- Forename
- Surname
- Address
- Postcode
- Date of Birth
- Other dates (i.e. death, diagnosis)
- NHS Number
- Sex
- Ethnic Group

Need to Know: Only those individuals who need access to the information should have access.

By using the above transfer mechanisms, patient data can be safely transferred from referring GP practices to Lawrence Hill Health Centre and then onward from Lawrence Hill Health Centre either in the form of discharge reports or onward referral requests to primary or secondary care.

Data retention
Patient and staff records should be retained for an appropriate duration according to best practice relating to the type of information under consideration.

Information Security Events
Where a member of staff suspects or realises that there has been a breach of patient confidentiality they should immediately notify the Clinical Governance Committee and the Senior Partner.

All/any confidentiality breaches will be notified to the Commissioner in question and an action plan agreed with that Commissioner.

All/any confidentiality breaches will be investigated by the Clinical Governance Committee and reviewed by the Senior Partner.

Caldicott Guardian
A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Guardian plays a key role in ensuring that the NHS, Councils with Social Services responsibilities and partner organisations satisfy the highest practicable standards for handling patient identifiable information.

Lawrence Hill Health Centre's Caldicott Guardian is as set out in the Governance Framework Overview.

7. IT equipment

Lawrence Hill Health Centre outsources its IT requirements to a specialist provider who provides hardware, software, technical support and strategic IT advice.

Hardware
Specialist advice is taken with regard to all hardware purchases. All mobile equipment e.g. laptops are allocated to specific responsible individuals.

Software
Specialist advice is taken with regard to all software purchases.

Antivirus software is updated according to advice from technical support but this is generally more than once per year.

Communications
Lawrence Hill Health Centre has an N3 communications link which is subject to a maintenance and support agreement with BT.

Lawrence Hill Health Centre retains compliance with Information Governance requirements which has been confirmed via an IG Statement of Compliance as well as maintaining a Logical Connection Architecture that is approved by Connecting for Health.

Technical support
Specialist support is retained to ensure smooth operation of systems including remote support and emergency support for both hardware and software. Where technical support is outsourced, contractual agreements are to be put in place which not only set out the commercial terms of the relationship(s) but also ensures confidentiality regarding corporate and medical data.

User training
Staff are required to develop good IT skills and are used to working with information systems, business and office packages as required by their job roles

Disaster recovery
A business impact assessment and business continuity plans are undertaken/reviewed whenever there is a structural change in the IT infrastructure, including replacement of servers.

Daily back-ups combined with technical support that can provide a fully-configured replacement server within 48 hours comprise the key components of a disaster recovery plan.

8. Access Control Policy

System security comprises the following:

Risk Assessments
The system security requirements
Prior to implementation of strategic systems changes, a risk assessment will be undertaken to determine the security requirements given the data concerned. For example, the level and type of access controls, location of hardware associated with the system, type of data held, etc.

User Account Management
User accounts should be amended immediately upon there being a change in the staff team to ensure that all user accounts are appropriate. This could be the existence of an account of the level of information to which the member of staff has access and includes creation and removal of access rights.

The Senior Partner is responsible for ensuring that access rights are appropriate

Network Security
Lawrence Hill Health Centre ensures that its local network is protected by authentication, encryption and network connection controls which prevent unauthorised access including via wireless technology.

Secure Logon Procedures
All computer systems should have a logon procedure that includes at least a unique user ID and password. The following features should be put in place for all Lawrence Hill Health Centre systems:

- System/application identifiers are not to be displayed until the logon procedure has been successfully completed.
- Where login errors are made there should be no indication as to which part of logon information is incorrect. This prevents unauthorised users identifying patterns when attempting to gain access to systems.
- The number of unsuccessful consecutive logon attempts is limited to 3.
- There is no limit as to the maximum time allowed for any one logon. However, password protected screen savers are used prevent unauthorised use.
- The password being entered is not displayed in clear text. The systems show a number of asterisk characters.
- Passwords should not be transmitted in clear text over the network under any circumstances.

Identifying users
In order to facilitate access control and audit functions all users have unique identifiers in the form of a unique username and password combination. Group IDs are not to be used.

Password management system
A password management system should operate as follows:

- No group passwords on the system; all users will be identified as individuals (including system administrators) when they log on.
- Users should change their initial password (issued by the system administrator) following their first logon.
- The system should log user passwords and prevent re-use.
- Users should change their own passwords at least quarterly but can do so more often where they feel their current one has been compromised.
- There are to be no restrictions on the use of alphas and/or numerics in order that users can set memorable passwords and are therefore encouraged to change them frequently.
- Passwords should be stored separately from application system data.
- All passwords should be stored or transmitted using encryption or hashed.

Use of system utilities
System utilities are identified, disabled where not necessary. Access to and use of any functional system utilities is strictly controlled.

Session time-out
Timed and password protected screen savers should be used to prevent unauthorised access to data for timed-out sessions. The screen saver should be set to come on at 15 minutes or less.

Information access restrictions
File storage systems should be constructed in order to ensure all and only appropriate personnel have access to a folder which can then be viewed, altered, copied or deleted.

Data file owners are required to password protect all files which contain identifiable patient or staff data.

Sensitive system isolation

All of Lawrence Hill Health Centre systems are considered to hold sensitive data and therefore there controls apply to all systems and isolation strategies are not considered appropriate/beneficial.

9. Acceptable use of IT equipment

Prohibited Activities
Staff should not create, store, transfer (from any media or via email) or deliberately receive material that could be judged to be offensive. Offensive/inappropriate material or activities can include:

- Material that is abusive, threatening, serves to harass or bully, discriminates, encourages discrimination on racial/ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- Material that may be obscene, indecent or tasteless.
- Material that may cause distress, inconvenience or anxiety.
- Material about illegal activities, including pornography, drugs, computer hacking, militant/extremist behaviour, violence or weapons – unless it is clearly related to your professional role.

If staff receive inappropriate email or become unintentionally connected to a website, which contains offensive or inappropriate material, the member of staff should disconnect from the site immediately and inform their Line Manager.

Deliberate activities with any of the following consequences are prohibited:

- Corruption or inappropriate destruction of data
- Using equipment in a way that makes systems unavailable to others
- Wasting staff effort or computing resources
- Introducing any weakness to, or compromising IT security.

Staff should not download and/or install any software unless authorised by the Senior Partner.

User names and passwords
When staff are logged into a computer under their own username, they must either log out, 'lock' the computer or activate a password protected screensaver if they leave it.

Should staff wish to use an unattended computer where a previous user has left their access open, they must log out from that session before they commence their own session.

Staff must not disclose a personal password to anyone. A username and personal password is for one person's use only. If a member of staff thinks someone else knows their password they must change it immediately and inform the Senior Partner.

Monitoring of activity
Where monitoring of systems takes place to identify system failure/capacity problems and misuse there will not be any monitoring of individual users unless there is justification to do so from general monitoring or concerns raised.

Personal use of IT equipment

Staff can use IT equipment and facilities for personal use, provided that it is of an appropriate nature, isn't during work time, and cannot be considered as 'excessive' based on the following:
Timing of personal use:

- Staff may make personal use of email & Internet, provided that they only do so during 'unpaid' break periods, such as lunchtime, coffee break or outside of 'general work' hours.

Excessive use:

- Sending large 'attachments' (such as letters, photographs) in personal emails takes up system storage space and communication capacity that is required for practice purposes.
- Sending large numbers of personal emails especially if this is likely to stray into general work hours.
- Downloading large files from the internet.

Large files:

- Any file (or combination) that is larger than 5 Megabytes.

Any breach of this Acceptable Use Policy may be considered as misuse and an investigation may take place.

10. Freedom of Information Act 2000/Data Protection Act 1998

Lawrence Hill Health Centre supports the Freedom of Information Act 2000 in making public information available to those who request it.

We will do this by:

- Making information available to patients and for staff as appropriate upon request;
- Making sensible charges within legally acceptable parameters that are reflective of the actual cost of providing the information.

Where a patient requests access to their records or requests a copy of their records The Old School Surgery will respond in accordance with the Data Protection Act 1998 requirements.

Appendix 1. Request for Access to Health Records

Section 1. Details of Patient	
(Mr/Mrs/Miss/Ms)	2. Date of Birth
Surname	3. Current Address
Forename	
Any former names	Postcode

Section 2 Details of Records to be Accessed	
☐ Health records dated from/to:	☐ Health records relating to the following injury or condition:
☐ All health records except those relating to the following condition.	☐ All information contained on my health records from birth

Section 3 - Declaration

I declare that information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health record referred to above, under the terms of the Access to Health Records Act (1990) / Data Protection Act (1998).

- ❑ I am the patient
- ❑ I have been asked to act by the patient and attach the patient's written authorisation.
- ❑ I have parental responsibility/legal guardianship for the patient who is under age 16 and [is incapable of understanding the request][has consented to me making this request] (delete appropriately)
- ❑ I have been appointed the Guardian for the patient, who is over age 16 under a Guardianship order
- ❑ I am the deceased patient's personal representative and attach confirmation of my appointment.
- ❑ I have a claim arising from the patient's death and wish to access information relevant to my claim – the information will support my claim for the following reasons:

.....

I am aware that a charge may be payable if my request under GDPR law is deemd excessive

Signed ..... Date .....

Please note that it may be necessary to provide evidence of identity (i.e. Driving License). If there is any doubt about the applicant's identity or entitlement, information may not be released; you will be informed if this is the case.

Section 4. Internal Pre-processing Checks

Sufficient details to process application? Yes/No *[date]:* ... /... /... Signed: ……

If "No" letter sent to seek Further Information? Yes/No *[date]:* ... /... /... Signed: ……

Adequate Further Information Received Yes/No

Proceed? Yes/No

Note: Information must be provided within 40 days (21 for access to records of the deceased) of receipt of the completed application

Section 5. Administration Fee

❑ (£10.00 for computerised records) received? Yes/No [date]: ... /... /... Signed: ……

❑ (£50.00 for manual records) received? Yes/No [date]: ... /... /... Signed: ……

Section 6. Processing of Request

Name of Lead Health Professional: ……..…….

❑ Correspondence sent / contacted? Yes/No [date]: ... /... /... Signed: ……

Outcome: ❑ Appointment to be made with Lead Health Professional

made for [date]: …….. at [time]: …… Initials: ……

❑ Supervised Appointment to be made with: …… …..

made for [date]: …….. at [time]: …… Initials: ……

❑ Copies of notes to be sent

❑ Applicant advised of outcome Yes/No [date]: ... /... /... Signed: ……

Section 7. Processing Application

Access to records provided? Yes/No [date]: ... /... /... Signed: ……

Further Action: Corrections requested? Yes/No

Corrections actioned? Yes/No [date]: ... /... /... Signed: ……

Comments: