



Guest Security: Hospitality Industry Principles and Good Practice

UKHospitality guidance for accommodation providers

Foreword

Every day, millions of people stay in accommodation businesses across the United Kingdom.

Whether travelling for work, visiting friends and family, taking a holiday, attending an event or seeking temporary accommodation, guests place significant trust in the businesses they choose to stay with. They trust that their accommodation provider will offer not only comfort and hospitality, but also a safe, secure and welcoming environment.

That trust carries responsibility.

Accommodation providers have long recognised the importance of guest security and wellbeing. Across the UK, hotels, serviced apartments, holiday parks, pubs, lodges, hostels and other accommodation businesses work hard to provide environments where guests can relax, enjoy their stay and feel confident that their privacy and security are being protected.

The sector has a strong record of delivering secure and welcoming experiences across diverse operating models. However, the operating environment continues to evolve.

Technological developments have transformed the guest journey. Online booking platforms, self-service kiosks, digital room keys and mobile applications are increasingly common. Booking arrangements have become more complex, with accommodation often being arranged through employers, conference organisers, travel management companies, online travel agents and group booking platforms. At the same time, guest expectations around privacy, personal data and security have never been higher.

These developments bring significant opportunities. They can improve convenience, reduce administrative burdens and enhance the guest experience. However, they also create new considerations for accommodation providers.

Questions that may once have been straightforward can now require careful judgement. How should staff respond when a guest requests a replacement room key but cannot produce identification? What is the appropriate response when someone requests access to a room but is not listed on the booking? How can businesses take advantage of new technology while maintaining robust verification standards? How should guest information be protected in an increasingly digital environment?

These principles and good practice guidance has been developed in collaboration with accommodation providers from across the sector. It combines operational experience, practical examples and established good practice to provide guidance on one of the most important aspects of guest security - protecting guest privacy and ensuring that access to accommodation is managed safely and appropriately.

It recognises that accommodation providers operate in a wide variety of settings. A large city-centre hotel, a rural holiday park, and an independent guest house may all face

different challenges. Different business models require different approaches and there can be no single solution that applies in every circumstance.

This document sets out a framework of principles and recommendations that businesses can adapt to their own circumstances through risk assessment, staff training and operational planning.

Importantly, guest security should never be viewed as being in competition with the guest experience.

The most effective security arrangements are reflected in well-trained staff, clear communication, respectful handling of personal information and thoughtful procedures that protect guests.

Ultimately, strong guest security measures help to build trust, confidence and positive enjoyable experiences. They support staff in making good decisions, provide reassurance to guests and contribute to the welcoming environments that define the best of the accommodation sector.

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

Executive summary

Why this guidance matters

Guest security is one of the key foundations of the accommodation sector.

Whilst accommodation providers manage a wide range of health, safety and operational responsibilities, the ability to protect guest privacy and control access to accommodation is particularly important. Guests must be confident that their personal information will be handled appropriately and with due confidentiality, that access to their accommodation will be controlled responsibly and that staff have the training and support necessary to make good decisions.

The overwhelming majority of guest stays take place without incident. Nevertheless, accommodation providers continue to encounter situations that require careful judgement and consistent decision-making.

These include:

- Requests for replacement room keys
- Requests for access by individuals not named on bookings
- Management of group and corporate bookings
- Protection of guest privacy
- Use of digital room access technology
- Staff access to occupied rooms
- Aggressive or challenging behaviour where access is refused

This guidance has identified a number of common themes across accommodation providers of different sizes and operating models.

First, **guest security and privacy are closely linked**. Protecting information about a guest's identity, location or room number is often an important component of protecting their physical safety and wellbeing.

Second, **staff play a critical role**. Technology and physical security measures can support good outcomes, but staff remain the most important safeguard when unusual or unexpected situations arise.

Third, **consistency matters**. Even well-designed procedures can become ineffective if they are applied inconsistently between teams, departments or shifts.

Finally, **guest security should be viewed as an ongoing process** of review and improvement, not a one-off exercise.

Accommodation providers that regularly review incidents, learn from experience and adapt their procedures are often best placed to respond to changing risks and expectations.

Five principles of guest security, privacy and room access

The recommendations contained within this report are built around five core principles, providing a framework that can be applied across different accommodation settings and operating models.

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.

Operational pressures or customer expectations should never result in unnecessary compromise of guest security arrangements.

This does not mean creating barriers for guests or adopting unnecessarily restrictive processes. Rather, it means ensuring that decisions are guided by a clear understanding of potential risks and a commitment to protecting guests from harm.

When difficult decisions arise, businesses should be able to demonstrate that guest wellbeing remained the central consideration. Alongside this, under no circumstances should staff be expected to place themselves at risk or in harm's way when attempting to enforce or support guest security measures.

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.

Accommodation providers should ensure that guest information is only shared where operationally necessary and that staff understand the importance of handling information appropriately.

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.

Verification processes should be robust enough to prevent unauthorised access while remaining practical for guests and staff.

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

Principle 4: Well-trained staff are the strongest safeguard

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

Staff are often required to make decisions in situations that do not fit neatly within established procedures. They need the confidence, knowledge and support necessary to exercise good judgement.

Investment in training, communication and staff 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.

Continuous improvement helps ensure that guest security arrangements remain practical, proportionate and aligned with current risks.

Chapter 1: Creating a culture of guest security

Why culture matters

When people think about guest security, they often think first about locks, keys, access cards and security technology.

While these measures are important, experience across the accommodation sector consistently demonstrates that guest security depends just as much upon organisational culture, staff confidence and operational consistency.

Few guest security incidents are due to security systems failure. Instead, they arise because staff are placed in difficult situations, procedures are unclear, information is incomplete or decisions are made inconsistently.

For this reason, guest security should be viewed as an organisational responsibility rather than solely a security function.

The most effective accommodation providers create environments where guest security is embedded into everyday operations and where staff understand both the procedures they are expected to follow and the reasons those procedures exist.

Leadership and accountability

Strong guest security arrangements begin with visible leadership.

Senior managers should ensure that guest security is recognised as a priority throughout the organisation and that appropriate resources are allocated to support effective implementation.

This includes:

- Maintaining documented procedures
- Reviewing risk assessments
- Supporting staff training
- Monitoring incidents and trends
- Reviewing emerging risks
- Promoting continuous improvement

Importantly, accountability should be clear.

Staff should understand who is responsible for decision-making, escalation and policy oversight. This becomes particularly important when unusual situations arise that require judgement beyond routine procedures.

The role of risk assessment

Different accommodation providers face different risks.

A large city-centre hotel may encounter very different challenges to a rural holiday park or serviced apartment operation. Likewise, businesses serving conference delegates may face different considerations to those primarily serving leisure travellers.

For this reason, guest security arrangements should be informed by risk assessment rather than relying solely on standardised procedures.

Areas that businesses may wish to consider include:

- Guest access arrangements
- Replacement key procedures
- Digital room access technology
- Group booking arrangements
- Staff room access
- Lone working
- Management of guest information
- Building layout and access control

The objective is to minimise risk, by identifying foreseeable risks and implementing appropriate controls.

Supporting staff to make good decisions

Procedures are important, but they cannot anticipate every possible scenario.

Staff will inevitably encounter situations that fall outside standard processes. A guest may lose their identification. A family member may seek access to a room. A late-arriving guest may appear to have legitimate booking information but not be listed on a reservation.

In these situations, staff need confidence as well as procedures.

Businesses should encourage staff to:

- Prioritise guest security
- Ask questions when unsure
- Escalate concerns as soon as they arise
- Apply procedures consistently
- Seek support

Staff should never feel pressured into compromising guest security arrangements in order to avoid inconvenience or confrontation.

Learning from incidents and ‘near misses’

The accommodation sector has a strong culture of learning from operational experience and this approach should extend to guest security.

Businesses should frequently review:

- Security incidents
- Privacy breaches
- Unauthorised access attempts
- Replacement key issues
- Incidents that had the potential to cause harm but did not result in actual harm – known as ‘near misses’
- Reporting requirements
- Guest feedback

The purpose of review should not be to assign blame, but to identify opportunities for improvement.

When handling guest data, any data retained by businesses should be proportionate to its legitimate purpose, processed in accordance with applicable data protection legislation, collected and retained for the clearly defined purpose of guest security, and not kept for longer than is necessary.

Good practice spotlight

One accommodation provider identified significant variation in how replacement key requests were handled across different shifts.

Although no serious incidents had occurred, management recognised that inconsistent practice created unnecessary risk.

The business responded by introducing a single verification framework, refresher training and periodic audits. Staff reported greater confidence in handling requests and management gained greater assurance that procedures were being applied consistently.

Practical actions for operators

Accommodation providers should consider:

- ✓ Maintaining documented guest security procedures
- ✓ Assigning responsibility for guest security at management level
- ✓ Reviewing risk assessments regularly
- ✓ Recording and reviewing incidents and ‘near misses’

- ✓ Auditing key operational procedures
- ✓ Supporting staff to escalate concerns
- ✓ Incorporating guest security into training programmes
- ✓ Reviewing procedures following significant incidents or changes to operations

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, staff and visitors.

Chapter 2: Supporting secure arrivals and check-in

Why this matters

The guest journey often begins long before check in.

The booking process, arrival experience and check-in procedure all play an important role in creating a safe and secure stay. They are often the first opportunities for accommodation providers to verify information, establish accurate occupancy records and communicate important information to guests.

For most guests, check-in is a straightforward and routine process. However, accommodation providers also encounter situations that require additional judgement and care. Guests may lose identification, bookings may have been made by third parties, additional occupants may arrive unexpectedly or information may be incomplete.

Well-designed check-in procedures help create a positive guest experience while ensuring that appropriate safeguards are in place from the start of a stay.

The role of verification

Verification is one of the most important safeguards available to accommodation providers.

The purpose of verification is not to create unnecessary barriers for guests. Rather, it is to provide reasonable assurance that access to accommodation is only granted to authorised individuals.

The level of verification required may vary depending on the circumstances. A guest checking into a room for the first time may require a different approach to a guest requesting a replacement room key three days into their stay. Similarly, a business traveller booked through a corporate travel system may present different verification challenges to a family staying at a holiday park.

Whatever the circumstances, the underlying principle remains consistent: staff should be satisfied that they know who they are dealing with before access to accommodation is granted.

Creating accurate occupancy records

Accurate occupancy information supports both guest security and operational effectiveness, particularly when taking bookings over the phone.

Accommodation providers should seek to maintain records that accurately reflect who is staying on site and who is authorised to access accommodation.

This can be particularly important where:

- Additional guests arrive after check-in
- Rooms are booked by employers or third parties, particularly online travel agents who do not provide booking details
- Accommodation is shared between multiple occupants
- Group bookings are involved
- Guests have similar names
- Names can be ambiguous
- Long-stay guests extend their reservations

The objective is not to create unnecessary administration. Rather, it is to ensure that staff have sufficient information available when decisions about access need to be made.

When gathering guest data, any data retained by businesses should be proportionate to its legitimate purpose, processed in accordance with applicable data protection legislation, collected and retained for the clearly defined purpose of guest security, and not kept for longer than is necessary.

Replacement key requests

One of the most common guest security scenarios encountered by accommodation providers involves requests for replacement room keys or access credentials.

Lost keys are a normal part of operating accommodation businesses. Guests may accidentally leave access cards in rooms, misplace them during a stay or experience technical issues with digital access credentials.

While such requests are common, they also represent one of the areas where inappropriate access could potentially occur if procedures are not followed consistently.

For this reason, replacement key requests should be treated as an important verification point. This is true of both digital and physical keys.

Good practice approach

Where possible, staff should seek to verify a combination of information before issuing replacement access credentials.

Photo identification is the most secure form of identification, though there is no legal requirement to show photo ID. Other identification, such as credit cards, could also prove useful. However, accommodation providers should recognise that guests may not always have identification immediately available.

The objective is not to insist on a particular form of identification in every circumstance, but to obtain sufficient assurance that the individual requesting access is the legitimate guest. The list below gives some alternatives.

Examples may include:

- Guest name
- Room number
- Arrival date
- Departure date
- Length of stay
- Booking method
- Booking reference
- Contact information
- Names of other occupants

Scenario: Lost key, no identification

A guest approaches reception and explains that they have lost their room key while out for dinner. They are unable to produce identification because their wallet remains in the room.

This is a situation that many accommodation providers encounter.

A proportionate response may involve using multiple verification questions, reviewing booking information and considering other information available through internal systems, this should be data only the guest could offer. Staff may also consider whether there are other means of establishing confidence in the guest's identity.

The lost key, if digital, should be deleted from the system.

The core principle is that access should only be granted once confident verification has taken place.

Supporting positive guest experiences

Verification procedures should be delivered professionally and respectfully.

Most guests understand the importance of protecting access to accommodation and appreciate the reassurance that appropriate procedures provide.

Staff should explain processes clearly, avoid creating embarrassment and communicate that verification measures are intended to protect all guests.

How procedures are delivered can be just as important as the procedures themselves.

Practical actions for operators

Accommodation providers should consider:

- ✓ 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

When handling guest data, any data retained by businesses should be proportionate to its legitimate purpose, processed in accordance with applicable data protection legislation, collected and retained for the clearly defined purpose of guest security, and not kept for longer than is necessary.

Chapter 3: Protecting guest privacy throughout the stay

Why privacy matters

Guest privacy is a fundamental element of guest security.

Guests share a significant amount of personal information with accommodation providers. They provide names, contact details, payment information, travel arrangements and, in many cases, details about where they are staying and for how long.

While accommodation providers routinely handle this information responsibly, it is important to recognise that privacy concerns extend beyond data protection obligations.

Information that appears routine can become highly sensitive when it reveals a guest's location, confirms their presence at a property or enables someone to gain access to them.

For guests, protecting privacy may be particularly important. However, accommodation providers should avoid making assumptions about which guests may be vulnerable. Consistent privacy standards provide protection for everyone.

Privacy as a security issue

A guest's room number may appear to be operational information.

However, if disclosed inappropriately it may reveal a guest's location.

Similarly, confirming whether an individual is staying at a property may seem harmless in some circumstances. Yet that information may be used in ways that are not immediately apparent to staff.

For this reason, privacy and security should be viewed as closely connected.

Managing room numbers discreetly

Many accommodation providers have already adopted practices designed to minimise unnecessary disclosure of room numbers.

Examples include:

- Writing room numbers rather than announcing them
- Removing room numbers from physical keys
- Using room wallets or key sleeves
- Providing information through secure digital channels
- Avoiding unnecessary display of room details
- Refraining from asking a guest their number at breakfast, etc

There is no single correct approach. The objective is simply to avoid unnecessarily broadcasting information that identifies where a guest is staying.

Requests for guest information

Accommodation providers regularly receive requests from someone not listed on the booking seeking information about guests.

These may come from:

- Family members
- Friends
- Colleagues
- Partners/former partners
- The police, emergency services or other authorities
- Delivery companies
- Members of the media
- Members of the public

In many cases the request may appear entirely legitimate.

However, staff are rarely in a position to understand the full context behind such requests.

For this reason, accommodation providers should adopt clear and consistent approaches to handling guest information. When handling guest data, any data retained by businesses should be proportionate to its legitimate purpose, processed in accordance with applicable data protection legislation, collected and retained for the clearly defined purpose of guest security, and not kept for longer than is necessary.

A simple principle

As a general rule, staff should not confirm whether a named individual is staying at a property.

This approach protects guests, provides clarity for staff and removes the need for staff to make complex judgements about individual circumstances.

Internal information sharing

Privacy considerations also apply within businesses.

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.

This is not simply about compliance. It is about ensuring that information is handled thoughtfully and responsibly.

Scenario: Telephone enquiry

A caller contacts reception and asks whether a particular guest is staying at the property.

The caller explains that the matter is urgent and that they need to speak to the guest immediately.

Rather than confirming the guest's presence, a safer approach may be to explain that guest information cannot be disclosed and, where appropriate, offer to take a message making it clear you would take the message whether the guest was present or not, and the action of taking a message does not confirm the guest's presence or not. The caller's identity and their message can then be conveyed to the guest.

This allows staff to maintain privacy standards while remaining helpful and professional.

Practical actions for operators

Accommodation providers should consider:

- ✓ Reviewing how room numbers are communicated
- ✓ Assessing the use of physical keys with identifiable room numbers
- ✓ Establishing clear procedures for handling guest enquiries
- ✓ Limiting unnecessary information on operational reports
- ✓ Providing privacy-focused training
- ✓ Reviewing who in their own property requires access to guest information
- ✓ Reinforcing privacy expectations across all departments

Chapter 4: Managing access to accommodation securely

Why access control matters

Accommodation providers have a responsibility to ensure that access to guest accommodation is appropriately controlled throughout a stay.

This responsibility extends beyond check-in and to all staff.

Requests for additional keys, duplicate credentials, access by additional occupants and requests from individuals not listed on bookings all create situations that require careful judgement.

Most requests are entirely legitimate. Effective procedures help ensure that access decisions are made consistently and securely.

Additional occupants

Modern travel arrangements are often flexible.

Family members may arrive later than the lead guest. Friends may join a booking after check-in. Business colleagues may travel separately.

Accommodation providers should seek to accommodate these situations where possible while maintaining appropriate safeguards.

Good practice may include:

- Recording details of additional occupants when the first guest arrives
- Updating booking information for any changes to registered guests
- Obtaining authorisation from lead guests
- Maintaining clear notes on internal systems

The objective is to reduce uncertainty when future access requests arise.

Requests from individuals not listed on bookings

Staff occasionally encounter situations where an individual seeks access to a room but is not named on the reservation.

They may possess booking information, know the name of the guest or appear to have a legitimate connection to the booking.

However, access decisions should not be based on assumptions or familiarity.

Staff should seek appropriate verification and always obtain confirmation from the named guest as staying in the room.

Avoiding assumptions

One of the most important lessons from operational experience is the importance of avoiding assumptions.

People who appear to have a legitimate reason for seeking access may not always be authorised to receive it.

Likewise, genuine guests may sometimes struggle to provide information immediately.

For this reason, procedures should focus on verification and authorisation rather than appearances or assumptions.

Scenario: Late-arriving guest

A guest arrives at midnight and explains that their partner checked in earlier.

They know the room number and provide details about the booking.

Before issuing a key, staff should satisfy themselves via a proportionate response which may involve contacting the named guest, reviewing booking records and confirming that the individual is expected before access is granted.

The key objective is ensuring that access decisions are based upon appropriate evidence rather than convenience.

Balancing security and hospitality

Accommodation providers should not view guest security and hospitality/providing good customer service as competing priorities.

The most effective organisations combine both.

Guests are more likely to feel reassured when they can see that accommodation providers take privacy and access control seriously. Clear explanations, professional communication and respectful treatment can help ensure that security procedures support rather than detract from the guest experience.

Non-reception requests

There are examples where customers make requests for access to staff not on reception. This could include housekeeping and maintenance workers, for example. It is important that all team members are aware of the necessary protocols and follow them.

Practical actions for operators

Accommodation providers should consider:

- ✓ Reviewing room access procedures
- ✓ Establishing clear authorisation processes
- ✓ Recording access-related decisions where appropriate
- ✓ Supporting staff to escalate concerns
- ✓ Using scenario-based training
- ✓ Reviewing arrangements for additional occupants
- ✓ Monitoring recurring issues and trends

Strong access control arrangements help create confidence for guests, support staff in making decisions and contribute to safe and welcoming accommodation environments.

Chapter 5: Supporting safe stays in group and shared booking environments

Why this matters

Group bookings are an important part of the accommodation sector and include everything from conference delegates and corporate travellers, to sports teams, family gatherings, educational visits and organised tours.

While the principles of guest security remain the same, group bookings often introduce additional complexity. Accommodation may be booked by a third party, room occupants may change during a stay and guests may arrive at different times. In holiday parks and lodge environments, lead-booker arrangements may mean that multiple individuals have access to accommodation that was originally booked by a single person.

These arrangements require accommodation providers to balance flexibility with appropriate safeguards.

Understanding who is authorised

One of the most important considerations is understanding who has authority in relation to a booking.

Questions that may arise include:

- Who is authorised to request additional room access?
- Who can make changes to a booking?
- Who can authorise additional occupants?
- Who should be contacted when access requests arise?

The answers may differ depending on the nature of the booking.

For example, a corporate travel booking may involve an employer arranging accommodation for their employee. A conference booking may be managed by an event organiser. A holiday park booking may rely upon a lead-booker model.

Accommodation providers should ensure staff understand how authority is established and recorded.

Group arrivals and staggered check-ins

Not all members of a group necessarily arrive together.

It is increasingly common for guests to arrive separately due to differing travel arrangements. This can create uncertainty if accommodation providers do not have sufficient information about who is expected.

Where practical, businesses may wish to encourage advance sharing of rooming information or establish processes that allow expected arrivals to be identified clearly.

This can help reduce delays for guests while ensuring verification standards are maintained.

Holiday parks, lodges and caravan accommodation

Holiday parks, lodges and caravan sites often operate differently from traditional hotels.

Guests may move more freely around sites, accommodation units may be spread across larger areas and access may be controlled through a combination of physical keys, wristbands, vehicle passes, digital applications or access cards.

While operational arrangements differ, the same principles apply.

Businesses should seek to:

- Understand who is staying in accommodation units
- Maintain accurate booking information
- Verify requests for replacement access credentials
- Establish clear lead-booker responsibilities
- Manage changes to bookings appropriately

Practical actions for operators

Accommodation providers should consider:

- ✓ Establishing clear lead-booker procedures
- ✓ Reviewing rooming-list arrangements
- ✓ Recording authorised occupants where appropriate
- ✓ Reviewing procedures for late arrivals
- ✓ Providing staff with examples of common group-booking scenarios
- ✓ Ensuring holiday park and lodge procedures align with guest security principles. When gathering guest data, any data retained by businesses should be proportionate to its legitimate purpose, processed in accordance with applicable data protection legislation, collected and retained for the clearly defined purpose of guest security, and not kept for longer than is necessary.

Chapter 6: Using technology to support guest security

Technology as an enabler

Technology has transformed the guest experience.

Many guests now expect online booking, digital communications, mobile applications and self-service functionality as part of their stay. These technologies can improve convenience, reduce administrative burdens and create more personalised experiences.

When implemented thoughtfully, technology can also strengthen guest security.

However, technology should support good decision-making rather than replace it.

Self-service check-in

Self-service kiosks and digital check-in systems are becoming increasingly common across the accommodation sector.

These systems can improve efficiency and reduce waiting times. However, accommodation providers should ensure that verification standards remain appropriate.

Questions businesses may wish to consider include:

- How is guest identity verified?
- What information is displayed on screens?
- How are replacement credentials managed?
- What support is available when verification cannot be completed automatically?

Technology should be designed with guest security considerations in mind from the outset. This could include assessing the below:

- The positioning of kiosks with guest's data privacy in mind
- Potential coverage of the kiosks by CCTV, if not monitored consistently by staff
- How international travellers are managed
- How age verification can be managed

Digital room keys

Mobile room keys and digital access credentials can provide a secure and convenient alternative to traditional access cards.

Many systems offer advantages such as:

- Reduced risk of lost cards
- Enhanced audit trails

- Improved management of access permissions
- Faster deactivation of compromised credentials

Accommodation providers should nevertheless ensure they understand how access rights are created, managed and removed.

Protecting privacy in digital environments

Digital systems often hold significant amounts of guest information.

Privacy considerations should therefore be embedded throughout system design and operation.

Businesses should consider:

- Access controls
- User permissions
- Data retention
- Information sharing
- Security monitoring

Protecting digital information is an important part of protecting guest security.

Looking ahead

Emerging technologies such as digital identity solutions, biometric authentication and artificial intelligence may offer future opportunities to strengthen guest security.

Accommodation providers should approach new technologies thoughtfully, ensuring that innovation supports guest safety, wellbeing and trust. Ensure all emerging technologies are compliant with data protection and other existing legislation before adopting.

Practical actions for operators

- ✓ Review verification standards within digital systems
- ✓ Consider privacy impacts when introducing new technology
- ✓ Ensure staff understand digital access procedures
- ✓ Regularly review user permissions and access rights
- ✓ Test systems and contingency arrangements periodically

Chapter 7: Ensuring secure access to guest rooms by staff

Respecting private spaces

Guest rooms are both accommodation and private spaces.

Staff may need to enter rooms for a variety of legitimate reasons, including housekeeping, maintenance, inspections, guest requests and welfare checks. However, these visits should always be undertaken thoughtfully and respectfully.

The objective is to protect both guests and staff.

A consistent room-entry procedure

Many accommodation providers use structured room-entry procedures to create consistency and reduce misunderstandings.

A typical process may include:

1. Checking for 'Do Not Disturb' indicators
2. Knocking clearly
3. Announcing presence
4. Waiting for a response
5. Repeating the process if necessary
6. Entering cautiously where appropriate

The exact procedure may vary between businesses, but consistency within each individual business is important.

Different circumstances require different responses

A housekeeping visit may involve different considerations from a maintenance inspection or welfare check.

Staff should understand:

- Why access is required
- Whether guests are expected to be present
- Any known guest preferences or requirements
- Relevant lone-working procedures

Communication between departments can be particularly important in avoiding confusion.

Supporting staff safety

Guest security and staff safety are closely connected.

Staff who feel safe and supported are more likely to follow procedures consistently and make good decisions.

Depending on the environment, businesses may wish to consider:

- Lone-worker arrangements and equipment provision (e.g. personal alarms)
- Communication devices
- Welfare check procedures
- Escalation processes

The most appropriate measures will depend upon local circumstances and risk assessments.

Practical actions for operators

- ✓ Review room-entry procedures regularly
- ✓ Ensure staff are trained on room access and understand different room-access scenarios
- ✓ Consider lone-working arrangements and equipment provision (e.g. personal alarms)
- ✓ Encourage communication between departments
- ✓ Review procedures following incidents or concerns

Chapter 8: Building staff confidence through training

Why training matters

Procedures only work when staff understand them.

Training should therefore be viewed as one of the most important investments accommodation providers can make in guest security.

Staff can encounter situations that require judgement rather than simple compliance with rules. Effective training helps staff understand both the procedures they are expected to follow and the reasons those procedures exist.

Building confidence

Staff are more likely to make good decisions when they are trained.

Training should therefore focus not only on knowledge also on confidence and decision-making – potentially under pressure.

Topics may include:

- Guest verification
- Privacy and confidentiality
- Room access
- Conflict management
- Incident reporting
- Escalation procedures

Scenario-based learning can be particularly valuable because it reflects real operational situations.

Supporting consistency

A common cause of variation is inconsistent understanding between departments or shifts.

Training can help ensure that:

- Reception teams apply procedures consistently
- Housekeeping and maintenance teams understand room-access procedures and privacy expectations
- Managers respond consistently to escalations

Practical actions for operators

✓ Incorporate guest security into induction programmes

- ✓ Deliver refresher training regularly
- ✓ Use practical examples and scenarios
- ✓ Review learning following incidents
- ✓ Monitor consistency across departments

Chapter 9: Strengthening security through physical measures

The role of physical security

Physical security measures provide important layers of protection that support operational procedures.

While physical measures cannot eliminate risk entirely, they can reduce opportunities for unauthorised access and increase confidence for guests and staff.

Guest room security

Accommodation providers may use a variety of measures including:

- Electronic locking systems
- Self-closing doors
- Door viewers
- Secondary locking devices

The most appropriate combination will depend upon the nature of the property and its operating environment.

Building access controls

In addition to room-level controls, businesses may consider:

- Access-controlled lifts
- Restricted access corridors
- Staff-only areas
- CCTV coverage

The purpose of these measures is to support a safe and welcoming environment.

Managing master keys

Master keys require particular attention because of the level of access they provide.

Accommodation providers should consider:

- Who has access to master keys
- How keys are issued
- How keys are stored
- What happens if keys are lost
- Not allowing master keys to be removed from the property

Strong controls help protect both guests and staff.

Practical actions for operators

- ✓ Review physical security measures periodically
- ✓ Audit master-key arrangements
- ✓ Maintain security equipment appropriately
- ✓ Review access controls as buildings change
- ✓ Consider guest feedback regarding security and safety

Chapter 10: Learning from incidents and continuously improving

Continuous improvement

Guest security is not a fixed destination.

Risks change over time as technologies evolve, guest expectations develop and operating models adapt.

The most effective accommodation providers recognise that security arrangements should be reviewed and refined continually.

Learning from experience

Every organisation generates valuable learning opportunities.

These may come from:

- Incidents
- Near misses
- Guest feedback
- Staff observations
- Operational reviews

The objective should not be to allocate blame but to understand what can be improved.

Monitoring trends

Individual incidents may appear isolated. However, when viewed collectively they may reveal wider patterns.

Examples might include:

- Increasing replacement key requests
- Recurring privacy concerns
- Confusion regarding access procedures
- Training gaps

Monitoring trends (through consistent reporting and evaluation) can help businesses identify opportunities for improvement before problems become more significant.

Creating a culture of learning

Continuous improvement is most effective when staff feel comfortable sharing concerns and suggestions.

Accommodation providers should encourage:

- Open reporting
- Constructive discussion
- Learning from mistakes
- Collaboration across departments
- Opportunity for staff to share concerns

A culture of learning strengthens both guest security and staff confidence.

Practical actions for operators

- ✓ Record, report and review incidents and near misses regularly
- ✓ Analyse trends over time
- ✓ Update procedures where necessary
- ✓ Review training programmes
- ✓ Seek staff feedback
- ✓ Share learning across teams

Annex A: Quick-reference operational checklist

Please note this checklist is not exhaustive, and UKHospitality recommends operators refer to the full version when building their own practices and procedures within their specific businesses. When handling guest data, any data retained by businesses should be proportionate to its legitimate purpose, processed in accordance with applicable data protection legislation, collected and retained for the clearly defined purpose of guest security, and not kept for longer than is necessary.

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 staff 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

Annex B: Example verification framework

Accommodation providers may consider using a combination of information when verifying identity.

The priority documents to use are:

1. Government-issued photo ID
2. Other forms of official ID (e.g. bank cards)
3. Other forms of photo ID
4. Information available on phone wallets etc

Examples of relevant information include:

- Guest name
- Room number
- Arrival date
- Departure date
- Length of stay
- Booking reference
- Booking method
- Contact information
- Names of other occupants

Verification should be proportionate to the circumstances and should rely only on the minimum amount of guest info reasonably necessary to establish that the person requesting access is authorised to do so.

Annex C: Example room access decision tree

Request for room access received

↓

Is the individual listed on the booking?

→ Yes: Proceed with normal verification process.

→ No: Continue assessment.

↓

Can authorisation be obtained from the named guest?

→ Yes: Record and proceed in accordance with local procedures.

→ No: Do not grant access until appropriate verification and authorisation can be completed.

↓

Escalate concerns where necessary.

Annex D: Legislative framework

Accommodation providers should ensure that guest security arrangements align with relevant legal obligations.

Depending on circumstances, these may include:

- Health and Safety at Work etc. Act 1974
- Management of Health and Safety at Work Regulations 1999
- Occupiers' Liability Acts 1957 and 1984
- UK General Data Protection Regulation
- Data Protection Act 2018
- Equality Act 2010
- Worker Protection Act 2023

This report is intended to support good practice and should not be regarded as legal advice.