Sheffield Children's NHS
NHS Foundation Trust

Becton School
Together We Can

ONLINE SAFETY POLICY (E-SAFETY)

Date Published	**November 20**
Version	**1**
Approved Date	**November 20**
Review Cycle	**1 year**
Review Date	**November 21**

An academy within:

nexus Multi Academy Trust
Learning together to be the best we can be

Contents

Becton School

Online Safety Policy

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group / committee made up of:

- Headteacher / Senior Leaders
- Online Safety Coordinator
- Governors / Board

Consultation with the whole school has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Headteacher:	*November 2020*
The implementation of this Online Safety policy will be monitored by the:	*Online Safety Coordinator – Mel Kilner*
Monitoring will take place at regular intervals:	*Annually*
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*September 2021*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, Safeguarding Governor LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the *school* (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the *school.*

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the *school*, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the *school.*

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the *Governing* has taken on the role of *Online Safety Governor*. The role of the Online Safety *Governor* will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

Headteacher and Senior Leaders

- The *Headteacher* has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Online Safety Lead*.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority / MAT / other relevant body* disciplinary procedures).
- *The Headteacher/ Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.*
- *The Headteacher/ Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.*

Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

Network Manager / Technical staff

The Network Manager is responsible for ensuring:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the *school* meets required online safety technical requirements and any *Local Authority* Online Safety Policy / Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- *the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the *network / internet / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher/ Senior Leader; Online Safety Lead* for investigation / action / sanction
- *that monitoring software / systems are implemented and updated as agreed in school policies*
- Makes clear that staff accessing NHS systems do so in accordance with any corporate Sheffield Children's Hospital policies (see policy in appendices);

Teaching and Support Staff

Are responsible for ensuring that:

- **they have an up to date awareness of online safety matters and of the current *school* Online Safety Policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the *Headteacher /Senior Leader; Online Safety Lead* for investigation / action / sanction**
- **all digital communications with students / pupils / parents / carers should be on a professional level *and only carried out using official school systems***
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming

- online-bullying

Online Safety Group

The Online Safety Group provides a consultative group that has representation from the *school* community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. This group is part of the safeguarding group. The group will also be responsible for regular reporting to the *Governing Body.*

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- *the production / review / monitoring of the school filtering policy and requests for filtering changes.*
- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

Students / Pupils:

- **are responsible for using the *school* digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's* Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, letters, website and information about national / local online safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student / pupil records
- *their children's personal devices in the school (where this is allowed)*

Community Users

Community Users who access school systems / website as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / pupils* in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned online safety curriculum should be provided as part of PHSE lessons and should be regularly revisited**
- **Key online safety messages should be reinforced as part of a planned programme of tutorial / pastoral activities**
- **Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- **Students / pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.**
- *Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school*
- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site,*
- *Parents / Carers evenings / sessions*

- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)*

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's / academy's online safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and online safety*
- *Online safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school website will provide online safety information for the wider community*

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.**
- **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.**
- *It is expected that some staff will identify online safety as a training need within the performance management process.*
- *The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from CEOP / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The Online Safety Lead (or other nominated person) will provide advice / guidance / training to individuals as required.*

Training – Governors / Directors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- **Attendance at training provided by the Local Authority / MAT / National Governors Association / or other relevant organisation.**
- **Participation in school training / information sessions for staff or** parents.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (*at KS2 and above*) will be provided with a username and secure password by *Code Green who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (e.g. school safe)
- Code Green are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet
- *The school has provided enhanced / differentiated user-level filtering*
- *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place regarding the extent of personal use that users (staff / students / pupil's / community users) and their family members are allowed on school devices that may be used out of school.*
- ***Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured***. (

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices

including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device [1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes – To be handed in at the beginning of the day*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*No*	*No*	*No*
No network access				*No*	*No*	*No*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.

- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Students / Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	Y						Y	
Use of mobile phones in lessons		Y					Y	
Use of mobile phones in social time	Y			Y				
Taking photos on mobile phones / cameras		Y					Y	
Use of other mobile devices e.g. tablets, gaming devices		Y		Y				
Use of personal email addresses in school , or on school network		Y		Y				
Use of school email for personal emails		Y					Y	
Use of messaging apps			Y	Y				
Use of social media			Y	Y				
Use of blogs			Y	Y				

When using communication technologies, the school considers the following as good practice:

- The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. *Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).*

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, etc.) must be professional in tone and content. *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use.*
- *Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority / MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under school disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school permits reasonable and appropriate access to private social media sites*

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school /academy context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X

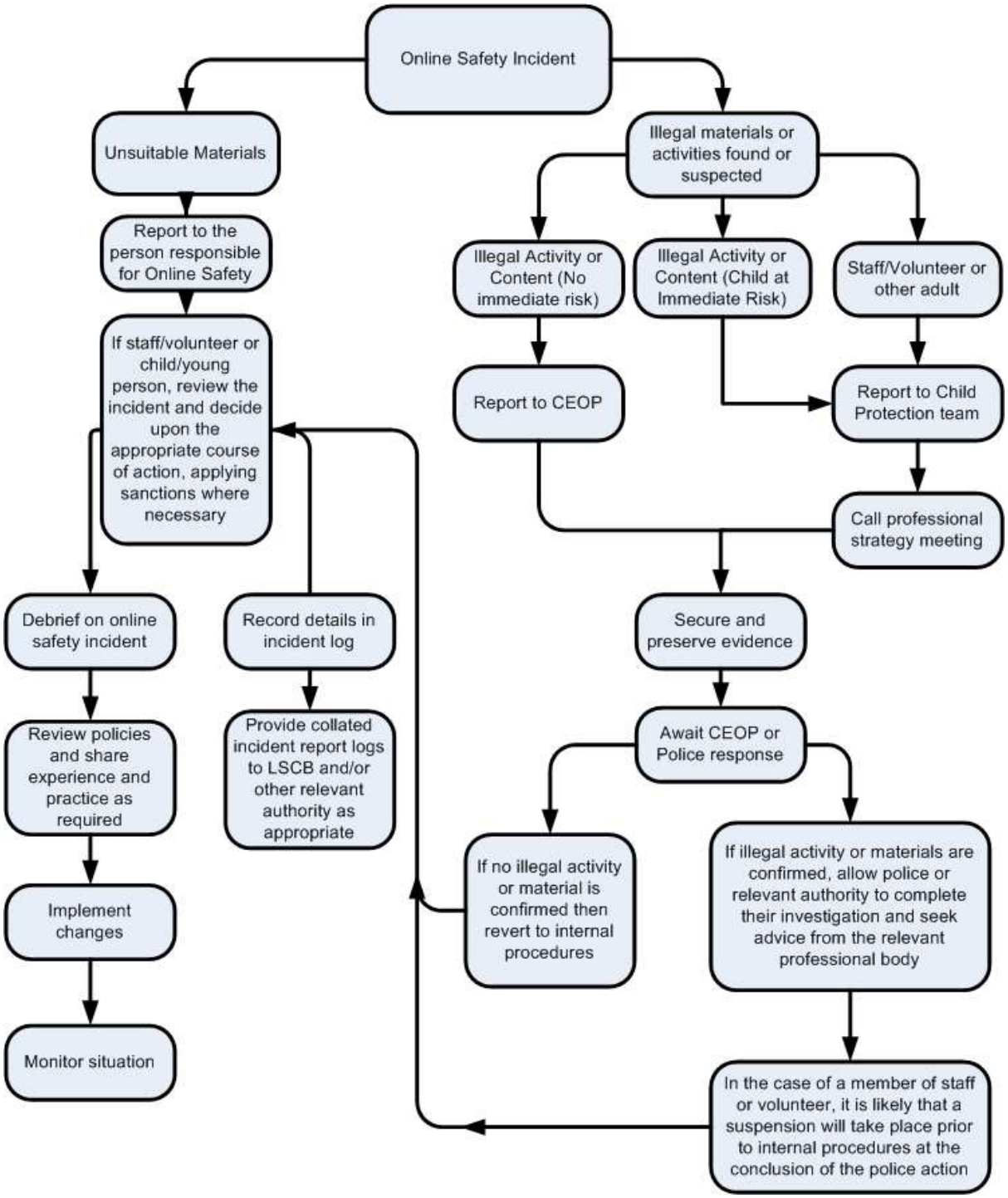
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non-educational)		X				
On-line gambling				X		
On-line shopping / commerce		X				
File sharing		X				
Use of social media		X				
Use of messaging apps			X			
Use of video broadcasting e.g. YouTube		x				

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X	X	X		X	X	X	X	X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X		X	X	X	X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X	X		X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X		X	X	X	X	X
Allowing others to access school network by sharing username and passwords	X	X	X		X	X	X	X	X
Attempting to access or accessing the school network, using another student's / pupil's account	X	X	X		X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X	X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	X	X	X

Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

Actions / Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	X	X			X	X		
Unauthorised downloading or uploading of files	X	X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X	X		X	X	X	
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X	X		X	X		
Deliberate actions to breach data protection or network security rules	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X		X	X		
Actions which could compromise the staff member's professional standing	X	X	X		X	X	X	

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X	
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X		X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X		X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

Appendices

Student / Pupil Acceptable Use Agreement

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the *school* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission
- I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the *school* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student / Pupil Acceptable Use Agreement Form

This form relates to the *student / pupil* Acceptable Use Agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems

I have read and understand the above and agree to follow these guidelines when:

- I use the *school* systems and devices (both in and out of school)
- I use my own devices in the *school* (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, website etc.

Name of Student / Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

Student / Pupil Acceptable Use Policy Agreement for younger pupils

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): .....

Parent / Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the *Student / Pupil* Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name: .....

Student / Pupil Name:.... .....

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Acceptable Use Policy
Accessed by school staff
Stored in pupil folder
Stored for the duration of time that the pupil is on roll + 1 month
Shredded when pupil has come off-roll

Signed: .....

Date: .....

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. *Students / Pupils* and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publically shared by any means, only your child's first name/initials will be used.

The school will comply with the Data Protection Act and request parent's / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree.

This form (electronic or printed)	The images
This form will be accessed by authorised staff at Becton School.	The images may be published. on Twitter, the school website or the local press,
This form will be stored as an electronic copy in the pupil file	The images will be accessed by authorised staff at Becton School. .
This form will be stored for the period in which you are involved with Becton School +1 month	The images will be stored as an electronic file in the secure staff area of the network
This information will be deleted from the Electronic records.	The images will be stored for the period in which you are involved with Becton School +1 month
	The images will be deleted from the server
	A request for deletion can be made to the Head Teacher

Digital / Video Images Permission Form

Parent / Carers Name:.....Student / Pupil Name:.....

As the parent / carer of the above student / pupil, I agree to the school taking digital / video images of my child / children.	Yes / No
I agree to these images being used:	
• to support learning activities.	Yes / No

• in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
Insert statements here that explicitly detail where images are published by the school	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: .....

Date: .....

Student / Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the Student / Pupil Acceptable Use Agreement.

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion,

promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school) systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

This form will be accessed by authorised staff at Becton School.
This form will be stored as an electronic copy in the pupil file
This form will be stored for the period in which you are involved with Becton School +1 month

This information will be deleted from the Electronic records.

Name: ..... Signed: .....

Date: .....

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

Becton would like to thank SWGFL for their support in the creation of this document

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	November 2018	November 2018	10	November 2018	November 2021

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	Clinical Records Committee Information Governance Committee Staff Side Executive Risk Management 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

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 (2016)'* 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. The IG Committee receives the minutes of the Clinical Records Committee and any escalated issues as necessary.

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 Security and Storage of Clinical Records

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
- NHS Code of Practice: Records Management
- Freedom of Information Act 2000
- Human Rights Act 1998

10 Version Control

Version	Date	Author	Status	Comment
8.4	January 2014	Peter Crowther	Archived	Addition of 3.13.2.

9	October 2014	Peter Crowther	Archived	Procedure for Disclosing Copies of Health Records removed from appendix (was B) as now dealt with via Subject Access Policy and Freedom of Information Policy. Small amendment to 3.10.1 regarding key storage. Amendments to 3.7 (Cross Referencing) to reflect increased use of FileFast across Trust. Terms of Reference for Clinical Records Committee (Appendix A) updated. Removed Organisation Chart (was C), as out of date. Plus minor updates and amendments.
10	November 2018	Mark Talbot	Approved	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.

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.

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

https://digital.nhs.uk/binaries/content/assets/legacy/excel/o/o/rmcop-retention-schedules.xls

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.