



PILSLEY PARISH COUNCIL

DATA PROTECTION AND CCTV POLICY

POLICY STATEMENT REFERENCE NUMBER	ADOPTED DATE	REVIEW DATE
1	May 2024	May 2025

DATA PROTECTION and CCTV POLICY

Introduction

The Data Protection Act 1998 regulates the processing of information relating to individuals. This includes the obtaining, holding, using, or disclosing of such information, and covers computerised records as well as paper filing systems and records. The Parish Council will hold the minimum personal information necessary to enable it to perform its functions. All such personal information is confidential and will be treated with care in order to comply with the law.

Summary of Data Protection Principles

Data users must comply with the Data Protection principles of good practice which underpin the Act.

These state that personal data shall:

1. Be obtained and processed fairly and lawfully (that the subject of the data has consented to its collection and use).
2. Be held only for specified purposes.
3. Be adequate, relevant, and not excessive.
4. Be accurate and kept up to date.
5. Be held for no longer than necessary.
6. Be accessible to data subjects under the Act.
7. Be subject to the appropriate security measures.
8. Not be transferred outside the Parish Council or to any country outside of the EEA unless it has adequate protection relating to the processing of data.

The Parish Council holds and processes information about its staff, Councillors, contractors and, where appropriate, members of the public. The Data Protection Act 1998 ("The Act") covers both computerised and manual records which contain personal data and sets out a number of rights and principles which those who use personal information, such as the Parish Council must follow. The Parish Council will keep some forms of information longer than others in line with financial, legal or archive requirements.

Responsibilities

All staff or councillors who process, have access to or use personal data must ensure that they familiarise themselves with this policy and any data security policy and abide by the principles set out in the policy at all times. This policy has been developed to ensure this happens.

Staff and councillors owe a duty of confidence which extends to handling of personal data. If you record or process personal data in any form you must ensure that you comply with this Policy and the requirements of the Act.

The Council has overall responsibility for the Data Protection Policy. The Clerk is responsible for making sure the policy and procedures for handling requests and complaints are in place and are understood by councillors and people working for the council.

It is the responsibility of the individual collectors, keepers, and users of personal data to apply the provisions of the Data Protection Act. Therefore, staff are required to be aware of the provisions of the Data Protection Act 1998, such as keeping records up to date and accurate, and its impact on the work they undertake on behalf of the Parish Council.

Any breach of the Data Protection Policy, whether deliberate, or through negligence may lead to disciplinary action being taken.

All staff are responsible for ensuring that: -

- They comply with this policy and internal procedures for handling access requests.
- Any personal data held, electronic or paper format, is kept securely.
- Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.
- They promptly forward all initial requests for personal data (known as subject access requests) to the Clerk; and when asked to do so, provide responses promptly to requests and reviews.
- The information provided to the Parish Council in connection with their employment is accurate and as up to date as possible.

What does the Act apply to?

The Act applies to both manual and electronically held data. The Act will also apply to emails that contain personal data about individuals sent or received by Parish Council staff or Councillors. Subject to certain objections, individual data subjects will be entitled to make a request and have access to information (including e-mails) containing personal data concerning them provided that they can provide sufficient information to us to locate the relevant emails.

Sensitive Personal Data

The Parish Council may from time-to-time process sensitive personal data regarding employees or individuals that it deals with. "Personal data" relates to living individuals that could be identified by the information. "Sensitive personal data" is information as to a data subject's racial or ethnic origin, political opinion, religious beliefs, trade union membership, sexual orientation, or marital status, physical or mental health, offences or alleged offences and information relating to criminal proceedings. This information may be processed for equal opportunity monitoring or to meet the needs of individuals with disabilities, or for disciplinary proceedings or other legal obligations. Any personal or sensitive data that the Parish Council holds will only be held for the purposes for which it was gathered.

Data Subjects' consent

Certain types of personal data may be processed for particular purposes without the consent of the individual data subject. The Act also allows for certain third parties to have access to personal data without the consent of the individual concerned. However, it is the Parish Councils policy to seek express consent wherever practicable. This allows individuals an opportunity to raise any concerns.

or objections. The Parish Council will consider any such objections but reserves the right to process personal data in order to carry out its functions as permitted by law.

Right to Access Personal Data

Councillors, staff (past and present), members of the public and individuals who have dealings with the Council have a right to access personal data that is being held about them in so far as it falls within the scope of the Act and to request the correction of such data where it is incorrect.

The Act gives rights to individuals in respect of personal data held about them by others.

The rights are: -

- a) Right of subject access.
- b) Right to prevent processing likely to cause damage or distress.
- c) Right to prevent processing for the purpose of direct marketing.
- d) Right in relation to automated decision making.
- e) Right to take action for compensation if the individual suffers damage or distress in contravention of the Act.
- f) Right to take action to rectify, block, erase or destroy inaccurate data.
- g) Right to make a request to the Information Commissioner's Office for an assessment to be made as to whether the provisions of the Act have been contravened; and
- h) Right to compensation- compensation can be claimed by the data subject from a data controller for damage or damage and distress caused by any breach of the Act.
(Compensation for distress alone can only be claimed in limited circumstances.)

How to make a Data Access Request

All requests for access to data held by the Parish Council should be formally requested in writing to the Parish Clerk, Homestead Farm. 10 Alfreton Road, Newton, Derbyshire, DE55 5TP.

Fee Charging

The Council's publication scheme details a charge of 10p per A4 sheet, on each occasion that access is requested. Before any information is disclosed, we require payment of the fee and will advise the requester in writing of the total cost.

Once full details of a request have been received with the relevant fee **and identity** has been confirmed, the Parish Council will provide a response within 20 calendar days after the date of our receipt. The Parish Council does not need to comply with a request where it has received an identical or similar request from the same individual unless a reasonable interval has elapsed between compliance with the original request and the current request.

CCTV POLICY

Introduction

This Policy is intended to specifically guide and control the management, operation, use and confidentiality of the CCTV system installed in the village by the Parish Council.

The policy will be subject to periodic review by the Parish Council to ensure that it continues to reflect the public interest and that it and the system meets all legislative requirements. The Parish Council accepts the Data Protection Principles of the 1998 Act as follows:

- Data must be fairly and lawfully processed,
- Processed for limited purposes and not in any way incompatible with those purposes,
- Adequate, relevant, and not excessive,
- Accurate and secure,
- Not kept for longer than is necessary,
- Processed in accordance with individual's rights,
- Subject to guidance on good practice,
- Not transferred to countries without adequate protection,

Statement of Purpose

The underlying purpose of the CCTV system installed in the village by the Parish Council is to provide a safe and secure environment for the benefit of those who might visit, work, or live in the area. (The system will not be used to invade the privacy of any individual, except when carried out in accordance with the law).

More specifically, the scheme will be used for the following purposes:

- To reduce the fear of crime of people living or visiting Pilsley and to ensure that people are able to enter and leave the area without fear of intimidation by individuals or groups.
- To reduce the potential for vandalism of property and to prevent, deter or detect crime and disorder,
- To assist the police, parish council or other law enforcement agency with the identification, detection, apprehension, and prosecution of offenders by examining and using retrievable evidence relating to crime, public order, or contravention of byelaws,
- To deter potential offenders by publicly displaying the existence of CCTV having cameras clearly sited that are not hidden,
- To assist all emergency services to carry out their duties and responsibilities,

Responsibilities of the Owners of the Scheme

The Parish Council retains overall responsibility for the scheme.

Management of the System

A CCTV system prevents crime largely by increasing the risk of detection and prosecution of an offender. This policy must be read and understood by all persons involved in the operation and management of the scheme.

Day-to-day operational responsibility for the system rests with the Clerk to the Council, who will be the first point of contact about the system or, in the event of the Clerk's absence, the Chairman or Vice-Chairman of the Council.

Breaches of this policy by operators will be investigated by the Clerk to the Council and reported to the Parish Council.

Control and Operation of the System

The following points must be understood and strictly observed by anyone operating or accessing the system: -

1. Operators must act with due probity and not abuse the equipment or change any pre-set criteria to compromise the privacy of an individual.
2. The position of cameras, monitors and recorders must not be moved unless authorised in writing by the Clerk to the Council.
3. No public access will be allowed to the system except for lawful, proper, and sufficient reason, with prior approval of the Clerk of the Council or the Chairman / Vice-Chairman of the Parish Council in consultation with the Police.
4. The Police are permitted access to the system if they have reason to believe that such access is necessary to investigate, detect or prevent crime.
5. Recordings will be securely stored to comply with data protection and should only be handled by the essential minimum number of persons. Digital images will be erased after a period of 1 month.
6. Images will not normally be supplied to the media, except on the advice of the Police if it is deemed to be in the public interest. The Clerk of the Council would inform the Chairman of the Council of any such circumstances.
7. As records may be required as evidence in Court, each person handling a recording may be required to make a statement to a police officer and sign an exhibit label. Any images that are handed to a police officer should be signed for by the police officer and information logged to identify the recording and show the officer's name and police station. The log should also show when such information is returned to the Parish Council by the police and the outcome of its use.
8. Any event that requires checking of recorded data should be clearly detailed in the log of incidents, including Crime numbers if appropriate.
9. Any damage to equipment or malfunction discovered by an operator should be recorded by the Clerk as soon as possible and contact made with the company responsible for maintenance. Such contact shall be logged together with a corresponding log when a repair has been made.
10. Any request by an individual member of the public for access to their own recorded image must be made on an 'Access Request Form' and is subject to the standard fee. Forms are available from the Parish Clerk and will be submitted to the next meeting of the Parish Council for consideration and reply, normally within 40 days.

Accountability

Copies of the CCTV Policy are available in accordance with the Freedom of Information Act, as are any reports that are submitted to the Parish Council providing it does not breach security needs.

The Police will be provided with a copy of this CCTV Policy.

Any written concerns, complaints, or compliments regarding the use of the system will be considered by the Parish Council, in line with the existing complaints policy.