Online Safety Policy

Date First Published	**March 2024**
Version	**1**
Last approved	**March 2024**
Review Cycle	**Annual**
Review Date	**March 2025**

An academy within:

"Learning together, to be the best we can be"

1. Scope

1.1 This overarching e-Safety policy has been developed and published to outline the Nexus Multi Academy Trust commitment to a best practice approach in safeguarding children and young people from harm. Our aim is to have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.

1.2 Safeguarding children is everyone's responsibility. Everyone who comes into contact with children and families has a role to play.

1.3 Our pupils' welfare is our paramount concern. The Trust, through its defined quality assurance processes, will ensure an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

1.4 Every one of our academies is a community and all those directly connected - staff members, governors, parents, families and pupils - have an essential role to play in making it safe and secure.

2. Ethos

2.1. We believe that all our academies should provide a caring, positive, safe and stimulating environment that promotes the social, physical and moral development of each individual child.

2.2. We recognise the importance of providing an environment within our academies that will help children feel safe and respected. We recognise the importance of enabling children to talk openly and to feel confident that they will be listened to.

2.3. We recognise that all adults within the academy - including permanent and temporary staff, volunteers and governors - have a full and active part to play in protecting our pupils from harm.

2.4. We will work with parents to build an understanding of the school's responsibilities to ensure the welfare of all children, including the need for referrals to other agencies in some situations.

3. The legal framework

3.1. This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

3.2. It also refers to the DfE's guidance on protecting children from radicalisation.

3.3. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3.4. The policy also considers the computing programmes of study within individual academies and schools.

4. Roles and responsibilities

4.1 The Policy Review Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The Trust board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

4.2 All Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or academy approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

4.3 The Executive Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.4 Details of the school's Designated Safeguarding Lead (DSL) and Deputy/deputies responsibilities are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Executive Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Executive Headteacher, ICT team and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school safeguarding and child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Executive Headteacher and/or governing board

This list is not intended to be exhaustive.

4.5 The ICT team is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

4.6 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

4.7 Parents\Carers

Parents\ Carers are expected to:

- Notify a member of staff or the Executive Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the ICT systems and internet
- Parents\Carers can seek further guidance on keeping children safe online from the following organisations and websites

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

4.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

5. Educating and Supporting Children about Online Safety

5.1 Our Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

All schools:

- The safe use of social media and the internet will also be covered in other subjects where relevant.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for our SEND cohort.

5.2. When educating children within our settings we keep in mind the 4 Cs of online safety. The four Cs are "content", "contact", "conduct" and "commerce".

6. Educating Parents\Carers

6.1. The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents\carers.

6.2. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Executive Headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Cyber Bullying

7.1. Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

7.2. We help to prevent cyber-bullying by ensuring that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

7.3. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

7.4. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

7.5. The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

7.6. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

7.7. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

8. Examining Electronic Devices

8.1 The Executive Headteacher, and any member of staff authorised to do so by the Executive Headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence
- Before a search, the authorised staff member will:
- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

- Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
- When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:
- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

8.2 If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected

offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves
- If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:
- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Any searching of pupils will be carried out in line with:
  - The DfE's latest guidance on searching, screening and confiscation
  - UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
  - Our behaviour policy / searches and confiscation policy
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

9. Acceptable use of the internet in school

9.1. All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

9.2. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

9.3. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

10. Staff Using Work Devices Outside School

10.1. All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

10.2. Staff members must not use the device in any way which would violate the school's terms of acceptable use.

10.3. Work devices must be used solely for work activities.

10.4. If staff have any concerns over the security of their device, they must seek advice from the IT Team.

11. How the Trust will respond to issues of misuse

11.1. Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policies and ICT acceptable use policy. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

12. Training

12.1. All new staff members will receive training, as part of their induction, on safer internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

12.2. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

12.3. By way of this training, all staff will be made aware that:

12.3.1. Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

12.3.2. Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

12.3.3. Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

12.4. Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

12.5. The DSL and deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

12.6. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

12.7. Volunteers will receive appropriate training and updates, if applicable.

12.8. More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Review

13.1 This policy will be reviewed every year by the Policy Review Board.

Appendix

Ref No: CP38

Sheffield Children's NHS Foundation Trust

Corporate Policy

Clinical Records Management Policy

Author & Contact Person	Date Approved by Information Governance Committee	Implementation Date	Version Number	Issue Date	Review Date
Mark Talbot – Associate Director for Health Records and Patient Access	October 2022	November 2022	11	November 2022	November 2025

REQUIREMENT	ACTION
Who should be aware of the policy and where to access it	Executive Directors, Clinical Directors, Associate Directors, Heads of Departments. All staff with responsibility for clinical records.
Who should understand the policy	Executive Directors, Clinical Directors, Associate Directors, Heads of Departments. All staff with responsibility for clinical records.
Who should have a good working knowledge of the policy	All staff involved in the administration of clinical records.
Whether the policy should be included in the General Trust Induction Programme and/or departmental specific induction programme	Awareness of policy only
Where is the policy available	Trust Intranet
Copy to be sent to HR with a request for inclusion in induction documents	No
Copy to:	IT for Intranet site
Process for monitoring the effectiveness of this document	Yes, through audit.
Patient version	No
Groups/persons consulted	Information Governance Committee
Training	Via Clinical Records Committee
This policy is subject to the Freedom of Information Act	

IMPORTANT NOTICE

Due to the Independent Inquiry into Child Sexual Abuse all records should be retained until further notice. This means all clinical and corporate records in whichever format held i.e. paper or electronic.

CONTENTS

1. OBJECTIVE STATEMENT OF PURPOSE AND EQUALITY IMPACT ASSESSMENT 4

2. ROLES AND RESPONSIBILITES 4

3. RELEVANT PROCEDURAL DETAILS 6

3.1 Records Management Procedures and Guidelines 6
3.2 Registering and Creating Clinical Records 6
3.3 Clinical Record Registration 6
3.4 Restricting Access to the Register 6
3.5 Clinical Record / Episode Folder Creation 7
3.6 The Clinical Records System 7
3.7 Patient/Client Held Records 7
3.8 Tracing and Controlling the Movement of Records 7
3.9 Security and Storage of Clinical Records 8
3.10 Retrieval and Availability of Clinical Records 9
3.11 Record Retention and Disposal 10
3.12 Service Continuity and Disaster Recovery Plans 11
3.13 Patient's Rights of Access and Management of External access to clinical Records……..11

4. TRAINING FOR STAFF WORKING WITH CLINICAL RECORDS 13

5. PROCESS FOR MONITORING COMPLIANCE WITH THE POLICY 13

6. DATA LOSS OR BREACH OF SECURITY 14

7. COMPLIANCE 14

8. ASSOCIATED DOCUMENTS 14

9. REFERENCES……..14

10 VERSION CONTROL…..……..……..15

Appendix A RECORDS RETENTION SCHEDULE
Appendix B: RECORDS TRACING PROCEDURES

1. OBJECTIVE STATEMENT OF PURPOSE

1.1. A clinical record includes any information created by, or on behalf of a health professional in connection with the care of a patient. This policy applies to all staff employed by Sheffield Children's NHS Foundation Trust ("the Trust").

1.2. This policy directs the principles and practice for managing clinical records at the Trust. It sets out how clinical records will be managed within the Trust and should be read in conjunction with the Trust's Records Management Strategy. The Trust uses both electronic and paper records to support the patient processes.

1.3. This policy is based on the requirements of the Department of Health document *'Records Management Code of Practice for Health and Social Care (2021)'* in addition to taking into account the recommendations and standards set by:

- The Audit Commission
- Public Records Act 1958
- General Data Protection Regulation (GDPR) 2018
- Freedom of Information Act 2000
- National Health Service Litigation Authority Risk Management Standards
- Department of Health (DOH), Standards for Better Care
- NHS Information Authority, Information Governance Standards
- Essence of Care, Department of Health (DOH (2001)

This policy relates to all clinical records for all specialities including private patients and radiological images.

EQUALITY IMPACT ASSESSMENT

This policy applies to all Trust employees irrespective of age, race, colour, religion, belief, disability, nationality, ethnic origin, sexual orientation or marital status, carer status, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership. All employees will be treated in a fair and equitable manner.

The Trust will take account of any specific access or specialist requirements (eg BSL Interpreter, documents in large print) for individual employees during the implementation of this policy.

2 ROLES AND RESPONSIBILITES

2.1 Chief Executive

2.1.1 The Chief Executive has overall responsibility for all records management and that includes management of clinical records. As the Trust Accountable Officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and service continuity. This is integral to ensuring appropriate, accurate information is available as required.

2.2 Caldicott Guardian

2.2.1 The Trust's Caldicott Guardian has a particular responsibility for reflecting patient's interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner and provides assurance to the Trust Board that clinical records are managed in accordance with this policy.

2.3 Data Protection Officer

2.3.1 The Data Protection Officer (DPO) has a statutory responsibility and is a legal role required by the GDPR. The Data Protection Officer is responsible for overseeing implementation of data protection and security measures to ensure compliance with the GDPR requirements.

2.3.2 The DPO will advise the Trust on matters relating to Data Protection regulation and will act as a contact and advice resource for Trust staff and the public.

2.4 Freedom of Information Lead

2.4.1 The Trust's nominated Freedom of Information (FOI) Lead responsible for all requests for information in relation to the FOI Act.

2.5 Responsibility for Records

2.5.1 The responsibility for maintaining the Register of Records' will be held centrally by the Trust Information Governance lead. This officer is accountable to the Chief Information Officer for day to day operation of this register and issues arising thereof. The Head of IT is the Trust Security Officer in relation to Records Management.

2.6 Local Record Managers and Information Asset Owners (IAO's)

2.6.1 The responsibility for local records management is devolved to the relevant directors, directorate managers and departmental managers all of whom have a responsibility for the management of any clinical records (paper and/or electronic) generated by their activities in addition to ensuring that records are managed in a way that meets the aims of the Trust's records management strategy.

2.6.2 Responsibility includes the construction, storage, maintenance and destruction of casenotes. Additional responsibility is given to oversee good records management practice and promote compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information held within clinical records

2.6.3 A requirement of the Trust to support compliance with GDPR is that IAO's must provide assurance that risks associated with clinical records are being managed effectively for those assets they are responsible for.

2.7 All Trust Employees

2.7.1 All Trust staff have a responsibility to ensure that all clinical records are maintained and managed in accordance with this policy.

2.8 The Clinical Records Committee

2.8.1 The Clinical Records Committee is responsible for the control and review of this policy and associated procedures relating to clinical records. The Clinical Records Committee, through the committee Chair will advise the Information Governance Committee on this policy.

2.9 The Risk Management, Legal & Governance Department

2.9.1 The department will ensure that the risk register is populated with risks identified with regards to clinical records in accordance with the Risk Management Strategy Policy (RMS00). They will ensure incidents are investigated and reported in accordance with the Policy for the Investigation of Incidents/Complaints or Claims

(CP126) and the Policy for the Management of Serious Untoward Incidents RM01.

2.9.2 They will also ensure that this policy is reviewed in accordance with the Policy for the Development and Control of Trust Procedural Documents (CP330).

2.10 Information Governance Committee

2.10.1 The Information Governance (IG) Committee will provide board assurance that the Trust complies with relevant Trust information governance related policies as listed in the information governance policy register.

3 RELEVANT PROCEDURAL DETAILS

3.1 Records Management Procedures and Guidelines

A number of Trust procedures, guidelines and local operating procedures will support the Clinical Records Management Policy. Staff working with records will be expected to be aware of the procedures and are responsible for adhering to them. All procedures will be available on the Intranet.

3.2 Registering and Creating Clinical Records

3.2.1 The Trust will establish and maintain mechanisms through which departments and other units can register the records they are maintaining. This applies to all clinical records in the Trust. The register of record collections will be reviewed annually by the Trust Information Governance Lead and facilitate:

- The classification of records into series; and
- The recording of the responsibility of individuals creating records.

3.3 Clinical Record Registration

3.3.1 Registration is the allocation of a unique identifier to a record and the entry of that identifier in a register. This applies to all records in the Trust. The purpose of registration is to:

- Provide evidence that clinical records and documents have been created and captured into a record keeping system
- Assist subsequent tracking, retrieval of files and patient related documents.

3.3.2 Each patient is registered with a unique patient identification number of the Master Patient Index (MPI). Unit numbers can be auto-collated in sequence by the Patient Administration System (PAS). The unit number is commonly referred to as the 'hospital number' and the MPI is maintained as a core part of a Patient Administration System. The Trust currently uses several systems including Medway, SystmOne, Care Notes and RIS.

3.3.3 Each high level records collection will be registered within the Trusts Information Asset register.

3.4 Restricting Access to the Register

3.4.1 The facility to register patients will be strictly restricted to specially trained staff who need to do this on a daily basis, and who have access to adequate printing facilities. This is in order to mitigate risks connected with data quality, and availability of accurate records information. Training will be undertaken as part of the local department induction utilising Training Manuals.

3.5 Clinical Record / Episode Folder Creation

3.5.1 While the patient's Acute hospital record is held electronically, temporary episode folders are created for each inpatient attendance. Episode folders are also currently created for outpatient attendances but the elimination of the folders and direct information acquisition is part of the eDMS work programme covering the next 2 years. An Episode folder will be created according to the local prepping standard operating procedures.

3.6 The Clinical Records System

3.6.1 The Trust operates a unified clinical records system.

The definition of a unified clinical record is:

- There should be ONE set of records for each patient.
- The patient should be identifiable by using the same numbering system traceable throughout the Trust.
- There should be a standard order of filing within the Case Note folder which specialties conform to.

The principle of the unified system does not imply that all the records comprising the clinical record are physically located together. The key principle is that they use of a common patient number system ensuring that a single unique patient identifier is allocated to each patient within the Trust.

The NHS number will be the ideal reference but where this is not available at the time of registration must be followed up.

3.6.2 The objective of the system is that a patient's entire past and current written medical history is available to all clinical care practitioners involved in the patient's care. The system minimises clinical risk created by incomplete information and inadequate information sharing e.g. drugs, allergies, child protection issues.

3.7 Patient / Client Held Records

3.7.1 Allied Health Professionals (AHP) and Specialist Nursing staff may operate a patient held record system for patients attending for review. The record remains the property of the Trust (as data controller) and should be made available to the patient upon request.

3.7.2 There are advantages and associated risks with patient held records that must be acknowledged and mitigated. Risks associated with recording and relying upon important clinical information solely entered in hand held records include the information being altered or lost.

3.7.3 Whenever possible, information should be duplicated in the clinical record. This guarantees the reliability and integrity of recorded information and its authenticity. With equal importance, it also ensures the availability of that information to the Trust should it be required for the investigation of a complaint, a claim or any other purpose. The records strategy for 2019-2021 includes the digitising and merging of these records into the Trust electronic record. This will eliminate the risks associated with multiple records and record keeping.

3.8 Tracing and Controlling the Movement of Records – local records practice

3.8.1 Accurate recording and the knowledge of the whereabouts of all types of clinical records is essential if the information they contain is to be located quickly and efficiently for patient care at all times.

3.8.2 Tracking of records within a records management system is required to:

- Enable timely retrieval of the record
- Prevent the loss of records
- Monitor usage for the maintenance of systems and security
- Maintain an auditable trail of records transactions
- Support the requirements of the rights of the individual

3.8.3 It is every manager's responsibility to ensure effective measures are in place, and used properly within their area as required. The local library is registered with the central record referred to in 3.2.1.

3.8.4 Once a Case Note has been booked out from its library to an individual, that individual remains responsible for the record until it is returned to the library or re-traced to another individual.

3.8.5 Accountability of notes that are not in the tracked location is with the location and department where the notes were last tracked to. If a set of notes are tracked to an individual, but they do not have them, they will be asked to find the notes.

3.8.6 For clinical records which do not form part of the Acute site casenotes, a suitable tracing system must be used. Compliance is measured via Clinical Audit and will be reported to the Clinical Records Committee.

3.8.7 Any requests for clinical records to be taken outside the trust must be:

- Made by a Trust clinician who is responsible for the collection, transport, safekeeping and return of the notes.
- Via a subject access request route, e.g. disclosure of notes to the patient, the patient's representative or at the request of the courts or other agency.

3.9 <u>Security and Storage of Clinical Records</u>

3.9.1 Responsibilities for safe storage/loss of records:

The manager for the area is responsible for ensuring the effective and efficient operation of current and non-current storage facilities for records within their department, including the safe-keeping, accessibility and environmental storage of records.

Storage arrangements must protect against unauthorised access of patient information. Areas and libraries housing Clinical Records should have the following features:

- suitably access control systems
- safe storage of keys

Clinical Records must also be maintained in a way which prevents unauthorised access, destruction, alteration or removal. All rooms housing records (including offices) must be locked when left unattended. (See also the Information Security Policy / Data Protection Regulation).

Irretrievable loss of any record must be reported by completing an incident report form in accordance with the Trust's Incident Reporting Procedures (see Policy for the Investigation of Incidents/Complaints and Claims CP126 and Policy for the Managing of Serious Untoward Incidents RM01).

3.9.2 Protection against fire

An adequate fire protection system including both detection and alarm must be in place in libraries or other such areas where large quantities of records are permanently housed. Records should be stored within a structure able to withstand fire for a minimum of 30 minutes. Where sprinkler or drencher systems are installed they should dispense an appropriate media that will not cause harm to paper records but will put out fires either in paper or other media. Specific advice can be sought from the Trust's Fire Officer.

3.9.3 Protection against water

Areas where records are stored must be safe from risk of water damage or high humidity. Basement areas and attics are particularly susceptible to ingress of water, are high risk and if at all possible should be avoided for the storage of records.

3.9.4 Environment for storage of paper

Clinical records kept in dedicated record storage facilities should have a visual check for signs of damage and/or degradation and be flagged with the relevant library managers where any occurrence is found.

In libraries and larger stores, lighting should provide a minimum illumination of 100 lux at floor level in order to meet health and safety requirements. A secondary automatic light system, independent of the normal supply, should ideally be provided for use in an emergency. Other emergency lighting, such as torches in each storage area, should also be available.

Microfilm records should be stored in accordance with BS 1153, *Processing and storage of silver-gelatin-type microfilm.*

3.9.5 Shelving and boxing

Records in dedicated records storages should be stored off the floor to provide some protection from flood, dampness and dust.

The width of aisles and general layout of storage areas must conform to fire, health and safety, and similar regulations.

3.10 Retrieval and Availability of Clinical Records

3.10.1 Central Clinical Record Libraries

Access to Clinical Records Libraries should be restricted to authorised personnel only and managed in line with the Policy for Access to Medical Records and Records Security. Clinical Records stored off the main site are stored within sub libraries overseen by administrative and clerical staff, who are responsible for ensuring access to the records does not contravene the Trust's Code of Practice for Safeguarding Patient Information.

3.10.2 Off-site Storage

Wherever possible, records should be stored on Trust premises and under the Trust's direct control. Where storage with contractors is unavoidable, records must be stored at least to standards equal to our own, and must include an adequate business continuity plan. When setting up contracts and tenders, this must be taken in to account by both Managers and the Procurement Department. This must be documented via the privacy impact assessment.

3.10.3 Availability of Records

Trust staff have a responsibility for ensuring Clinical Records are stored in a manner that allows the record to be retrieved promptly 24 hrs a day, 365 days per year for patient treatment by those properly authorised to do so.

Attention must be paid to ensure that security arrangements allow staff who may require records for an emergency admission to gain access to any area where Clinical Records are stored.

3.10.4 Removal of Records from Trust Premises

Records – paper or records held on digital devices must only be taken out of the hospital by members of staff where their work necessitates home visits or for clinics in geographically dispersed areas. Records should not be left unattended at any time and must never be left unattended in cars. Access to digital notes over the web is controlled by IT in a password protected and encrypted environment.

3.10.5 Case Note Transfer of Clinical Records to Other Healthcare Providers

The Trust must ensure that an individual's Clinical Record is available in the event of an emergency admission, 365 days a year, 24 hours a day.

Original records will only be transferred to other healthcare providers in the area, where there is a reciprocal operational arrangement in place that guarantees their return in emergency circumstances within one hour. In all other circumstances photocopied or digital records will be supplied and original records retained.

Requests for copies of records from other healthcare providers should be dealt with by following the Trust's 'Subject Access' process.

3.10.6 Records required for Research and Audit projects

Paper Clinical Records required specifically for Research purposes, must be obtained via the managers of the individual libraries

Staff requiring records for Clinical Audit or Service Evaluation must have their project approved and registered by the Quality and Standards, Legal and Governance Department and must complete a privacy impact assessment.

3.11 Record Retention and Disposal

3.11.1 Records retention and disposal will be controlled in accordance with the current Department of Health guidance on records storage which can be accessed via the Department of Health website www.dh.gov.uk/publications.

3.11.2 Retention and Disposal of Clinical Records

Clinical Records for Children and Young People should be retained **'Until the patient's 25th birthday or 26th if young person was 17 at conclusion of treatment; or 8 years after patient's death if death occurred before 18th birthday'.** This schedule identifies the minimum retention period.

The decision to NOT scan a patient's clinical record(s) will be made by the Head of Legal and Governance for any litigation case. For Clinical Records where a decision has been made to not scan or destroy will be clearly marked on the front cover:

'PLEASE DO NOT ARCHIVE - PLEASE CONTACT LEGAL & GOVERNANCE'.

The destruction of original clinical records shall only be done with the authority of the Information Governance lead and in accordance with the Procedure for the Destruction of Records policy (CP1503).

http://nww.sch.nhs.uk/Health%20Services%20Management%20-%20SCH/documents/corporate/CP1503_Procedure_for_the_Destruction_of_Records.pdf

All clinical records in the Trust will be managed in accordance with this procedure.

3.12 Service Continuity and Disaster Recovery Plans

3.12.1 The responsibility for emergency preparedness and response to potential disasters involving/affecting clinical records is an integral part of each holding department's business continuity plan. These plans will be periodically risk assessed and updated as necessary to ensure that risk of loss or destruction is kept to a minimum.

3.12.2 If the Trust is taken over by another organisation then responsibility for safe and secure records management arrangements will transfer to that organisation.

3.13 Patient Rights of Access and Management of External Access to Clinical Records

3.13.1 Facilitated access to clinical records must be commensurate with its content and its business use. Further information can be found in the 'Code of Practice – Release of information'.

3.13.2 In accessing clinical records within the Trust, it is imperative that all staff will have regard to the following:

General Data Protection Regulation (2018)

The GDPR applies to the processing of data relating to living EU citizens regulates the use of personal data when, on its own or in conjunction with other information, enables a living individual to be identified. Key principles within the legislation ensure that data is processed fairly and lawfully, is only used for a legal purpose, is accurate, is only retained for as long as is necessary for its primary purpose of collection and appropriate security measures are in place to protect that particular data.

Common Law Duty of Confidentiality
The general principle in common law duty of confidentiality is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the data subject's consent.

Sharing confidential information without consent will normally only be justified in the public interest in the following circumstances:

- when there is evidence that the child or vulnerable adult is suffering or is at risk of suffering significant harm or
- where there is reasonable cause to believe that the child or vulnerable adult is suffering or is at risk of suffering significant harm or
- to prevent serious crime, i.e. significant harm, arising to children and young people or serious harm to adults, including through the prevention, detection and prosecution of serious crime.

Working Together 2006 states that:
In deciding whether there is a need to share information, professionals need to consider their legal obligations, including whether they have a duty of confidentiality to the child.

Where there is such a duty, the professional may lawfully share information if the child consents, or if there is a public interest of sufficient force. The professional must judge this, based on the facts of each case.

Where there is a clear risk of significant harm to a child, or serious harm to adults, the public interest test will almost certainly be satisfied. However, there will be other cases where practitioners will be justified in sharing some confidential information in order to make decisions on sharing further information or taking action. The information shared should be proportionate. Decisions in this area need to be made by, or with the advice of, people with suitable competence in child protection work such as Named Doctor or Named Nurse for Child Protection, or senior managers. For further information, consult the Trust Policy for the Safeguarding of Children and Vulnerable Adults.

The Access to Health Records Act 1990

The Access to Health Records Act 1990 applies to records of deceased patients and only applies to records created since 1 November 1991. The Act allows access to the deceased's personal representative to enable them to carry out their duties and to anyone who has a claim resulting from the death. This is not a general right of access and the right of access is a restricted right when there is evidence the deceased did not wish for any part of their information, or if disclosure of the information would cause serious harm to the physical or mental health of any person or disclosure would identify a third person who had not consented to that disclosure.

Human Rights Act 1998

Article 8 of the Human Rights Act 1998 states that any living individual is entitled to (especially applicable with regard to records management) the right to respect for their family life, private life, their home and correspondence. However the right is not absolute and provisions are made for interference with those rights in some circumstances. If the Trust complies with the requirements set out in the Data Protection regulation and the common law duty of confidentiality, the requirements of Article 8 will be met.

Caldicott Report

The original Caldicott Report, in 1997, highlighted six principles for NHS organisations to adhere to in order to protect patient information and confidentiality. They are:

- Justify the purpose.
- Don't use patient identifiable information unless it is necessary.
- Use the minimum necessary patient-identifiable information.
- Access to patient identifiable information should be on a strict need-to-know basis.
- Everyone with access to patient identifiable information should be aware of their responsibilities.
- Understand and comply with the law.

A review of the Report (Information: To Share or Not to Share), in 2013, made further recommendations, including one further principle:

- The duty to share information can be as important as the duty to protect patient confidentiality.

Freedom of Information Act 2000

The Freedom of Information Act 2000 lays down requirements for the Trust, as a public body to keep and make information available on request. The essence of the Act allows for a general right of access to recorded information held. The aforementioned right of access is subject to certain conditions and exemptions.

In general, patient identifiable information is not normally subject to disclosure to third parties, however in case of doubt, enquiries should be directed to the Information Governance Lead who will consult with the Caldicott Guardian and the Freedom of Information (FOI) Lead. (See also the Non Clinical Records Policy relating to FOI and access to records)

Formal requests from third parties or patients for copies of Clinical Records must be directed in writing to:

Data Protection Officer
Sheffield Children's NHS Foundation Trust
Western Bank, Sheffield, S10 2TH

4 TRAINING FOR STAFF WORKING WITH CLINICAL RECORDS

4.1 It is essential that staff working with Clinical Records are made aware of the key principles within this Policy at induction, notably in respect of confidentiality and data protection. Managers are responsible for local departmental induction training for all staff, part of which must include local operational records procedures.

5 PROCESS FOR MONITORING COMPLIANCE WITH THE POLICY

5.1 The Board seeks independent assurance that an appropriate and effective system of managing records is in place and that the necessary levels of controls and monitoring are being implemented

5.1.1 The Trust Board obtains assurance about the management of all clinical and non-clinical records from the Information Governance Committee.

5.1.2 The Clinical Records Committee will monitor policy and procedure compliance (see monitoring table below) to ensure that records systems and procedures are implemented according to organisational requirements and meet anticipated outcomes. The Clinical Records Committee is responsible to the Information Governance Committee.

5.2 The regulatory environment requires that the following external accreditation standards are used to monitor and audit the performance of the Trust's Clinical Records management policies and processes.

Standards used as the Trust's performance indicators:

- NHSLA Risk Management Standards
- Health Care Standards
- Data Accreditation Standards
- The Audit Commission Standards

5.3 The Clinical Records Committee will monitor the effectiveness of this policy by reviewing information sets including:

- Summary of incidents
- Summary of failure to track records
- Storage requirements
- Proforma Approval

And in addition by using the monitoring table below:

Minimum requirements to be monitored	Process for Monitoring	Responsible Individual/ Committee	Frequency of Monitoring	Responsible Committee For Review of Results	Responsible Individual /Committee For Development of Action Plan	Responsible Committee for Monitoring of Action Plan
Duties	Audit	CRC	Annual	CRC	CRC	IGC
Legal obligations that apply to records	Review of Policy	CRC	3 yearly	CRC	CRC	IGC
Process for tracking records	Audit	CRC	3 yearly	CRC	CRC	IGC
Process for creating records	Audit	CRC	3 yearly	CRC	CRC	IGC
Process for retrieving records	Audit	CRC	3 yearly	CRC	CRC	IGC
Process for retention, disposal and destruction of records	Refer to the Procedure for the Destruction of Records					

CRC = Clinical Records Committee
IGC = Information Governance Committee

6 DATA LOSS OR BREACH OF SECURITY

Any breach of confidentiality be that through loss or disclosure of Information Technology or paper health or social care records, constitutes an incident which must be reported in accordance with the Policy for the Investigation of Incidents/Complaints and Claims CP126 and Policy for the Managing of Serious Untoward Incidents RM01.

7 COMPLIANCE

Non-compliance with the requirements of this policy and associated policies relating to confidentiality of information, information security and freedom of information duties may result in disciplinary action.

8 ASSOCIATED DOCUMENTS

Policy for the Investigation of Incidents/Complaints and Claims CP126 Policy for the Managing of Serious Untoward Incidents RM01. Procedure for the Destruction of Records CP1503

9 REFERENCES

- Public Records Act 1958
- General Data Protection Regulation (GDPR) 2018
- Information Governance Framework
- Common law of Confidentiality
- Access to Health Records Act 2000
- Records Management Code of Practice 2021
- Freedom of Information Act 2000
- Human Rights Act 1998

10 Version Control

Version	Date	Author	Status	Comment
10	November 2018	Mark Talbot	Archived	Updating and removal of references and local medical records processes (several of the appendices) with the introduction of EDMS. Appendices removed: • Appendix A – Terms of Reference – Clinical Records Committee • Appendix C – Casenote Electronic Tracking – Filefast quick reference guide • Appendix D – Policy for Access to the Medical Records Library and Records Security • Appendix E – Code of Practice for safeguarding patient information – to become a separate document. • Appendix F – Duplicate Records – Creation and Reconciliation Procedure Policy updated to reflect the wider clinical records functions across the Trust. Retention schedules removed and replaced with hyperlink to NHS Digital website. Updated to include references to General Data Protection Regulation (GDPR) 2018.
10.1	July 2021	Mark Talbot	Archived	Minor amendment to Appendix 2 to provide clearer update to saving of emails.
11	October 2022	Mark Talbot	Approved	Update to version number and review date.

APPENDIX A

CLINICAL RECORDS RETENTION SCHEDULE

At the time of writing, the Independent Inquiry into Child Sexual Abuse (IICSA) chaired by Hon. Dame Lowell Goddard has requested that large parts of the health and social care sector **do not destroy** any records that are, or may fall into, the remit of the inquiry.

Investigations will take into account a huge range of records which may include, but are not limited to, adoption records, safeguarding records, incident reports, complaints and enquiries. Outside of this inquiry, it is also important to consider that these records are likely to require longer than the standard retention periods given in this Code. Before any records are destroyed you are advised to check for any further update from the inquiry website at www.iicsa.org.uk.

The '*Records Management Code of Practice for Health and Social Care 2016'* includes the retention schedule that details a **Minimum Retention Period** for each type of health record. Records (whatever the media) may be retained for longer than the minimum period.

However, records should not ordinarily be retained for more than 30 years. Where a retention period longer than 30 years is required (eg to be preserved for historical purposes), or for any pre-1948 records, The National Archives (see note 1 below) should be consulted. Organisations should remember that records containing personal information are subject to the Data Protection Regulation 2018.

The following types of record are covered by this retention schedule. This includes the function and the format of these records:

Function:

- Patient health records (electronic or paper-based, and concerning all specialties, including GP medical records);
- Records of private patients seen on NHS premises;
- Accident & Emergency, birth and all other registers;
- Theatre registers and minor operations (and other related) registers;
- X-ray and imaging reports, output and images;
- Integrated health and social care records
- Data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes. This can include data for service management, research or for supporting commissioning decisions.

Format:

- Photographs, slides and other images including biometrics and genetics;
- Microform (ie microfiche/microfilm);
- Audio and video tapes, cassettes, CD-ROMs, etc;
- E-mails that are of clinical relevance to the patient;
- Computerised records; and
- Scanned documents
- Text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient) such as Twitter and Skype
- Websites and intranet sites that provide key information to patients and staff.
- Any patient related discussions must be entered into the patient record including any information received by letter or secure e-mail.

Full details of the '**retention schedules**' can be found here:

Records Management Code of Practice 2021 - NHS Transformation Directorate (england.nhs.uk)

APPENDIX B

RECORDS TRACING PROCEDURE

In order to locate clinical records in a timely fashion and to reduce the number of missing notes, it is essential that tracing of all notes is as accurate as possible. It is crucial that records are tracked on their journey around the Trust. This procedure document is designed to ensure that notes are tracked and that all documentation reflects a true and auditable record.

Local casenotes (i.e. not part of the main patient clinical record) are sometimes requested by employees of the Trust. These local casenotes need to be tracked to the requesting locations. The casenotes are to be tracked in and out of local departments using a tracer card or a tracker book system.

Tracing Procedure

Casenotes are requested from the local library and are tracked out by entering into a tracker book/card. The tracker book/card must be completed by filling in the following:

- Patient Name – Surname and First Name
- Hospital Number
- Date booked out
- Date booked in (once casenote returned)
- Tracked to location

Each tracking book must be an A-Z A4 book and each page prepared as detailed below.

Patient Surname and First Name	Hospital Number	Date Booked Out	Date Returned	Tracked To Location
Smith John	123456	01.04.09		Joe Blogs – Risk Mgment
Jones Helen	654321	03.04.09	04.04.09	Dr Briggs – S3

The front of the book must be clearly labelled with the location of where the casenotes are stored within the department. The start date of the book must be clearly visible.

If any alphabetical sections of the book become full, the front label must be completed with the finish date, a new book must be started and all current casenote information must be transferred to the new book. **The A-Z tracking books will be provided by the local departments and must be stored within the department and kept for a minimum of 6 months for audit purposes and then destroyed as per the Trust destruction process.**

Upon return of the casenote, the tracking book/card “date returned” section in the book is completed.

PLEASE ENSURE THAT ALL WRITING IS CLEAR AND LEGIBLE.