



## **CCTV POLICY for Smart Doorbell cameras with recording facilities**

***Do not devise harm against your neighbour, while he lives securely  
beside you  
(Proverbs 3:29)***

<b>Reviewed and updated by Headteacher</b>	<b>April 2025</b>
<b>Date ratified by the Chair of Governors</b>	<b>April 2025</b>
<b>Review Cycle</b>	<b>Bi-Annually or when there is a change in statutory guidance or legislation</b>
<b>Review Date</b>	<b>April 2027</b>

**This Policy is based on the model policy provided by Somerset Local Authority**

## Contents

1. [Introduction](#)
2. [About this policy](#)
3. [The Data Protection Principles and Privacy by Design](#)
4. [Responsibilities of the Trust/Academy/School](#)
5. [Responsibilities of the Data Protection Officer](#)
6. [Responsibilities of the headteacher](#)
7. [Purpose and justification](#)
8. [How the Trust/Academy/School manages the doorbell](#)
9. [Security](#)
10. [Storage and retention of images](#)
11. [Subject Access Requests](#)
12. [Access and disclosure to other third parties](#)
13. [Complaints](#)

## Contacts and Review Information

Data Protection Officer

[dposchools@somerset.gov.uk](mailto:dposchools@somerset.gov.uk)

School Data Protection Lead

[CrowcombeOffice@crowstog.co.uk](mailto:CrowcombeOffice@crowstog.co.uk)

## Introduction

- 1.1. At Crowcombe and Stogumber Cof E Primary School, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use a Smart Doorbell to ensure that we can see who is visiting the Crowcombe Cof E Primary School site. The Smart Doorbell, with recording facility, collects images (personal data) of individuals that may be used by the school for specific purposes.
- 1.2. The purpose of this policy is to manage and regulate the use of the Smart Doorbell at Crowcombe Cof E Primary School and ensure that:
  - We comply with the UK GDPR
  - The images that are captured are useable for the purposes we require them for.
  - We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation and their rights are being upheld.
- 1.3 The Smart Doorbell we are using has a recording facility and captures still images of people who could be identified, as well as information relating to individuals for any of the following purposes:
  - Observing who is visiting the school
  - Using images of visitors to investigate potential criminal activity

## About this policy

- 2.1 This policy has been created with regard to the following statutory and non-statutory guidance:
  - Home Office (2013) '[The Surveillance Camera Code of Practice](#)'
  - Information Commissioner's Office (ICO) (2014) '[CCTV Code of Practice](#)'
  - The ICO's guidance on [Smart Doorbells](#)
- 2.2 This policy has due regard to legislation including, but not limited to, the following:
  - The UK General Data Protection Regulation
  - The Data Protection Act 2018
  - The Freedom of Information Act 2000
  - The Protection of Freedoms Act 2012
  - The Regulation of Investigatory Powers Act 2000

2.3 This policy operates in connection with the following Crowcombe and Stogumber Cof E Primary Schools policies:

- Data Protection and Freedom of Information Policy
- Digital Images Policy
- Security Policy (if applicable)

## The Data Protection Principles and Privacy by Design

3.1 Data collected from the Smart Doorbell will be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date;
5. Kept for no longer than is necessary for the purposes for which the personal data are processed;
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3.2 The Crowcombe Cof E Primary School will follow the ICO's guidelines on Privacy by Design – before planning installing and using the Smart Doorbell, the Crowcombe Cof E Primary School will:

- Consider whether the Crowcombe Cof E Primary School can fulfil its requirements through a less privacy-intrusive system that does not include recording.
- Carry out a Data Privacy Impact Assessment (DPIA) to assess security risks and how the rights of individuals will be upheld.
- Identify a lawful basis for the use of the Smart Doorbell.

## Responsibilities of the School

4.1 The school, as the corporate body, is the data controller. The governing board of Crowcombe and Stogumber Cof E Primary Schools therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

4.2 The role of the data controller includes:

- Processing Smart Doorbell footage legally and fairly
- Collecting Smart Doorbell footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting Smart Doorbell footage that is relevant, adequate and not excessive in relation to the reason for its collection.

- Ensuring that any Smart Doorbell footage identifying an individual is not kept for longer than is necessary.
- Protecting Smart Doorbell footage containing personal data against accidental, unlawful destruction, alteration, and disclosure.

## Responsibilities of the Data Protection Officer

- 5.1 As a school we are data controllers in law and are required to appoint a Data Protection Officer. Our DPO is Amy Brittan and can be contacted at [dposchools@somerset.gov.uk](mailto:dposchools@somerset.gov.uk)
- 5.2 The DPO is responsible for ensuring compliance with current Data Protection legislation and with this policy. Their responsibilities are laid out in the Data Protection policy, but in relation to the Smart Doorbell they include:
- Ensuring that all data controllers at the school handle and process footage in accordance with the 6 data protection principles.
  - Ensuring that footage is obtained in line with legal requirements.
  - Supporting the School to complete a Data Privacy Impact Assessment when installing or replacing the doorbell (see paragraph 3.2).
  - Reviewing the effectiveness of the current system and making recommendations if appropriate.
  - Ensuring that footage is destroyed in line with legal requirements when it falls outside of its retention period.
  - Informing data subjects of how their data captured in footage will be used by the School; their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.

## Responsibilities of the headteacher

- 6.1 The headteacher has the following responsibilities:
- Meeting with the DPO to decide where the Smart Doorbell is needed to justify its means.
  - Liaising with the DPO regarding the lawful processing of the footage.
  - Reviewing this policy to ensure it is compliant with current legislation.
  - Monitoring legislation to ensure the school is using the Smart Doorbell fairly and lawfully.
  - Communicating any changes to legislation to all members of staff.

## Purpose and justification

- 7.1 The school will only use the Smart Doorbell for the safety and security of the school and its staff, pupils and visitors by verifying the identity of individuals.

- 7.2 The school may share doorbell footage to assist the police in identifying persons who have committed an offence (see paragraph 12.1).
- 7.3 The school may use footage as part of disciplinary and grievance processes. This will be communicated to students and staff through the school Privacy Notices.
- 7.4 If the doorbell is no longer required the school will deactivate and remove it.

## How the school manages the doorbell

- 8.1 The school is registered as a data controller with the Information Commissioner's Office, which also covers the use of Smart Doorbells.
- 8.2 Signage is clearly and prominently placed by the doorbell to the school, informing individuals that they are being recorded on the camera.
- 8.3 The doorbell will not record audio by default, as audio recording may be considered an excessive intrusion of privacy. If audio recording is possible, this option will be turned off.
- 8.4 The doorbell will not be trained on private vehicles or property outside the perimeter of the school. The camera on the doorbell faces forward and can not pan or focus in on any other location.

## Security

- 9.1 The doorbell is a standalone entry system, it is not networked. Access to the doorbell software is only permitted by authorised school staff.
- 9.2 The school's authorised doorbell administrators are:
  - Mrs Kate Lewis, Headteacher
  - Ms Kate McCrimmon, Office Administrator
- 9.3 A visual display monitor for the doorbell is located in the main office, headteachers office and main hall. The monitor screen is not in sight of the general public and is turned off when there is no requirement to view live images.
- 9.4 The doorbell will be tested for security flaws once a term to ensure it is properly maintained at all times.
- 9.5 Any unnecessary footage captured will be securely deleted from the system.

## Storage and retention of images

- 10.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.
- 10.2 The footage is kept on a rolling 100 images unless there is a current incident that is being investigated;
- 10.3 All retained data must be stored in a searchable system. Only a primary copy should be kept, and secondary copies should only be created in exceptional circumstances.

## Subject Access Requests (SARs)

- 11.1 Individuals have the right to request access to video footage relating to themselves under the Data Protection Act 2018.
- 11.2 All requests should be made to the Headteacher or the Data Protection Officer. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified, for example, date, time and location. Requests may be written or verbal.
- 11.3 The school will immediately indicate receipt and then respond within one calendar month of receiving the request.
- 11.4 The school reserves the right to refuse access to video footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.
- 11.5 All attempts will be made to allow the viewing of the footage. If others can be identified, the school will assess the risk to others from the video being viewed by the requester. If there is likely to be a risk of harm, the school may consider the following options where appropriate:
  - Obtain the consent of others to share the video with the requester;
  - Use video-editing software to blur the faces of others who can be identified from the video;
  - Provide selected still images from the footage and blur the identifiable faces;
  - Provide a transcript or written description of the contents of the footage.
- 11.6 If all options have been considered and the school still consider there to be a risk to others from the requester viewing the footage, the school may decline the request to view the footage (although relevant exemptions in the Data Protection Act 2018 will need to be identified by the school provided to the requester).

- 11.7 The school should not provide copies of the footage to others unless instructed to do so in law or there is no risk to individuals who may be identifiable from the footage.

## Access to and disclosure to other third parties

- 12.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators) and with the correct authorisation.
- 12.2 Requests from third parties should be made in writing to the Headteacher/Governing Body or the Data Protection Officer. However, consideration must also be given to the following paragraph (12.3)
- 12.3 Consideration should always be given to the safeguarding and best interest of pupils. Data Protection should not be used as an excuse to prevent the viewing of images if there is an overwhelming need. All disclosures and the reasons for release should be recorded.
- 12.4 The data may be used within the school's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures. This will be communicated to staff through the school Privacy Notices.

## Complaints

- 13.1 Complaints and enquiries about the operation of the doorbell within the school should be directed to the Headteacher/Governing Body or the Data Protection Officer in the first instance.