

Buildings Security Assessment Form & Action Plan

*This form is based on the General Practice Risk Assessment provided by Adam Tuckett Avon IM&T Consortium –
With thanks to IG toolkit resource pack)*

Building Assessed: 168 Medical (Newcourt)

Assessed By: Natalie Ryan

Date of risk assessment: 10/08/2026

Date of previous risk assessment: 04/09/2025

1. Is access to the outside of the building controlled i.e. covered by CCTV?		
Yes	Risk Level: Low	Action Plan: Outside covered by visible CCTV
2. Does the outside of the building have security lighting, floodlighting or street lighting?		
Yes	Risk Level: Medium	Action Plan: Lighting at entrance, the side of the building and in car park.
3. Are there warnings on windows, visible alarms etc that warn potential intruders that there are physical security measures in place?		
No	Risk Level: Medium	Action Plan: No signage but alarms and CCTV visible
4. Are accessible windows suitably protected with locks?		
Yes	Risk Level: Low	Action Plan: All low windows are only accessible via a locked gate
5. Do the downstairs windows have security bars?		
No	Risk Level: Medium	Action Plan:
6. Are the windows closed and checked every evening?		
Yes	Risk Level: Medium	Action Plan:

Buildings Security Assessment Form & Action Plan

*This form is based on the General Practice Risk Assessment provided by Adam Tuckett Avon IM&T Consortium –
With thanks to IG toolkit resource pack)*

7. Are blinds closed and checked every evening?		
Yes	Risk Level: Low	Action Plan: Part of Host base closure procedure, if required
8. Are skylights suitably protected by bars and locks?		
N/A	Risk Level: High/Low/Medium	Action Plan:
9. Are external doors suitably protected e.g. by 5 lever locks?		
Yes	Risk Level: Medium	Action Plan:
10. Is there a burglar alarm with intruder monitors covering all areas especially those containing IT equipment or records?		
Yes	Risk Level: Medium	Action Plan:
11. Is the alarm system connected to a police station or call response centre?		
Yes	Risk Level: Medium	Action Plan: Connected to an Alarm Centre
12. Are you able to ensure all keys stored on site are not obvious and any instructions regarding key instructions or keypad codes are stored securely?		
Yes	Risk Level: Medium	Action Plan:
13. Are keypad codes changed regularly?		
Yes	Risk Level: Medium	Action Plan:
14. Are alarm codes changed regularly?		
N/A	Risk Level: Medium	Action Plan: 168 are responsible for changing codes and

Buildings Security Assessment Form & Action Plan

*This form is based on the General Practice Risk Assessment provided by Adam Tuckett Avon IM&T Consortium –
With thanks to IG toolkit resource pack)*

notifying the operational team.		
15. Are staff aware of the procedure for challenging unidentified visitors in controlled areas?		
Yes	Risk Level: Low	Action Plan: Staff are aware of challenging unidentified visitors and what to do to call for help when needed.
16. Do staff ensure that the Drug Cupboard or the access to the Drug Cupboard is logged and managed appropriately?		
Yes	Risk Level: Medium	Action Plan: Drug cupboard locked at all times and key held within a keysafe.
17. Do staff ensure that paperwork is not left unattended in the Consultation Area or other sensitive areas?		
Yes	Risk Level: Low	Action Plan: Data protection and GDPR training is compulsory for all operational teams
18. Are screensavers in use on computers that are used to display information about patients?		
Yes	Risk Level: Low	Action Plan:
19. Are identity passes/cards worn by all staff at all times?		
Yes	Risk Level: Low	Action Plan: Staff required to wear name badges at all times
20. Are visitors escorted at all times in secure areas?		
Yes	Risk Level: Low	Action Plan: Visitors are required to sign into the visitors book and provided with an identifying lanyard.
21. Is a log of visitors maintained?		
Yes	Risk Level:	Action Plan:

Buildings Security Assessment Form & Action Plan

*This form is based on the General Practice Risk Assessment provided by Adam Tuckett Avon IM&T Consortium –
With thanks to IG toolkit resource pack)*

Low		
22. Is IT equipment situated where it cannot be viewed by visitors or the public from outside the premises?		
Yes	Risk Level:	Action Plan:
Low		
23. Are deliveries to and collections from the site, supervised?		
Yes	Risk Level:	Action Plan:
Low		
24. If a back door or loading bay is used to receive deliveries – is this secured when not in use?		
N/A	Risk Level:	Action Plan:
High/Low/Medium		
25. Is new equipment stored securely prior to installation?		
Yes	Risk Level:	Action Plan:
Low		
26. Is the movement of IT equipment out of the site subject to authorisation and control? i.e. use of laptops and portable equipment off site.		
Yes	Risk Level:	Action Plan:
Low		
27. Are lock down devices used to secure IT equipment?		
No	Risk Level:	Action Plan:
Low		
28. Are laptops and other portable equipment stored securely overnight?		
Yes	Risk Level:	Action Plan: Kept in secure cupboard
Low		
29. Are back-up Tapes stored securely, for example in the site safe?		
N/A	Risk Level:	Action Plan:

Buildings Security Assessment Form & Action Plan

*This form is based on the General Practice Risk Assessment provided by Adam Tuckett Avon IM&T Consortium –
With thanks to IG toolkit resource pack)*

High/Low/Medium		
30. Is IT equipment asset marked?		
Yes	Risk Level: Low	Action Plan:
31. Do assets have visible ID markings?		
Yes	Risk Level: Low	Action Plan:
32. Is electronic equipment stored away from the risk of burst water pipes?		
Yes	Risk Level: Low	Action Plan:
33. Is electronic equipment stored away from the risk of splashing from taps or sinks and the risk of water running from windows or condensation?		
Yes	Risk Level: Low	Action Plan:

Any there any other observations from the review?

Date of Next Review: 10/08/2027

Review Carried Out By: Natalie Ryan

Action Plan Follow-up Date N/A