

Subject: Project Outline - Review of BPC's compliance with data protection legislation

Date: 8 July 2026

Author: A Thom, Clerk

1. Context

- 1.1. The 25/26 internal audit noted that BPC's data protection policies require review
- 1.2. The last data audit was done in 2018 this is being reviewed.

2. Legislation

- 2.1. Local councils are subject to the General Data Protection Regulations (GDPR) 2018 and the UK Data Protection Act 2018.
- 2.2. This Legislation places obligations on BPC when handling personal data. If a living person can be identified from the data then it is personal data. ie this definition is broader than just a name, address, or phone number.
- 2.3. A small parish council is not expected to operate like a large organisation, but it must be able to show that it has identified its data, assessed risks, documented decisions and taken reasonable steps to protect personal information.

3. Data Protection Roadmap (NALC)¹

- 3.1. Mapping what data you hold and why
- 3.2. Identifying the lawful basis for each purpose
- 3.3. Assessing risks and protecting people's rights
- 3.4. Creating policies and embedding good practice

4. Project objective

To review BPC compliance with UK GDPR and the Data Protection Act 2018 and carry out any corrective actions identified.

5. Data audit

I have started a data audit using the template provided by the internal auditor. The audit to date has identified:

- 5.1. Disposal Schedule

Add Electoral Registers to the Disposal Schedule. I have several times used the registers used beyond the relevant year to check eligibility for burial in the Blackawton Cemetery. Qualifying former resident the person must have been an inhabitant or parishioner of Blackawton for a period of not less than three years and have ceased to be resident in the parish due to their bodily or mental infirmity or sickness. I plan to retain for ten years for this purpose.

- 5.2. Note - Emails – Are kept while they are useful and relevant. I download specific emails and have set the system to delete all emails after 900 days. My reasoning is a full audit year and some leeway for ongoing projects. But not holding longer than necessary.

- 5.3. These are judgement decision and alternative approaches

6. Legal Bases

Questions about legal bases as noted in action items:

- 6.1. Does public task cover the Parish Cllrs names, phone number, PC email address on the website and in the parish newsletter (so long as that's in the privacy notice), or is consent required
- 6.2. Parish Community Website - The Parish Council operates a community website. It posts material from other organisations, groups and individuals. eg the Blackawton Beacon parish newsletter which is produced by residents associated with the Church. What is the recommended method that others use to manage compliance with data protection in this situation.
- 6.3. Legal basis for sharing the personal data of volunteers working on council projects or committees.
- 6.4. Legal basis for sharing personal data with other parties when responding to and enquiry or request.
- 6.5. Note that consent cannot be used if it cannot be freely given.
- 6.6. I have asked Devon Association of Local Councils for advice and been referred to Breakthrough Communications who are more expert in data protection.

¹<https://www.nalc.gov.uk/resource-report/data-protection-roadmap.html>

6.7. I will also ask whether it is possible for DALC with NALC to provide a list of standard PC actions and the related legal bases (with caveats). It seems to me very inefficient to for Clerks to try work this out individually. And Clerks are not expert in data protection law.

7. What data is held?

7.1. Cllrs are asked to advise where they store Parish Council data.

8. Wind Turbine Feasibility Study

8.1. An assessment is required of how the project will collect and process personal data. This should have been done before the project commenced.

8.2. I have offered training to the Steering Group (refused) and set up @blackawtoncommunity.com emails for the non-councillor members.

9. Update/create required documents

9.1. I have created a new privacy policy using the template provided by the 25/26 internal auditor and with reference to the 2018 policy.

9.2. I have created a new Public Privacy Notice using the Society of Local Council Clerks template and with reference to the 2018 Notice.

9.3. I have reviewed the Role Holders Privacy Notice

9.4. I have created a new Public Privacy Notice using the Society of Local Council Clerks template

9.5. I have created a new Councillor and Committees Data Protection Checklist using the Society of Local Council Clerks template

9.6. I have not yet created Data Breach Response Procedure and request form or and Subject Access Request Procedure and response form. DALC lists these as recommended. The internal auditor is of the view they should exist.

9.7. I think that the documents better reflect how personal data is processed.

10. Actions Identified

10.1. Consider appointing a Data Information Officer to respond in the Clerk's absence. In BPC's situation in my view this isn't required.

10.2. Cllrs and Steering Group Committee members to please complete a checklists & advise where they store Parish Council data.

10.3. Note that emails cannot be forwarded to private emails and are subject to information requests.

10.4. Assist Cllrs to automate deletion of old emails if required.

10.5. Add Electoral Registers to the Disposal Schedule.

10.6. Contract with website provider

10.7. Obtain advice on legal bases

a) Does public task cover the Parish Cllrs names, phone number, PC email address on the website and in in the parish newsletter (so long as that's in the privacy notice), or is consent required

b) Parish Community Website - The Parish Council operates a community website. It posts material from other organisations, groups and individuals. eg the Blackawton Beacon parish newsletter which is produced by residents associated with the Church. What is the recommended method that others use to manage compliance with data protection in this situation.

c) Sharing the personal data of volunteers working on council projects or committees

10.8. Wind Turbine Feasibility Study Steering Group data processing assessment.

10.9. This is an ongoing project.

Appendices

- 1.1. Data processors must abide by the six Principles of data protection:
 - a) Data processing must be fair, lawful and transparent.
 - b) Data must only be used for the reasons specified.
 - c) The controller should only process the data they need.
 - d) Data should be accurate.
 - e) Data should not be kept for longer than necessary.
 - f) Data should be kept secure, protected against unlawful processing or loss.
- 1.2. The controller is responsible for, and must be able to demonstrate compliance ('accountability')

2. Lawful Basis for processing personal information (at least one of these must apply):

- a) Consent.
- b) Contract: the processing is necessary for a contract you have with the person, or because they have asked you to take specific steps before entering into a contract.
- c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- d) Vital interests: the processing is necessary to protect someone's life.
- e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions and the task or function has a clear basis in law.
- f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the person's information which overrides those legitimate interests.

2.2. Data subject's rights

The data subject is the individual that can be identified by personal data held. Any data subject has certain rights which the data processor will need to meet.²

3. Data Controller & Processor

3.1. 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data •

3.2. 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller³

3.3. Who is a controller of personal data?

In most cases a local council will be a data controller. The ICO view is that Councillors with council information on their own computers are also likely to be a controller – and the various obligations including a requirement to have appropriate measures to safeguard personal data apply.⁴

² <https://devonalc.gov.uk/knowledge-bank/information-management/data-protection/>

³ SLCC AN174-Information-Management-Data-Protection-Data-Controller SLCC Accessed 20240624

⁴ Society of Local Council Clerks Data Protection and Freedom of Information AN174 – Information management: Data protection: Data Controller