



Guest Security: Hospitality Industry Principles and Good Practice Guidance

Introductory factsheet

What's the issue?

Every day, millions of people stay in accommodation businesses across the United Kingdom. They trust that their accommodation provider will offer not only comfort and hospitality, but also a safe, secure and welcoming environment.

Technological developments have transformed the guest journey. These developments bring significant opportunities. However, they also create new considerations for accommodation providers when it comes to keeping our guests safe and secure.

UKHospitality and its members has produced guidance on protecting guest privacy and ensuring that access to accommodation is managed safely and appropriately.

The full guidance is intended to support accommodation providers in reviewing their arrangements, sharing good practice and continuing to strengthen standards across the sector.

This factsheet sets out the key principles and a simple checklist for operators, especially those who may not have considered this area as a specific risk assessed process. The full principles and guidance can be found on the UKHospitality website here: www.ukhospitality.org.uk/guidance/guest-safety

Five principles of guest security, privacy and room access

The guidance is built around five core principles, providing a framework that can be applied across your business model in a way that is most effective for your operation.

Principle 1: Guest security comes first

Guest security should be the primary consideration when decisions are made regarding access to accommodation, guest information and operational procedures.

Principle 2: Privacy is an essential part of security

Privacy should not be viewed solely as a data protection issue. Information that appears routine can become highly sensitive when it reveals a guest's location, confirms their presence at a property or enables unauthorised access to accommodation. Protecting guest privacy is therefore an important component of guest security.

Principle 3: Verification should be proportionate but effective

Accommodation providers should take reasonable steps to verify identity before granting access to accommodation or issuing access credentials.

Different circumstances may require different approaches. However, the principle remains consistent: access should only be granted when employees are satisfied that appropriate verification has taken place.

Principle 4: Well-trained employees are the strongest safeguard

While technology, physical security measures and written procedures all play important roles, employees remain the most important safeguard within any guest security framework.

Investment in training, communication and employee support should therefore be viewed as an investment in guest security.

Principle 5: Security arrangements should continually improve

Guest security is not static. Technologies evolve, operating models change and guest expectations develop over time. New risks emerge while existing risks may change in nature or significance.

Accommodation providers should regularly review incidents, near misses, guest feedback and operational experience to ensure that arrangements remain effective.

Quick-reference operational checklist

Strong guest security cultures are rarely built through a single initiative. They are developed through consistent leadership, clear communication and a shared commitment to protecting guests, employees and visitors.

The full guidance document sets out in detail how you can adapt your own business practices to ensure this commitment is carried out on a practical level.

Please note this checklist and factsheet is intended as an introduction to the more detailed guidance document. This is not exhaustive, and UKHospitality recommends operators refer to the full version when building their own practices and procedures

within their specific businesses. This can be downloaded from the UKHospitality website here: www.ukhospitality.org.uk/guidance/guest-safety

At the top

- ☐ Secure senior leadership buy-in and accountability to the five guest security principles
- ☐ Allocate sufficient resource to support implementation
- ☐ Ensure staff know exactly who is responsible for guest security within the business

Risk assessment

- ☐ Make sure you've got a risk assessment on guest security incorporating the below where appropriate, and it's up to date. This will be specific to your business – you will know how best to identify foreseeable risks and implement appropriate controls using the principles and guidance provided

Who's staying with you

- ☐ Establish a framework with the core principle that staff are satisfied that they know who they are dealing with before access to accommodation is granted. This may include the below steps.
- ☐ Reviewing check-in procedures regularly
- ☐ Maintaining accurate occupancy records
- ☐ Establishing a consistent verification framework
- ☐ Recording replacement key activity
- ☐ Providing staff with practical examples and training
- ☐ Reviewing unusual access requests
- ☐ Communicating verification procedures positively to guests
- ☐ Ensure that support is available from senior management if guests react negatively to the process being followed

Protect the privacy of your guests

- ☐ Manage room numbers discreetly e.g. writing room numbers rather than announcing them, removing room numbers from physical keys, using room wallets or key sleeves etc.
- ☐ As a general rule, staff should not confirm whether a named individual is staying at a property

☐ Rooming lists, breakfast reports, housekeeping schedules and operational documents should contain only the information necessary for staff to perform their roles and should never be publicly accessible.

Group bookings

- ☐ Have a framework for lead-booker procedures
- ☐ Document late arrivals to group bookings
- ☐ Don't assume: people who appear to have a legitimate reason for seeking room information may not always be authorised to receive it. Ensure procedures focus on verification and authorisation rather than appearances or assumptions, especially when it comes to group bookings.

Technology

- ☐ Have a framework for self-check kiosks. This could include how guest identity is verified, what information is displayed on screens and how replacement cards are managed
- ☐ Manage digital cards – including when access is restricted, replacement cards are issued or lost cards reported.

Staff access to rooms

- ☐ Implement a room entry procedure e.g. check 'Do Not Disturb' indicators, knocking clearly, announcing presence
- ☐ Review working arrangements for lone staff
- ☐ Ensure employees understand different room-access scenarios

Physical security

- ☐ Make sure physical security equipment (self closing doors, locks, door viewers, card access lifts) are working and inspected regularly
- ☐ Audit the use of master keys and ensure there is a clear use policy around them
- ☐ Review security systems and related areas such as CCTV during and after any physical changes to the building and access points (e.g. refurbishments)

Continuous improvement

- ☐ Monitor, report and record any trends (e.g. increased replacement key requests, recurring privacy concerns, training gaps) and use lessons learned to continually keep your risk assessment evolving
- ☐ Encourage open reporting, constructive discussion and learning from mistakes across everyone in the business