THE STATE HOSPITALS BOARD FOR SCOTLAND

KEY AND LOCK POLICY

Policy Reference Number	SP12	Issue: 3
Lead Author	Deputy Physical Security Manager	
Contributing Authors	Clinical Security Liaison Managers	
	Team Leaders	
Advisory Group	Security, Risk & Resilience, Health & Safety Group	
Approval Group	Policy Approval Group (PAG)	
Implementation Date	27 July 2023	
Next Review Date	27 July 2026	
Accountable Executive Director	Director of Security, Estates & Resilience	

The date for review detailed on the front of all State Hospital policies/procedures does not mean that the document becomes invalid from this date. The review date is advisory and the organisation reserves the right to review a policy/procedure at any time due to organisational/legal changes.

Staff are advised to always check that they are using the correct version of any policy/procedure rather than referring to locally held copies.

The most up to date version of all State Hospital policies/procedures can be found on the intranet:
http://intranet.tsh.scot.nhs.uk/Policies/Policy%20Docs/Forms/Category%20View.aspx

REVIEW SUMMARY SHEET

No changes required to policy (evidence base checked)	☐

Changes required to policy (evidence base checked)   ☒

Summary of changes within policy:

June23 Review
There has been a new key safe system installed within the hospital and policy has been updated accordingly.

Contents   **Page**

1. POLICY PURPOSE

The purpose of this policy is to ensure:

a) locks and keys are used correctly in order to maintain the security of The State Hospital (TSH) and the safety of staff, patients, visitors and volunteers.
b) the correct locks are in the correct location to provide the appropriate level of security for that location.

2. SCOPE

This key and lock policy applies to all staff and any other member of the public who by the nature of their position, business and frequency of visits have received a security induction and hold a TSH staff pass or unescorted pass. This policy only applies to security key bunches i.e. keys normally collected from the key room.

- Only individuals who have received a security key induction will be authorised to collect and use security keys.
- All personnel that are required to walk around the campus unescorted will require access to a security key.
- Access levels to key safes will be determined by Security Department following assessment of the role, risk to security and health and safety of staff concerned.
- All personnel approved to hold keys must receive a security key induction before being authorised to collect keys.
- Following the key induction, all personnel will be required to sign a form to confirm they have received and understand the security and key induction.
- A record will be kept by security and forwarded to the learning centre monthly of all personnel who have received a Security and Key induction.
- All security key breaches will be reported through DATIX and investigated.

3. ROLES AND RESPONSIBILITIES

- The Security Department is responsible for controlling access to keys by way of setting access levels for individuals based on their role.
- All key holders are responsible for ensuring all keys are secured at all times while in their possession.
- All key holders are responsible for ensuring that they return security keys to the correct location.
- All key holders are responsible for reporting any fault, breakage or loss to the security department immediately.
- All staff are responsible for reporting any security breaches they witness.
- Control room staff and Senior Clinical Cover are responsible for accounting for all keys on site once daily.
- Security staff are responsible for checking each key bunch to ensure all items are fit for purpose, once weekly.
- All key holders are responsible for ensuring that any doors they open are then secured or this responsibility is transferred over to another individual who acknowledges and accepts responsibility for this.
- All key holders are responsible for reporting any faults with locks to security department immediately.
- The Deputy Physical Manager must be informed of any locks that have been removed or replaced.
- A locking schedule will be maintained by the Estates department and audited by the Deputy Physical Security Manager annually.
- The Security Department will be audited annually by external agents.

4. PROCEDURE

4.1 Accessing keys

- To access a key, present your pass to the reader and enter your PIN followed by the (green) enter key. The screen above the key pad will show *take press the (green) enter button again this will give you options on which key to take. Press the (green) enter button once more and the door will open automatically.
- The key slot that is illuminated is the only key that can be collected.
- Once you have removed your keys from the safe you must check that all keys are secured properly i.e. the key ring is secure.
- Before closing the door, check that the LED display reader is showing the correct details i.e. your name.
- On returning your key, present your pass to the reader and enter your pin number then hold the black I-Fob up to the recess on the reader. If you are at the correct safe, the door will open and return your key to the slot illuminated.
- If you are at the wrong safe, the door will not open and a message I-Fob not recognised will show on the display screen. The key safe's are colour coded and the key bunches will have a corresponding coloured bead on the bunch where the keys should be returned too.
- If you return your key to the wrong safe the display screen will say I-Fob not recognised and the safe will alarm. If this happens, the keys should be removed and returned to the correct safe. If the key ca not be removed this should be reported to a member of the security department who will remove the key or report the fault. If this does not happen, there may be a management investigation, which could lead to disciplinary action being taken.
- Always check the LED screen when returning your keys this will tell you that you are at the correct safe.
- Never allow anyone else to insert there keys in a safe if you have opened the door, the door should be closed and the next person should follow the procedure above.
- The keys must be attached to your belt and the belt being attached to your person before leaving the key room. Once you attach your keys to your belt they should not be removed from your belt (with the exceptions being training in Islay, using the gym or going on a patient outing) until you have returned to the key room. Anyone found with security keys not attached to their belt out with the key room may be subject to a management investigation, which may lead to disciplinary action being taken.
- Control room staff- will complete a key check at 07:30 hrs and 22:15 hrs daily.

4.2. Loss or damage

- Loss of a security key must be reported to the nurse in charge or head of department who in turn will inform the duty security manager immediately.
- The Duty Security Manager will immediately inform Director of Security, Estates & Resilience or appropriate other director.
- Any faults with a security key must be reported to security staff immediately. Do not return a faulty key to the key safe, hand it to a member of security staff.
- If you have any difficulty with any locks report this to Duty Security Manager immediately who in turn will inform the estates department.
- If you have any difficulty with any of the key safes report it to security staff immediately.

4.3. Leaving the hospital

- It is the responsibility of everyone who lifts a security key to ensure that keys do not leave the hospital.
- No keys should go beyond the key room door leading back into reception other than security staff who require these keys to access the vehicle lock.

- To help prevent keys leaving the hospital there is fob attached to all key bunches that activates an alarm when you reach the tube stiles in reception. This is not guaranteed to activate every time.
- It is the responsibility of everyone carrying security keys to ensure they are returned to the key safes before leaving the hospital.
- If a member of staff leaves the hospital with security keys they will be subject to a management investigation that may lead to disciplinary action being taken.
- If staff are responding to an emergency situation outside the hospital then all keys should be handed to security staff before leaving the hospital. Security staff will return these keys to the correct safes where staff can collect them on their return.
- Staff going on external outing can leave their keys in the key safe situated in the vehicle lock. This key safe operates the same as described above.
- Only the member of staff who deposited their key in this safe will have access to remove this key.

4.4. Attending PMVA course or Gym

- Any staff attending the Gym or PMVA course can deposit their keys in safes within the office areas of the sports centre and Islay for the duration of the course or session.
- When collecting a key from these safes the safe will offer the first key available at the same access level as the one placed in the safe. The keys are colour coded with a coloured bead that will correspond with the colour on the safes in the main key room this will allow the staff member to return them to the correct safe in the main key room at the end of their shift.

4.5. Key Security

- When not in use keys must be concealed. On no account must any security keys be allowed to reach the hands of a patient.
- Although these keys are magnetic and cannot be copied staff must keep all keys out of sight of patients, in a key pouch or trouser pocket.
- All security keys uplifted from the key room must be returned by the recipient. If due to exceptional circumstances this is not possible, the Control Room should be made aware of the circumstances immediately.
- Only staff assigned to the responsibility of letting patient access/egress wards and departments should do so. No other member of staff should allow patients in or out of departments.
- Under no circumstances should any member of staff remove or tamper with any keys from a bunch of security keys.

5. EQUALITY AND DIVERSITY

The State Hospitals Board (the Board) is committed to valuing and supporting equality and diversity, ensuring patients, carers, volunteers and staff are treated with dignity and respect. Policy development incorporates consideration of the needs of all Protected Characteristic groups in relation to inclusivity, accessibility, equity of impact and attention to practice which may unintentionally cause prejudice and / or discrimination.

The Board recognises the need to ensure all stakeholders are supported to understand information about how services are delivered. Based on what is proportionate and reasonable, we can provide information/documents in alternative formats and are happy to discuss individual needs in this respect. If information is required in an alternative format, please contact the Person-Centred Improvement Lead on 01555 842072.

Line Managers are responsible for ensuring that staff can undertake their role, adhering to policies and procedures. Specialist advice is available to managers to ensure that reasonable adjustments

are in place to enable staff to understand and comply with policies and procedures. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

Patient pre-admission assessment processes and ongoing review of individual care and treatment plans support a tailored approach to meeting the needs of patients who experience barriers to communication (e.g. Dementia, Autism, Intellectual Disability, sensory impairment). Rapid access to interpretation / translation services enables an inclusive approach to engage patients for whom English is not their first language. Admission processes include assessment of physical disability with access to local services to support implementation of reasonable adjustments. Patients are encouraged to disclose their faith / religion / beliefs, highlighting any adapted practice required to support individual need in this respect. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

Carers / Named Persons are encouraged to highlight any barriers to communication, physical disability or anything else, which would prevent them from being meaningfully involved in the patient's care (where the patient has consented) and / or other aspects of the work of the Hospital relevant to their role. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy".

The volunteer recruitment and induction process supports volunteers to highlight any barriers to communication, physical disability or anything else, which would prevent them from contributing meaningfully to patient care and / or engage in other aspects of the work of the Hospital relevant to their role. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

6. STAKEHOLDER ENGAGEMENT

Key Stakeholders	Consulted (Y/N)
Patients	N
Staff	Y
The Board	Y
Carers	N
Volunteers	Y

7. COMMUNICATION, IMPLEMENTATION, MONITORING AND REVIEW OF POLICY

This policy will be communicated to all stakeholders within The State Hospital via the intranet and through the staff bulletin.

The Person Centred Improvement Service will facilitate communication with Volunteers.

Security, Risk & Resilience, Health & Safety Group (the Advisory Group) will be responsible for the implementation and monitoring of this policy.

This policy will be reviewed every three years, on significant change or if legislation changes.