

CCTV and Covert Monitoring Policy

Policy on a page

1 What is the CCTV and Covert Monitoring Policy?

This policy outlines Howes Percival's approach to the use and operation of CCTV to ensure compliance with relevant laws.

2 Why is the CCTV and Covert Monitoring Policy important?

This firm has a responsibility to explain when we use CCTV, the purpose of using CCTV and how any Data recorded by CCTV cameras will be processed in accordance with our Data Protection Policy and Data Retention Policy and Schedules to ensure we are compliant with UK GDPR and confirm the firm's best practice.

3 Who should I speak with if I have, or my client has, a question about our use of CCTV?

Hannah Steggles, the Data Protection Officer (DPO) for the firm is always the best person to ask about our use of CCTV or anything data protection related. In the event that Hannah is unavailable, James Howarth acts as the Deputy DPO and can also assist.

4 What happens if I fail to meet my responsibilities outlined in this policy?

A failure to fulfil your responsibilities, as defined in this policy, could lead to disciplinary action. The firm take risk management seriously and expect all partners, consultants and staff to follow this policy.

CCTV and Covert Monitoring Policy

1 Scope

- 1.1 This Policy sets out Howes Percival LLP's ("**we**", "**our**", "**us**", the "**Firm**") position in relation to the use and operation of CCTV at our Leicester, Northampton and Norwich offices. As a result, and to ensure compliance with the UK General Data Protection Regulation ("**UK GDPR**") and related data protection laws (including, the Information Commissioner's Code of Practice for surveillance cameras and personal information) ("**the Data Protection Laws**"), the Firm has implemented this policy on the use of its CCTV system and in particular the collection and processing of Personal Data obtained from it.
- 1.2 This policy should be read in conjunction with the Firm's Data Protection Policy (the "**DP Policy**"). Unless stated otherwise, this policy adopts the definitions set out in the DP Policy.
- 1.3 We believe that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff, clients and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns. Images recorded by surveillance systems are Personal Data which must be processed in accordance with the Data Protection Laws. We are committed to complying with our legal obligations and ensuring that the legal rights of visitors, clients, employees, workers, consultants and partners, relating to their personal data, are recognised and respected.

2 Status

- 2.1 This policy is non-contractual and may be varied or withdrawn, at any time, without notice.
- 2.2 This policy is applicable to all partners, consultants, staff (both permanent and temporary including contractors and agency workers) and work experience students.
- 2.3 This policy may also be applicable to visiting members of the public and clients who visit our Northampton and/or Norwich and/or Leicester office from time to time.
- 2.4 This policy is regularly reviewed and monitored for applicability and effectiveness and will be reviewed if substantive change occurs. If no substantive change occurs the policy will be reviewed, at least, annually.
- 2.5 This policy was last reviewed by the Data Protection Officer on 2 February 2026.

- 2.6 This policy was approved on behalf of the firm by the Board and Practice Group Leaders (PGLs) in February 2026.

3 Definitions

- 3.1 This policy adopts the definitions set out in the DP Policy with the following additional terms which have the following meanings:
- 3.1.1 **CCTV:** means fixed and domed cameras designed to capture and record images of individuals and property. The Firm currently operates CCTV at its Northampton, Leicester and Norwich offices.
- 3.1.2 **Data:** in respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.
- 3.1.3 **Surveillance systems:** means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

4 Policy Statement

- 4.1 We currently use CCTV cameras to view and record individuals at our Northampton, Leicester and Norwich Offices. Our Northampton office is based at Nene House, 4 Rushmills, Northampton, NN4 7YB. Our Norwich office is based at Flint Buildings, 1 Bedding Lane, Norwich, NR3 1RG. Our Leicester office is based at 3 The Osiers Business Centre, Laversall Way, Braunstone Town, Leicester LE19 1DX.
- 4.2 This policy outlines why we use CCTV, how we will use CCTV and how we will process Data recorded by CCTV cameras to ensure we are compliant with the Data Protection Laws and best practice.
- 4.3 We recognise that information that we hold about individuals is subject to the Data Protection Laws. We are committed to complying with all our legal obligations under the Data Protection Laws. The images of individuals recorded by CCTV cameras are Personal Data therefore are subject to the Data Protection Laws.
- 4.4 A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

5 Personnel Responsible

- 5.1 The Firm's Data Protection Officer has been delegated responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed is the Data Protection Officer's responsibility. Day-to-day operational responsibility for CCTV cameras and the storage of Data recorded is the responsibility of Wayne Mardel, Facilities and Health & Safety Manager.

6 Reasons for the Use of CCTV

- 6.1 As set out above, we currently use CCTV at our Northampton, Leicester and Norwich offices. We believe that such use is necessary for our legitimate business purposes, including;
- 6.1.1 to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime,
 - 6.1.2 for the personal safety of employees, workers, consultants and partners, visitors and other members of the public and to act as a deterrent against crime,
 - 6.1.3 to support law enforcement bodies in the prevention, detection and prosecution of crime,
 - 6.1.4 to assist in day-to-day management, including ensuring the health and safety of staff and others,
 - 6.1.5 to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings, and
 - 6.1.6 other purposes as set out in any Privacy Notices or Privacy Policies issued from time to time.
- 6.2 This list is not exhaustive, and other purposes may be or become relevant.

7 Monitoring

- 7.1 CCTV monitors the entrance to our Northampton car park, giving a view of the barrier arm, keypad and intercom, and monitors the front entrance to our Northampton building and an area of the car park which is part of our demise. It primarily covers cars entering our

car park and individuals visiting our offices. The CCTV operates for 24 hours a day, and this Data is continuously recorded.

- 7.2 At our Norwich office, the CCTV monitors the main reception entrance (inner and outer doors), the entrance to the car park and the alleyway from the car park to the main road. It primarily covers those visiting our offices (but is angled so as not to cover members of the public walking by) and cars entering our car park. Again, the CCTV operates for 24 hours a day, and this Data is continuously recorded.
- 7.3 At our Leicester office, the CCTV monitors the main entrance, the car park and the full perimeter of the building. It primarily covers those visiting our offices (but is angled so as not to cover members of the public walking by) and cars entering our car park. Again, the CCTV operates for 24 hours a day, and this Data is continuously recorded.
- 7.4 Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property.
- 7.5 Images are monitored by authorised personnel during working hours every day, the Northampton, Leicester and Norwich offices are open for business.
- 7.6 Employees/partners using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant Data.

8 How we operate any CCTV

- 8.1 Where CCTV cameras are placed in the workplace, we will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. Such signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.
- 8.2 Live feeds from CCTV cameras can be viewed by our employees who are at reception in the relevant office, and this is only done where reasonably necessary to allow those employees to view individuals prior to allowing them to enter the premises.
- 8.3 We will ensure that recorded images are only viewed by approved employees/partners whose role requires them to have access to such Data. This may include HR employees, IT personnel and partners/employees responsible for making decisions in connection with the use of CCTV images and Data. Recorded images will only be viewed in a secure and restricted manner.

9 Storage of Data gathered by CCTV

- 9.1 In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that Data gathered from CCTV cameras is stored in a way that maintains its integrity and security. Currently such Data are stored on internal hard drives and are overwritten every three weeks.
- 9.2 We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

10 Retention and Erasure of Data gathered by CCTV

- 10.1 The Data from the CCTV at our Northampton office is stored on a 2TB internal hard drive and is stored for 21 days on such hard drive (such storage is on a loop (so the oldest Data is overwritten every three weeks).
- 10.2 The Data from the CCTV at our Norwich office and Leicester offices is each stored on a 4TB internal hard drive, and such Data is stored for 30 days (such storage is on a loop (so the oldest Data is overwritten every three weeks).
- 10.3 If Data needs to be retained beyond the time periods set out in paragraph 10.1 and 10.2, and subject to authorisation being received from the Data Protection Officer, it will be stored separately and securely. Generally, such Data will not be stored longer than is necessary for the purpose for which the Data is needed and in accordance with our Data Retention Policy and Schedule. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, Data will be kept long enough only for incidents to come to light. In all other cases, recorded images will be kept for no longer than 2 months (subject to paragraph 10.5 below)
- 10.4 Data from the CCTV system may be retained for longer than that stated in paragraph 10.1, 10.2 and 10.3 above, in the following circumstances:
- 10.4.1 we are required by law enforcement bodies to preserve evidence from a CCTV recording,
- 10.4.2 we require the Data to establish, exercise or defend claims involving the Firm, or
- 10.4.3 if otherwise required by law (which includes any court order served on us) to store the Data for a longer period.

- 10.5 At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

11 Use of additional Surveillance Systems

- 11.1 Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a Data Privacy Impact Assessment (**DPIA**).
- 11.2 A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.
- 11.3 Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better alternative solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.
- 11.4 No surveillance cameras will be placed in areas where there is an expectation of privacy unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

12 Covert Monitoring

- 12.1 We will only engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) in highly exceptional circumstances. This includes, but is not limited to, instances where there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no alternative less intrusive way to tackle the issue.
- 12.2 In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the Data Protection Officer and the Board. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision.

- 12.3 Any covert monitoring that does take place will be carried out only by those authorised by the Firm to do so.
- 12.4 Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

13 Ongoing Review of CCTV Use

- 13.1 We will ensure that the ongoing use of existing CCTV cameras in the workplace is reviewed periodically to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

14 Requests for Disclosure

- 14.1 No images from our CCTV cameras will be disclosed to any third party, without express permission being given by the Data Protection Officer. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.
- 14.2 In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.
- 14.3 We will maintain a record of all disclosures of CCTV footage.
- 14.4 No images from CCTV will ever be posted online or disclosed to the media.

15 Subject Access Requests

- 15.1 Data subjects may make a request for disclosure of their personal information, and this may include CCTV images (**Data Subject Access Request**). A Data Subject Access Request is subject to the statutory conditions from time to time in place and should be made in writing, in accordance with our DP Policy (see paragraph 17 of the DP Policy).
- 15.2 In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.
- 15.3 We reserve the right to obscure images of third parties when disclosing CCTV Data as part of a subject access request, where we consider it necessary to do so.

16 Complaints

- 16.1 If you have questions about this policy or any concerns about our use of CCTV, then you should speak to the Data Protection Officer in the first instance.
- 16.2 Where this is not appropriate or matters cannot be resolved informally, employees should use our formal grievance procedure.
- 16.3 You also have the right to complain at any time to the Information Commissioner’s Office.

17 Individual Data Protection Rights

- 17.1 As a data subject, you have a number of individual rights when it comes to how we handle your Personal Data. Details of those rights are set out in paragraph 16 of the DP Policy.

Change History Record

Version	Revision Description	Date Revised
2.0	Update to include Norwich CCTV and annual review	19/01/2024
3.0	Annual review and moved to new branding template	15/10/2024
4.0	Update to include Leicester CCTV and review	02/02/2026