NHS
Cheshire and Wirral
Partnership
NHS Foundation Trust

Document level: Trustwide (TW)
Code: SOP20
Issue number: 1.1

Decommissioning Premises (Moves and Closures)

Lead executive	Medical Director
Authors details	Trust Records & Information Governance Manager 01244 397384

Type of document	Standard Operating Procedure
Target audience	All CWP staff
Document purpose	To provide staff with guidance to ensure that when Trust buildings are part or fully closed or services relocated, they are fully cleared of all items, including confidential information, IT equipment and furniture and office equipment and left safe, clean and tidy.

Approving meeting	Information Governance & Data Protection Sub-Committee	Date 22-Jan-20
Implementation date	22-Jan-20	

CWP documents to be read in conjunction with	
HR6 IM7 SOP16 EP10	Mandatory Employee Learning (MEL) policy Confidentiality policy Archiving records with Dataspace Information Security Incident Response Plan

Document change history	
What is different?	Policy recoded in line with policy library reshape
Appendices / electronic forms	N/A
What is the impact of change?	N/A

Training requirements	No - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Clinical representatives of the Information Governance & Data Protection Sub-Committee
Corporate services	Corporate representatives of the Information Governance & Data Protection Sub-Committee
External agencies	N/A

Financial resource implications	None

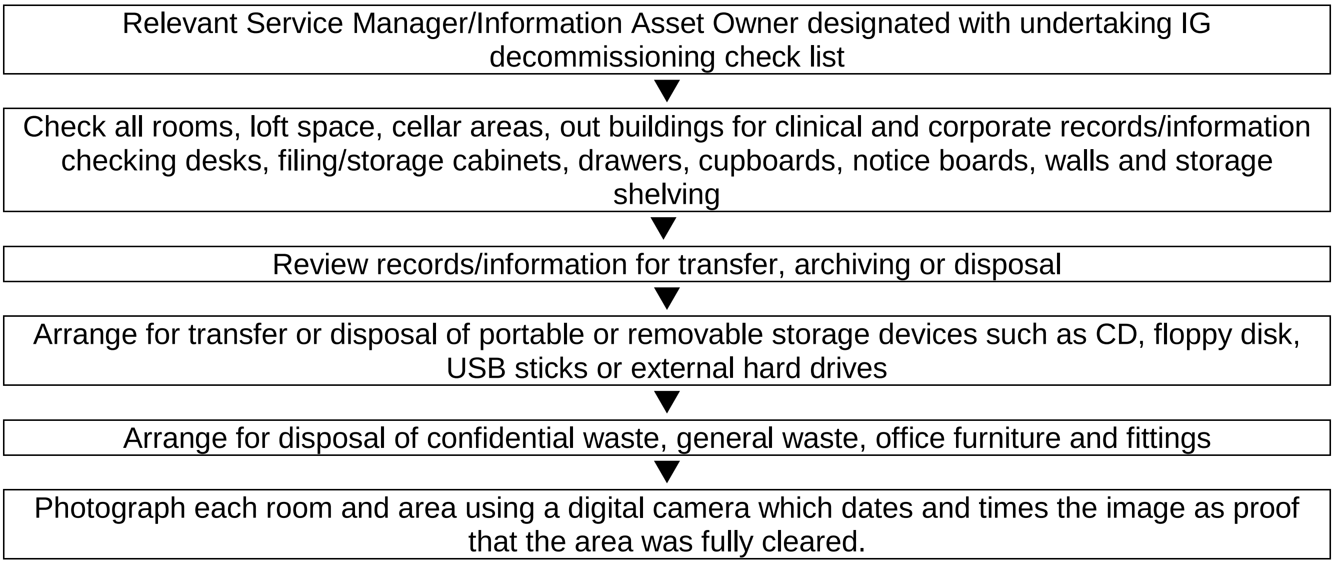
External references

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable? N/A		
Is the impact of the document likely to be negative? - If so can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A N/A N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	N/A	
What is the level of impact?	N/A	

Contents

Quick reference flowchart for vacating buildings information governance procedure

For quick reference the guide below is a summary of actions required.



Relevant Service Manager/Information Asset Owner designated with undertaking IG decommissioning check list

Check all rooms, loft space, cellar areas, out buildings for clinical and corporate records/information checking desks, filing/storage cabinets, drawers, cupboards, notice boards, walls and storage shelving

Review records/information for transfer, archiving or disposal

Arrange for transfer or disposal of portable or removable storage devices such as CD, floppy disk, USB sticks or external hard drives

Arrange for disposal of confidential waste, general waste, office furniture and fittings

Photograph each room and area using a digital camera which dates and times the image as proof that the area was fully cleared.

1. Introduction

This standard operating procedure is to provide staff with guidance to ensure that when Trust buildings are part or fully closed or services relocated, they are fully cleared of all items, including confidential information, IT equipment and furniture and office equipment and left safe, clean and tidy.

Decommissioning impacts on patients and staff and therefore requires a formal decommissioning process which ensures compliance with the principles of Data Protection Legislation. In particular the Trust must ensure the protection of all information assets, keeping them safe, secure and confidential at all times. The Senior Information Risk Owner (SIRO) is accountable for the Trust's Information Risk Management. The SIRO must have assurance that we undertake formal processes for the decommissioning of our services and properties. The end to end process must be fully risk assessed and consider the controls and assurance for all aspects of the activities involved, with specific focus on the protection of all information assets and property management functions. These actions will prevent future serious data breaches and leave the building safe and secure.

2. Scope

This procedure is applicable to all staff, including contractors, temporary / agency staff and volunteers that are involved with the following:

- Full or part closure of buildings
- Services or departments moving to new premises
- Moving within a building
- Transfer of services to a new provider (Remaining at original site or relocating to new premises)
- Termination of services i.e. services disbanded and not being re-commissioned (Contracts include exit plans and form part of the contract)
- Disposing of equipment no longer required in a building.

This procedure will also be relevant to Space Utilisation projects and Service Transformation projects.

3. Definitions

Decommissioned
Planned closure of a building, department / service or ward area from operation or use including redundant (no longer used or required in the location) IT equipment and office furniture.

Information Asset
An information asset can be defined as an operating system, infrastructure, business application, off-the-shelf product, user-developed applications, records and information. It will have recognisable and manageable value, risk, content and lifecycles and can range from a basic Excel spread sheet or database to a national system.

An Information Asset is Service User, Staff or Corporate information / data, processed by us and is held in an electronic or hard copy / manual format e.g.

- Electronic service user records
- Paper health records

- Audit records
- Paper records and reports including service user and staff records
- Contracts and agreements
- Staff files; sickness, employment details, appraisal, leave, etc.

Information Asset Owner (IAO)
This is someone who has been designated to take responsibility for the information assets for their service / team. They are expected to lead and foster a culture that values and protects all uses of the information that is held by the service on behalf of the organisation. The IAO is responsible for knowing what information the asset holds, what enters it and leaves it and why. They must also know who has access and why, and ensures the use is monitored and compliant with policy and legislation.

Electronic Media
Any type of device that stores and allows distribution or use of electronic information e.g. fax, laptops, PC's, tablets, Mobile Phones etc

Corporate Sensitive Information
Sensitive information is data that must be protected from unauthorised access to safeguard the privacy or security of an organisation e.g. anything that poses a risk to the organisation if discovered by a competitor or the general public. Such information includes acquisition plans, draft business plans or draft tender documents, financial data and supplier and customer information, among other possibilities.

4. Procedure

4.1 Planning and Preparation

All buildings or rooms that need to be vacated must be thoroughly checked by the designated Service Manager / IAO prior to handing over control of the building or rooms in order for the disposal or hand back of the building to take place.

Staff must ensure that all equipment, furniture and documents are removed from the premises and disposed of by an agreed means using the disposal processes offered by Facilities Services. Redundant IT equipment removals must be carried out by the ICT Managers and should be noted on the asset register.

When clearing the building or rooms particular attention must be paid to fixed items of furniture and fittings such as wall mounted cupboards / drawers, notice boards / white boards, bookcases / shelving which may have been used for the storage of documents or electronic media. An end stage checklist (appendix 2) must be completed to ensure that all agreed actions and tasks have been carried out before formal decommissioning takes place.

4.2 Confidential Destruction Arrangements

Paper
If there is a large quantity of confidential documentation which requires destruction, the Head of Facilities should be contacted to arrange for removal to an authorised destruction centre. An inventory of all material must be created by the service and a certificate of destruction obtained from the third party supplier and given to Facilities Services. Smaller quantities of confidential information can be

placed in the confidential consoles provided. The removal of these must be organised by the service lead as part of the final closure arrangements as detailed in the decommissioning checklist (appendix 2). In addition, confidential waste bags can be used and will be removed by the the Facilities Team. It is the responsibility of the service to request confidential waste bags from the Facilities Team in advance and then to request removal prior to the building closure.

Electronic

Deleting documents from electronic devices will not necessarily remove the information from the device. If there is any doubt about this process the ICT department should be contacted for further advice and guidance. An ICT manager will have been allocated by ICT and in attendance at decommissioning meetings. It is important that the disposal of redundant IT equipment is logged by the ICT department and and destroyed using secure and confidential method / s. This needs to be identified as part of the initial decommissioning meeting.

Staff should be aware that other office machinery, in particular standalone fax machines or printers have internal memory which can store a significant amount of information. These should also be listed for disposal.

4.3 Office Removal Companies

Where removal companies are engaged to assist with the relocation of an office, team or department the designated Service Manager / IAO in charge of the move should ensure that:

- Facilities Services have been made aware of the requirement to decommission the area so that the relevant advice / instruction can be made, and the decommissioning meetings organised to allocate responsibilities within the decommissioning check list.
- All sensitive documentation is securely packaged prior to the move.
- An inventory of all documentation is made prior to the boxes being removed.
- The inventory record should be kept separate to the main consignment of documents. The inventory record should be checked at the receiving location to ensure that nothing has been lost during the move.
- All electronic equipment is clearly labelled. Each item should be checked at the new location to ensure that it is complete and serviceable.
- Commercial removal companies employed to carry out the office or location move should be contracted as a same day, point to point service with no overnight storage at non-NHS premises.

4.4 Archiving of Patient and Corporate Records

Any records or documents that are not being transferred to the new accommodation must be archived in accordance with the Trusts archiving standard operating procedure. All documents held within a Team / Service or building must be appraised before deciding on transfer, archiving or disposal. Patient records and most corporate documents are subject to NHS Retention schedules. The Service Manager / IAO will ensure that only documents that have a specific retention period are identified for archiving. A full review of documents must be completed as part of the overall preparation in line with the NHS retention schedules. The service should ensure that any documents that are no longer required are either archived or disposed via the confidential waste arrangements and in keeping with this procedure. The designated Manager / IAO is responsible for contacting the Trust Records Lead to advise of any potential archiving that may be required. All records identified for archiving must be removed from the building prior to the final sign off.

4.5 Final Check and sign off of building

A full physical check must be incorporated into the decommissioning check list to ensure that a comprehensive inspection of the accommodation is completed by the designated Service Manager / IAO. The date for this will be agreed at the initial Decommissioning Meeting. This activity may also be supported by Health and Safety colleagues and any other identified and relevant interested parties. The Services Manager / IAO responsible in the team must sign the check list in appendix 2 to show that all areas of building / s or offices occupied by the service / team have been checked and found to be clear of any Personal, Confidential or Corporate Sensitive Information. The signed declaration must then be forwarded to the IG Team.

The declaration will cover the following areas:

- All redundant IT equipment has been removed from the premises and all items to be moved are listed on the asset register
- All documentation requiring transfer has been accounted for and will be securely moved to the new office / building or archive.
- A thorough check of all areas of the premises has been conducted by staff to ensure that no sensitive information has been overlooked.
- All office furniture and fixed storage areas have been examined to ensure that documents or electronic media have been located and moved or securely disposed of.

Obsolete items of furniture or furniture identified for re use elsewhere in the Trust must be subject to the same decommissioning checks as identified in the SOP. The final check date will be agreed in the initial decommissioning meeting and included on the decommissioning check list (appendix 2). Any locked compartments on furniture (without keys) for disposal will be forced open to ensure that no personal, confidential or corporate sensitive data is contained in it.

Once the final physical inspection has been completed within a building, the decommissioning sign off sheet (Appendix 2) will be completed and signed by the completing manager.

This document will be retained as part of the Decommissioning record.

5. Training

- Raising awareness to fully implement the procedure.
- To publish on the Intranet and communicate via the e-bulletin.
- The Procedure and associated documents should be provided to the service as part of the Decommissioning Project.

6. Monitoring

For this procedure:

- Staff responsible for office closures or moves are aware of their accountabilities and responsibilities regarding this procedure.
- All staff are aware of relevant procedural documents e.g. NHS Code of Practice: Records Management, ICT Policy, Information Governance Policy, Confidentiality Policy etc..
- Untoward incidents resulting from the loss of sensitive information during or following an office move or closure will be logged on DATIX and reported to the Information Governance Team (including the Caldicott Guardian) who will support further investigation in accordance with the Information Security Incident Response Plan (EP10)

7. Duties & Responsibilities

7.1 Chief Executive

The Chief Executive will assume overall accountability for ensuring that decommissioning issues are effectively addressed within the Trust.

7.2 Trust Board

The responsibility for the provision of an information governance procedure for decommissioning rests initially with the Trust Board and is delegated to the Information Governance Team. Additionally, the Trust Board will ensure through the line management structures that this policy is applied and that staff are aware of the decommissioning requirements.

7.3 Senior Information Risk Owner (SIRO)

The SIRO has ownership of the organisation's information risk policy and acts as advocate for information risk on the Board. The Decommissioning Premises (Moves and Closures) Standard Operating Procedure (SOP) forms part of the Trusts overall Information Risk Framework. The SIRO is responsible for ensuring that the SOP is developed and implemented and that it is reviewed regularly to ensure that it remains fit for purpose and supports the Trusts compliance with Data Protection Act Legislation.

7.4 Effective Services Team

Contracts include exit plans and form part of the contract. When the Trust is informed that a service will not be re-commissioned, the Effective ServicesTeam will include the SOP within the exit plan for agreement of roles and responsibilities to complete the process.

7.5 Information Governance/Health Records Team

Information Governance and Health Records Teams will provide guidance to support the Decommissioning process to ensure compliance with legislation and NHS Codes of Practice. The Teams will offer assistance with archiving and / or disposal of Personal or Confidential Identifiable Data.

7.6 ICT Service Support

ICT will allocate a manager that will attend the decommissioning meetings and liaise with services to arrange for the removal of existing IT equipment prior to the building closure.

7.7 Service Manager's/or Information Asset Owners (IAO) Responsibilities

Managers/IAO's must ensure that:

- All reasonable steps are taken to identify and protect all Personal or Confidential Identifiable Data used by or under the control of their teams. e.g. patient data in computer systems and on electronic media and in hard copy format
- Must ensure that all service contracts are cancelled that have been arranged by the service i.e. water coolers

- Ensure that Royal Mail have been contacted to arrange a change of address.
- Ensure that redundant information is disposed of in a secure, confidential and authorised manner. Approved methods of destruction must be used for hard copy information including confidential shredding, confidential waste bags and confidential waste consoles provided by the Trust.
- Staff are made aware of the procedure and monitoring of compliance is undertaken.
- The appropriate service manager willl also carry out final checks of buildings.

7.8 Employee's Responsibilities

Employees should take all reasonable measures to:

- Ensure their manager is aware of all Personal or Confidential Identifiable information to be transferred from the Service or building. Ensure that all data, in any format, is removed from their work area prior to vacating the offices or premises, including removal of information from whiteboards and pinboards.
- Ensure that redundant information is disposed of in a secure, confidential and authorised manner. Approved methods of destruction must be used for hard copy information including confidential shredding, confidential waste bags and confidential waste consoles provided by the Trust.
- Ensure that office furniture no longer required i.e. filing cabinets, desks and cupboards are emptied of all documents before the furniture is disposed of in accordance with Trust Policy and by authorised arrangement with Facilities Management.
- Ensure all personal items are removed from the site either by placing in the storage boxes provided for the transfer or removing from the site.

Appendix 1- Decomissioning Guidance

Health Records / Confidential / Corporate Sensitive information

This guidance document applies to all teams and staff who are moving accommodation and / or decommissioning buildings. It is essential that consideration is given to the identification, storage and transport of all types of information.

All too often when buildings are decommissioned and left empty confidential information can be left behind, particularly in forgotten spaces like loft spaces or basements. Empty buildings and offices are at risk of vandalism and burglary. We must all be vigilant when we are involved with this activity to avoid such an incident.

The Information Commissioner (ICO) is the regulatory body who oversees compliance with the Data Protection Act. If the ICO is aware of repeated data breaches e.g. loss of personal data or information by an organisation and there is a history of similar incidents by the same organisation, the ICO may impose a monetary penalty on that organisation. The monetary penalty could be up to €20M or 4% of annual budget for breaching a data subject's rights and €10M or 2% for breaching a controller's obligations

This is because the organisation has not demonstrated to have controlled measures in place to ensure that confidential information is kept secure at all times i.e. removed all personal and confidential information from the building and ensure that nothing has been left behind once the building has been vacated.

Top Tips

1. Plan Ahead – If you know when you are moving / decommissioning allow yourself plenty of time to do a full sweep of the building / area.
2. Check all rooms – Make sure you check all rooms, even the ones you don't use. This may include loft spaces, basements, cupboards that you have never used. Just because you personally have never used them for storage doesn't mean that someone else hasn't. If records or confidential information are stored in your building **you** are responsible for them.
3. Make an inventory – This is just to give you an idea of what confidential information may be stored in each room and also who it may belong to in terms of dealing with it.
4. Identify the types of confidential information in each room/area. – Different types of information can be dealt with in different ways:

Current patient records – These should be scanned onto the patient's electronic recordif using electronic records. If paper records are still being used they will need to be boxed and appropriate transport arranged for transferring records.

Discharged and Deceased Patient records – These should be boxed and indexed for archiving as per the Archiving Health RecordsRecords SOP

Personnel/Human Resources – Advice should be sought from HR on how to manage this paperwork.

Complaints/investigations – Advice should be sought from the Clinical Governance Team on how to manage this.

General Admin documents – Service Team or ward admin documents need to be sorted into general waste, confidential waste or identified for further storage. A retention schedule may apply to some documents. The NHS Retention schedule is available from the Trust Records Lead.

Confidential waste – should be shredded or put into the appropriate confidential waste sacks. Confidential waste should not just be left lying around for someone else to deal with.

Loose papers – We often come across random piles of loose papers. Do not presume that these are general waste. Someone will need to go through all of this to ensure there is nothing confidential.

Trust/Corporate Branded Documents – Template/blank documents that could be used fraudulently should be treated as confidential waste. These include things like unused prescription pads, template appointment letters, specimen bags, unused or unwanted letter headed paper and service specific referral forms.

General waste – Do not leave general waste/rubbish on shelves or in drawers. Any general waste/rubbish should be identified as such and bagged/boxed appropriately.

5. Check the entire room – Check behind radiators, cupboards and filing cabinets. Check under drawers, pull the bottom drawer out to check nothing has slipped down. If filing cabinets contain suspension files ensure there are no patient/staff names on the files and that all loose pieces of paper have been removed.
6. Allocate responsibility – Ensure specific people are assigned specific tasks. Historically, people have presumed someone else is "dealing" with it and this has not been the case.
7. If patient records need to be archived the Health Records Team should be notified as soon as possible.

Once the buildings/offices have been vacated a detailed final check is carried out by the appropriate Service Manager / IAO. For any outstanding actions regarding confidentiality the staff will be asked to return to the building to sort out any issues. Once these have been addressed the building/office will be checked again and then authorised for closing/de commissioning.

Appendix 2 - Decommissioning Information Governance Check List

Checklist Task	Completed Date	Completed By	Notes
Operational Lead identified to lead premises IG decommissioning / change of use.			
Estates to provide Operational Lead with a building/premises plan detailing all rooms, cellars, attics, garages, cupboards and other potential storage locations. Each 'area' must then be separately numbered.			
Responsible managers in departments transferring out of accommodation have been advised of procedures for safe transfer of records to new accommodation.			
Responsible managers in departments transferring out of accommodation have been advised to follow the Trust procedures for review, archiving and destruction of records.			
Checklist Task	**Completed Date**	**Completed By**	**Notes**
All desks, filing/storage cabinets, drawers, cupboards, and storage shelving have been thoroughly checked.			
Drawers, filing cabinets and removable fittings have been checked to ensure that no corporate or person identifiable information has been left (or fallen down) behind it.			
Any shelving and racking used for records storage should be examined and potentially dismantled to ensure that no corporate or person identifiable information has slipped under, behind or between shelves.			
Notice boards and walls have been checked.			
Where accommodation contains attic, out house, boiler room or similar areas, arrangements have been made for Estates Department to have each of these areas accessed so they can be inspected by the inspection team.			

Any remaining paper based records or documents found containing corporate or person identifiable information have been boxed, labelled with room number/description and location and removed from the decommissioned area to a secure area for further action by the relevant Service Manager.			
Any remaining portable or removable storage devices such as CD, floppy disk, USB sticks or external hard drives have been boxed and labelled with room number/description and location and removed from the decommissioned area to a secure area for further action by the relevant Service Manager.			
ICT Service Desk have been contacted in relation to any remaining equipment or media and have subsequently removed all equipment and media.			
Each individual room and area should be photographed using a digital camera which dates and times the image as proof that the area was fully cleared.			

Manager Name: ______________________________

Manager Designation: ______________________________

Manager Signature: ______________________________

Date: ______________________________

Complete check lists must be sent to the Trust Information Governance Lead.