SOUTHWATER PARISH COUNCIL

CONFIDENTIALITY POLICY

Reviewed:	February 2025
Approved:	Full Council – 29th November 2017
Review Period:	3 years
Next Review Date:	February 2028

INDEX

Contents

1. Introduction

1.1. Whilst it is the Council's intention that all information is transparent and accessible to the public, certain information may be restricted. This will be in line with its Data Protection Policy, Publication (Freedom of Information) Policy and Transparency Regulations.

1.2. This policy aims to protect confidential and sensitive information from unauthorised disclosure, ensuring compliance with the Data Protection Act 2018 and UK GDPR

2. Information Disclosure Rules, Confidentiality and Individual Liability

2.1. The Parish Council and individuals could be held liable if proprietary, confidential or personal information is deliberately, inadvertently or prematurely revealed through written correspondence, a web site or electronic communication. Staff and councillors are therefore prohibited from revealing such information that they have not been authorised to do so. Such information includes but is not limited to:

- financial information not already publicly disclosed through authorised channels.
- client information.
- employee information.
- electoral information.
- operational information.
- information provided to the Parish Council in confidence or under a non-disclosure or other agreement.
- computer and network access codes and similar or related information that might assist unauthorised access.
- legal proceedings, except as required by law or legal representatives.
- information that might provide an external organisation with a business advantage.

computer programs and databases, including their contents.

2.2. The Council will ensure that any confidential information it holds is only accessible to those with a legitimate need. All councillors and staff must acknowledge their responsibility to handle confidential information appropriately.

2.3. Any breaches of this policy may result in disciplinary action and/or legal consequences in accordance with the Council's **Data Protection Policy** and relevant employment policies.

3. Good Practice

3.1 When sending confidential external emails to multiple individuals (where recipients are not required to know who else the email has been sent to) use the "**BCC**" (blind courtesy copy) field.

3.2 Confidential documents should be stored securely, whether in digital or physical form, and only shared with authorised individuals. Digital files should be password-protected or encrypted where necessary.

3.3 Discussions involving confidential matters should take place in appropriate settings, ensuring that unauthorised individuals do not overhear sensitive conversations.

3.4 If a councillor or employee becomes aware of a potential breach of confidentiality, they must report it immediately to the Executive Officer for investigation.

3.5 When disposing of confidential documents, use shredding or secure disposal methods rather than standard waste disposal.

3.6 Employees and councillors should exercise caution when using personal devices for Council business and must ensure confidential data is not inadvertently shared or accessed by unauthorised individuals.

4. Monitoring and Review

4.1 The Council will review and update this policy as required to ensure compliance with legislation and best practices.