Astley Parish Council

May 2019

Annual Report on Data Protection

Background

1. The rules governing data protection are contained in the General Data Protection Regulations ("GDPR") which took effect in the UK from 25 May 2018, and the Data Protection Act 2018.

2. This report includes the following:
    i. Data audit and risk register (identifies all of the personal data held by the Parish Council together with the lawful basis being used to process data, any risks which have been identified, and also describes any actions required).
    ii. Privacy notices
    iii. Registration with Information Commissioner's Office
    iv. Data Protection Policy (includes all the processes that will be used to manage data protection, including the procedures to be followed for subject access requests, and in the case of any data breaches).

i. Data audit and risk register

Data processing activity	What is held?	Who is the data subject?	Lawful basis for processing	Risks to personal data?	Data Controls and actions to address risks
Councillor details: Clerk retains contact details/gathered for election purposes/published in accordance with Local Government Act.	Name, address, contact details, business and property interests.	Parish Councillors	Legal Obligation	Low – personal data restricted to what is required by law, and councillors will be made aware of the publishing requirements	1. Details will be published on website in accordance with statutory requirements. 2. Data will be held by Clerk, and will be deleted when a councillor retires from office. 3. Requests for this data from third parties shall be referred to the website. 4. Councillors to be provided with a copy of the privacy notice
Employee Information	Personal details, payroll and pension information	Clerk	Legal Obligation	Low – there is just one employee (Clerk) who is responsible for processing, and it should therefore be accurate.	Clerk to be provided with a copy of the privacy notice.
Website: Information relating to PC is published on the website, and on occasions this may include personal data. Photographs on website		Members of public	Consent	Medium – people could be identified from photographs on the website.	1.Photographs of individuals shall not be published on the website without the express permission of the individual. 2. Photographs will be deleted after a maximum of two years, and no copy of the photograph shall be retained by the PC

Planning Consultations: Consultations and decisions published by Shropshire Council, and shared with Parish Council. Clerk emails details of each consultation and decision to parish councillors. Also published with agenda and minutes, and discussed in open forum. Parish council comments on application provided by SC	Email, noticeboards, website, Onedrive cloud storage	Planning applicant/resident	Public Task	Low - data is already in the public domain	1. Clerk to check all information before sharing with parish councillors, and ensure sensitive personal data is redacted wherever possible before sharing or publishing. 2. Information in agenda and minutes to include only what is necessary to identify and discuss the consultation or decision. 3. Any correspondence between PC and applicant to be in accordance with data protection principles, and to be deleted within two years.
Electoral roll provided by SC, stored by Clerk	Names, address, marital status	Parish residents	Public Task	Low - data is already in the public domain	1. Clerk to retain in a secure place. 2. Electoral roll not to be shared with any other person. 3. Clerk to answer queries from parish council/councillors as and when they arise. 4. Members of the public be directed to SC website for any electoral roll queries.
Email or letter queries from residents or from other	Name, address, contact details,		Public task	Low – risk of data loss or	1. Any email letter or other form of query received by the PC which

third parties: General queries from members of the public/residents/other parties relating to parish matters which may contain personal data.	with possible sensitive personal data, depending on the nature of the query			accidental sharing.	contains personal data will be retained for a maximum of two years. 2. Such data may be stored on the PC laptop, held by the Clerk in a secure place. 3. The agreed privacy notice shall be provided to any person who contacts the PC. 4. In accordance with the agreed privacy notice, such data shall not be shared with any third party without the express permission of the data subject.
Minutes – matters raised by members of the public at meetings Maintained and published in accordance with Local Government legislation	Names and possibly other information	Residents/ members of the public	Legal Obligation	Low – individuals could be identified from minutes, agenda or accompanying reports	Every effort should be made to avoid inclusion of personal data in agenda or minutes. Where personal data or potential identifiers cannot be avoided, these should be kept to a minimum (Members of the public who attend the public forum or the annual meeting should be warned by the Chair that the issue may be included in public minutes, and given the chance to withdraw from the meeting if they wish).

Letter/email to residents asking them to perform actions (eg trim trees or hedges) In response to requests made at PC meetings.	Names, addresses and possible other personal data.	Residents/ members of the public	Public Task	Low - risk of data loss or accidental sharing.	1. Copy to be retained for a maximum of two years. 2. Information shall not be shared with any third party without express permission of the data subject.
Any other personal data which comes under the control of the PC which does not fit into any of the categories above	Names, addresses and possible other personal data.		To be confirmed as and when required	low	1. Clerk to process the data in accordance with the data protection principles, always ensuring that personal data is stored securely and not shared with any third party without the express permission of the data subject. 2. Clerk to bring report to the next meeting of the PC, to determine the way in which the data should be controlled.

Processing Systems

The data set out in the above register is processed using the following systems:

System	Risk	Notes and actions
Email - Hotmail	Possible sharing of emails by error. Non-secure email system	None – the email system is suitable given the risks, controls and actions identified in the data audit Training for staff and councillors included email security awareness.
Microsoft One Drive cloud-based storage	Potential unauthorised access to documents containing personal data.	Documents are encrypted during transfer to and from the Cloud based storage. This is sufficiently secure

		given the risks identified in the data audit.
Website	• Insecure hosting of the website • Lawful basis for using photographs of community events which could include personal data. • Consent needed for the email alert facility	Website uses Microsoft Azure and is hosted in Dublin. Hugo Fox has an improved privacy notice and improved form of documented consent.
Manual filing systems		Clerk to ensure manual filing systems are kept securely, and documents are retained no longer than necessary for lawful processing.

ii. Privacy Notices

(1) Privacy notices shall be provided to all data subjects, on behalf of the Parish Council. The privacy notice is available on the website, and anybody contacting the Parish Council will be directed to the privacy notice for their information.

iii. Registration with the ICO

The Data Protection Act 1998 requires organisations which are processing personal information to register with the ICO, unless they are exempt. The registration expires 25 February 2020 and the registration number is ZA306991.

Astley Parish Council Data Protection Policy

1. Principles of data protection

Astley Parish Council must adhere to the following principles in all its activities related to the control or processing of personal data:

(b) Must be processed lawfully, fairly and transparently.

(c) Is only used for a ***specific processing purpose*** that the data subject has been made aware of and no other, without further consent.

(d) Should be ***adequate, relevant and limited*** i.e. only the minimum amount of data should be kept for specific processing.

(e) Must be ***accurate*** and where necessary ***kept up to date***.

(f) Should ***not be stored for longer than is necessary***, and that storage is safe and secure.

(g) Should be processed in a manner that ensures ***appropriate security and protection*****.**

2. Governance Arrangements

There shall be an annual report submitted to the Parish Council for discussion and approval. The report shall include:

- Annual report from the Clerk giving details and results of the annual audit
- Data Protection Policy
- Data audit and risk analysis
- Report on subject access requests
- Report on data breaches
- Discussion of training requirements

3. Role of the Clerk

The Clerk will

- Ensure that data is held securely, password controlled on a need to know basis and back-up systems are in place
- Maintain a processing log of data
- Ensure that data is held no longer than is necessary and follows guidelines for its deletion
- Ensure that Consent Forms are obtained where necessary, recorded and reviewed as necessary
- Undertake data protection impact assessments where required for new projects as directed by the Council as Data Controller.
- Ensure the notification of personal data breaches in accordance with the agreed procedure.
- Report to Council on progress in compliance with GDPR to include any required monitoring identified

4. Subject Access Request

The Council will ensure that personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered.

The subject access request (SAR) form is available from the Clerk. The form must be completed in full, including submission of two forms of identification. The form must be submitted to the Clerk, who will manage and respond to the request.

1. Upon receipt of a SAR

(a) The data subject will be informed who at the Council to contact, the Data Controller.

(b) The identity of the data subject will be verified and if needed, any further evidence on the identity of the data subject may be requested.

(c) The access request will be verified (is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not additional information will be requested).

(d) If a request is unfounded or excessive (in particular because of its repetitive character); the Clerk may refuse to act on the request or charge a reasonable fee.

(e) Receipt of the SAR will be promptly acknowledged and the data subject will be informed of any costs involved in the processing of the SAR.

(f) If the Council does not process any data, the data subject will be informed accordingly.

(g) Data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned may be permitted.

(h) The data requested will be checked to establish if it involves data on other data subjects. This data will be filtered before the requested data is supplied to the data subject; if data cannot be filtered, other data subjects will be contacted to give consent to the supply of their data as part of the SAR.

2. Responding to a SAR

(a) The Council will respond to a SAR within one month after receipt of the request:

(i) If more time is needed to respond to complex requests, an extension of another two months is permissible, and this will be communicated to the data subject in a timely manner within the first month;

(ii) if the council cannot provide the information requested, it will inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

(c) If data on the data subject is processed, the Council will ensure as a minimum the following information in the SAR response:

(i) the purposes of the processing;

(ii) the categories of personal data concerned;

(iii) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses

(iv) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

(v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(vi) the right to lodge a complaint with the Information Commissioners Office ("ICO");

(vii) if the data has not been collected from the data subject: the source of such data;

(viii) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(d) Provide a copy of the personal data undergoing processing.

Implementing the Subject Access Requests Policy – Council Checklist on what MUST be done

All subject access requests must be submitted to the Clerk, using the form provided on the website.

1. A member of staff, and as appropriate, councillor, who receives a request to locate and supply personal data relating to a SAR must make a full exhaustive search of the records to which they have access.

2. All the personal data that has been requested shall be provided unless an exemption applies. (This will involve a search of emails/recoverable emails, word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems.)

3. A response shall be provided within one calendar month after accepting the request as valid.

4. Subject Access Requests will be undertaken free of charge to the requestor.

6.Any exempt personal data will be redacted from the released documents with explanation why that personal data is being withheld.

7. The Council must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the council relating to the data subject. What personal data is needed will be clarified with the requestor, who must supply their address and valid evidence to prove their identity. The council accepts the following forms of identification (* These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months):

• Current UK/EEA Passport

• UK Photocard Driving Licence (Full or Provisional)

• Firearms Licence / Shotgun Certificate

• EEA National Identity Card

• Full UK Paper Driving Licence

• State Benefits Entitlement Document*

• State Pension Entitlement Document*

• HMRC Tax Credit Document*

• Local Authority Benefit Document*

• State/Local Authority Educational Grant Document*

• HMRC Tax Notification Document

• Disabled Driver's Pass

• Financial Statement issued by bank, building society or credit card company+

• Judiciary Document such as a Notice of Hearing, Summons or Court Order

• Utility bill for supply of gas, electric, water or telephone landline+

• Most recent Mortgage Statement

• Most recent council Tax Bill/Demand or Statement

• Tenancy Agreement

• Building Society Passbook which shows a transaction in the last 3 months and your address

8. Where a requestor is not satisfied with a response to a SAR, the council must manage this as a complaint. This will be assessed by the Data Protection Officer in consultation with the Chair of the Parish Council.

5. Dealing with a data breach

No data breaches have been reported in 2018/19.

A personal data breach is a breach of security leading to destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This could be either accidental or deliberate. Examples might include accidentally sending an email to the wrong recipient, passing on information/personal data without permission or loss of a computer device which contains personal data.

If the data breach risks having a significant adverse impact (this might include emotional distress, physical or material damage) on the data subject, this is a '*notifiable breach'* and must be reported to the Information Commissioner's Office within 72 hours of becoming aware of it. When a personal data breach has occurred, we will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we will report the breach to the ICO, if it's unlikely then it won't be reported but will be recorded on a data breach register, maintained by the Clerk. If a breach is not reported, the rationale for this decision should be documented on the data breach register.

Responsibility for managing the response to a data breach lies with the Clerk, or in the event that the Clerk is unavailable it will be managed by the Chair of the Parish Council.

If a councillor, contractor or staff member becomes aware of a data breach they must report immediately to the Clerk (or if the Clerk is unavailable, to the Chair of the Parish Council).

The Clerk will then take steps to assess the nature and severity of the data breach. Details will be placed on the data breach register, and the ICO will be informed within 72 hours in the case of notifiable breaches.

Reports to the ICO will include the following information:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, we will inform them of the data breach as soon as possible.