Annesley & Felley Parish Council

New compliance reporting requirements for 2025/26

For the 2025/26 Annual Governance Statement (AGAR) the Parish Council will be required to complete and sign a new section (Assertion 10) as part of the annual AGAR submission.

Therefore the Parish Council has carried out a comprehensive review of email and website domains, website accessibility and compliance with GDPR and Data Protection regulations.

Assertion 10 requires the Parish Council to:

1) **Have a .gov.uk domain for its website and all email addresses for all Parish Council employees and Councillors.**

Action taken:

- The website has been transferred to a .gov.uk domain.
- .gov.uk email addresses have been issued to all employees and Councillors and will now be used for all Parish Council communications.

2) **Operate an accessible website.**

Action taken:

- WebAIM software has been used to assess the accessibility of the website and any errors have now been corrected.
- The website contains an accessibility statement that clearly states that some PDFs may not comply with the current standard, mainly relating to old PDFs and/or documents that have been scanned rather than created from digital documents.
- The website details the process and contact information for users of the website to report any issues.

3) **Comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.**

Action taken:

- Clerk appointed Data Controller and terms of reference have been approved and agreed. (See appendix 1)
- The Parish Council has produced a questionnaire style document to perform the data audit and mapping review. (See appendix 2)
- All relevant policies and processes, Data Security Breach Policy, Subject Access request, Consent Form, Records Retention Policy, CCTV Policy, Information Technology Policy, Use Your Own Device (BYOD) Policy have **been reviewed and adopted at the Parish Council meeting held on 3rd November 2025.** (See appendix 3). **A Privacy statement has also been added to the website**.
- **Following this comprehensive review the Council concludes that little personal sensitive data is processed or stored. Controls, processes and procedures are robust and roles and responsibilities are clearly defined to ensure compliance with Assertion 10. This report was accepted and approved at the Parish Council meeting held on 3rd November 2025. However all data processing and storage controls and procedures will be subject to continual review and discussion at future Parish Council meetings.**

Appendix 1 - Data Controller Terms of Reference

1. Purpose

The purpose of this document is to set out the role, responsibilities, and authority of the Parish Council's Data Controller (DC), as required under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The DC supports the Council in fulfilling its legal obligations to protect personal data, ensure compliance, and promote good practice.

2. Appointment

The Parish Council has appointed the Clerk as Data Controller.

3. Accountability

- The DC reports directly to the Parish Council.
- The DC is independent and shall not be instructed on the performance of their tasks.
- The Council will support the DC by providing necessary resources, access to data and processing activities, and training.

4. Key Responsibilities

The DC shall:
1. Inform and advise the Council, its Councillors, employees, and volunteers of their obligations under data protection law.
2. Monitor compliance with UK GDPR, the Data Protection Act 2018, Council policies, and data protection procedures.
3. Ensure training and awareness for Councillors, employees and volunteers.
4. Oversee the maintenance of the Council's records of processing activities (ROPA).
5. Advise on and review data protection policies, procedures, and privacy notices.
6. Advise on data protection impact assessments (DPIAs) and monitor their implementation.
7. Serve as the contact point for the Information Commissioner's Office (ICO) and cooperate with the ICO as required. (The Parish Council is registered with the ICO as a Data Controller).
8. Serve as the contact point for individuals regarding their data protection rights.
9. Identify and escalate risks relating to data protection compliance to the Parish Council.

5. Authority

- Access all personal data processing activities and relevant documentation within the Council.
- Obtain cooperation from employees and Councillors in carrying out duties.
- Report directly to Full Council on issues of compliance or concern.

6. Limitations

- The DC is not personally responsible for compliance; responsibility rests with the Parish Council as Data Controller.
- The DC shall not undertake tasks that create a conflict of interest with their monitoring role.

7. Review

These Terms of Reference shall be reviewed by the Parish Council annually, or sooner if required by changes in law, guidance, or council operations.

Appendix 2 - Data Audit/Map Review

A. The Parish Council has used the following process to ensure that they comply with the record keeping obligations under GDPR.

B. The document is designed to help the Parish Council to audit its personal data and it is important that it is completed as comprehensively as possible. The purpose of a data audit is to find out what data the Parish Council processes, what it is used for, where it is located and who has access to it. It is an important step in assessing whether there are any risks in the type of data processing the Parish Council carries out.

C. **Glossary:**

"**Personal Data**" is any information about a living person which can identify them. This is not just someone's name and address but any information which can identify them (directly or indirectly). For example, a phone number or email address is personal data. Any other contact information or a person's employment history, or credit history are all personal data.

"Data controller" is the person within the organisation who determines the how and what of data processing.

"Data processor" is the person that processes the data on behalf of the controller.

"Data subject" is the person about whom personal data is processed.

"Processing" personal data means storing or deleting any personal data on a computer, database or some manual files (e.g. HR, allotment tenancy files or invoices with contractor payment details). The word 'processing' also covers selecting a name for a mailing list or reading it off a screen during a call. It includes transferring and altering data. Indeed, practically anything done to personal data constitutes processing.

"Sensitive personal data or special categories of personal data" are any of the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; and biometric data.

Lawful basis for processing and storing data:

The lawful basis for processing and storing data are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation: the processing is necessary for you to comply with the law.

Vital interests: processing is necessary to protect someone's life.

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.

Legitimate interests: processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Part A:	**Annesley & Felley Parish Council Information**
1.	**Person completing questionnaire:** a) John Barlow b) Parish Clerk c) 01623 626178 d) clerk@annesleyparishcouncil.gov.uk
2.	**Data controller:** Clerk (Annesley & Felley Parish Council)
3.	**Date questionnaire completed** October 2025
Part B:	**COMMUNICATING PERSONAL DATA**
4.	**a) What type of personal data does the Parish Council keep?** **Councillors** - name, address, telephone number, email address and photograph. **Employees** - name, address, telephone number, email address, payroll and personal information and bank details. **Suppliers** - name, email address, telephone number and bank account details. **Allotment tenants** - name, address, telephone number and email addresses. **Hirers of the Parish Hall** - name, address, telephone number and email addresses. **Residents of the Parish** - name and address (copy of electoral register securely stored). **Cemetery records** - name, address, telephone number and email address held for any person purchasing a grave plot. **Email contacts & General correspondence received** – name, email address, telephone number and postal address **CCTV images** - images obtained from internal and external CCTV cameras situated in and around the Parish Hall. **b) Where does the Parish Council get the personal data from?** **Councillors** - provided by the Parish Councillors themselves. **Employees** - provided by the employee themselves and HMRC for PAYE and NI information. **Suppliers** - provided by the supplier themselves. **Allotment tenants** - provided by the Allotment tenants themselves. **Hirers of the Parish Hall** - provided by the Hirer themselves on the booking form. **Residents of the Parish** - provided by Ashfield District Council – copy of Electoral Register (held securely) **Cemetery records** - provided by the purchaser of the grave plot and funeral director. **Email contacts & General correspondence received** - provided by the e-mail/correspondence sender. **CCTV images** – provided by the internal and external CCTV cameras situated in and around the Parish Hall. **c) Why does the Parish Council collect or process the data – what does the council do with the personal data?** **Councillors** – contact details, update of web site. Lawful basis for data collection/process - Contract **Employees** – contact details, employment law, HMRC requirements and payroll processing. Lawful basis for data collection/process – Contract/Legal Obligation **Suppliers** – contact details and payment of invoices by bank transfer. Lawful basis for data collection/process - Contract **Allotment tenants** – contact details, record of tenancy detail and record of annual tenancy payment. Lawful basis for data collection/process - Contract **Hirers of the Parish Hall** – contact details, record details of booking and record payment for hire. Lawful basis for data collection/process - Contract **Residents of the Parish** – contact details and reference. Lawful basis for data collection/process – Data Sharing Agreement – responsibility of ADC to set up as they supply the data. **Cemetery records** – contact details, update cemetery records and record receipt of payment. Lawful basis for data collection/process - Contract

	Email contacts & General correspondence received – replies to emails, contact councillors, employees, suppliers and other relevant contacts. Lawful basis for data collection/process – Legitimate interests **CCTV images** - security monitoring services and insurance cover. Lawful basis for data collection/process – Legitimate interests **d) Who does the council disclose personal data to?** **Councillors** - Posted on the Parish Council web site, detailed in the minutes of the Parish Council meetings and held by Ashfield District Council. **Employees** – Posted on the Parish Council web site, detailed in the minutes of the Parish Council meetings , tax and NI information disclosed to HMRC **Suppliers** – Parish Councillors and employees. **Allotment tenants** – Parish Councillors and employees. **Hirers of the Parish Hall** – Parish Councillors and employees. **Residents of the Parish** – Employee (only used by the Parish Clerk for reference purposes) **Cemetery records** – Employees, Parish Councillors, Grounds maintenance contractor and funeral directors. **Email contacts & General correspondence received** – employees and Councillors **CCTV images** – Employees, Councillors and Nottinghamshire Police when requested. **e) Do the Parish Council meeting minutes contain personal data?** Names of Parish Councillors, Parish Clerk, Caretakers and potentially any other attendees of the meeting. **f) Does the Parish Council ever send personal data overseas and if so where to and to which organisation? This might include overseas companies providing database or email services.** No **g) Does the council collect any sensitive personal data?** No **h) If so for what reason?** Not applicable
Part C:	**SUPPLIERS, COMPANIES, AND OTHER ORGANISATIONS THE COUNCIL CONTRACTS WITH**
5.	About individuals or representatives of organisations which supply us with services such as for council repairs, or with whom we are in contact **a) Who does the council keep personal data about?** Suppliers and Contractors **b) What type of personal data does the council keep?** Name, telephone number, email address and bank details for payment of invoices by bank transfer. **c) Where does the council get the data from?** Provided by the supplier themselves. **d) Why does the council collect or process the data?** Contact details and for payment of invoices by bank transfer.
Part D:	**GENERAL QUESTIONS ABOUT PERSONAL DATA**
6.	**a) How does the Parish Council store the personal data collected?** One Parish Council owned laptop, 2 memory sticks for backups and cloud storage, CCTV hard drive and Councillors and Employees own personal computers, tablets and mobile phones. **b) Does the council take any steps to prevent unauthorised use of or access to personal data or against accidental loss, destruction or damage? If so, what?** The laptop is only used by the Parish Clerk and is password protected; therefore unauthorised use or access risk is very low. CCTV images are only accessed by the Caretakers and nominated Parish Councillors. **c) How does the council manage access to data?** Restricted number of authorised users, password controls. **d) What is the process involved in giving access to staff or councillors?** The laptop is only accessed/used by one person - Parish Clerk. CCTV images are held on the CCTV system with restricted access.
7.	**a) Do any procedures exist for e.g. correcting, deleting, restricting, personal data? If so, please**

	provide details. Data is only corrected, deleted by the Parish Clerk. Any changes are usually only made due to changes supplied by the data subject.
8.	**a) Who has access to / is provided with the personal data (internally and externally)?** Parish Clerk and Parish Councillors. **b) Is there an authorisation procedure for accessing personal data? If so, please provide details.** No due to the very restricted access to data.
9.	**Does the council provide a copy of all existing privacy notices?** Yes – Privacy notices have been adopted.
10.	**As far as the council is aware, has any personal data which was gathered for one purpose been used for another purpose (e.g. communicating council news?) If so, please provide details.** No
11.	**Does the council have any policies, processes or procedures to check the accuracy of personal data?** No - the data held is very limited and is mainly retained for contractual and legal obligations.
12.	**a) In the event of a data security breach occurring, does the council have in place processes or procedures to be followed?** Yes - Data Security Breach policy has been adopted. **b) What are these?** See Data Security Breach policy.
13.	**a) If someone asks for a copy of personal data that the council holds about them, i.e. they make a 'subject access request,' is there a procedure for handling such a request?** Yes – Subject Access Request Procedure has been adopted. **b) Is this procedure contained in a written document?** Yes – See Subject Access Request Procedure
14.	**Does the council have an internal record of the consents which the council has relied upon for processing activities?** Consent Form has been adopted.
15.	**a) Are cookies used on our Parish Council website?** The website uses Cookies for Google Analytics (this is fairly common and allows us to collect anonymous statistical information about the use of the site.). If no-one is using this information, we could stop setting these cookies by disabling Google Analytics on the site. In addition, there is one further cookie, "DYNSRV" which is set by the hosting company to improve the performance of the site. DYNSRV This cookie is added by our load balancer to track which web server to send the visitor to. Its purpose is to improve the performance of the website. **b) Does the council provide information about the cookies used and why they are used?** No. **c) Does the council keep a record of the consents provided by users to the cookies?** No, the site does not request consent for the use of these cookies. In general, sites do not record specific users' consent. They either make people aware that the site uses cookies (and so by using the site they consent), or they ask before setting any cookies. To the user, these too approaches look fairly similar. Users can use the site without cookies if they can make the appropriate settings in their browser. **d) Does the council allow individuals to refuse to give consent?** No, apart from it is possible for users who do not want to accept our cookies from making settings in their browser to this effect
16.	**Does the council have website privacy notices and privacy policies?** No.
17.	**a) What data protection training do staff and councillors receive?** Internal ongoing training only. **b) What does the training involve?** In house training carried out by the Clerk and Parish Councillors.

18.	**a) Does anyone in the council have responsibility for reviewing personal data for relevance, accuracy and keeping it up to date?** Yes - Parish Clerk **b) If so, how regularly are these activities carried out?** Ongoing process
19.	**a) What does the council do about archiving, retention or deletion of personal data?** See Records Retention Policy adopted. **b) How long is personal data kept before being destroyed or archived?** See Records Retention Policy **c) Who authorises destruction and archiving?** Parish Clerk in line with the Records Retention Policy
Part E	**MONITORING**
20.	a) Please identify any monitoring of the following systems that takes place. 'Monitoring' includes all monitoring of systems including intercepting, blocking, recording or otherwise accessing systems whether on a full-time or occasional basis. The systems are: (i) computer networks and connections The Parish Council only has two computer connections – Clerks home and the Parish Hall. The Clerks connection is not Public as it is within the Clerks residence. The Parish Hall connection should be monitored and the hub password changed on a regular basis. (ii) CCTV and access control systems The CCTV system should be monitored with the access password changed on a regular basis. List of authorised users must be maintained. See CCTV policy. (iii) communications systems (e.g. intercom, public address systems, radios, walkie-talkies) Not applicable (iv) remote access systems (security systems) The current access entry system does not record data/information relevant to an individual. (v) email and instant messaging systems. All employees and Councillors have .gov.uk email addresses that can be monitored and cancelled/removed by the domain hosting company. (vi) telephones, voicemail, mobile phone records Not applicable b) Does the council have notices, policies or procedures relevant to this monitoring? CCTV warning notices are sited throughout and around the Parish Hall building and a CCTV policy has been adopted. Access to the Parish Hall computer connection is monitored by the Caretakers and is also password controlled.

Appendix 3 – Policies and Forms (adopted by the Parish Council)

1. Data Security Breach Policy

GDPR defines a personal data breach as "a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Annesley & Felley Parish Council takes the security of personal data seriously; computers are password protected and hard copy files are kept in locked cabinets.

Consequences of a personal data breach

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

Annesley & Felley Parish Council's duty to report a breach

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and the Information Commissioner's Office (ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, Annesley & Felley Parish Council must report the breach to the ICO in the 72-hour timeframe.

If the ICO is not informed within 72 hours, Annesley & Felley Parish Council must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Annesley & Felley Parish Council must:

i. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
ii. Communicate the contact details of the person responsible for data protection for Annesley & Felley Parish Council
iii. Describe the likely consequences of the breach
iv. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse affects.

When notifying the individual affected by the breach, Annesley & Felley Parish Council must provide the individual with (ii)-(iv) above.

Annesley & Felley Parish Council would not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (i.e. Encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

Data processors duty to inform Annesley & Felley Parish Council

If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify Annesley & Felley Parish Council without undue delay. It is then Annesley & Felley Parish Council's responsibility to inform the ICO, it is not the data processors responsibility to notify the ICO.

Records of data breaches

All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data.

Record of Data Breaches

Date of breach	Type of breach	Number of individuals affected	Date reported to ICO/individual	Actions to prevent breach recurring

To report a data breach use the ICO online system:

https://ico.org.uk/for-organisations/report-a-breach/

2. Subject Access Request Form

This procedure is to be followed when an individual contacts Annesley & Felley Parish Council to request access to their personal information held by the Council. Requests must be completed within 1 month, so it should be actioned as soon as it is received. SAR's should be provided free of charge, however, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The steps below should be followed to action the request:

1. Is it a valid subject access request?
    a) The request must be in writing (letter, email, social media or fax).
    b) Has the person requesting the information provided you with sufficient information to allow you to search for the information? (You are allowed to request for more information from the person if the request is too broad.)

2. Verify the identity of the requestor.
    a) You must be confident that the person requesting the information is indeed the person the information relates to. You should ask for the person to attend the office with their passport/photo driving licence and confirmation of their address (utility bill/bank statement).

3. Determine where the personal information will be found
    a) Consider the type of information requested and use the data processing map to determine where the records are stored. (Personal data is data which relates to a living individual who can be identified from the data (name, address, email address, database information) and can include expressions of opinion about the individual.)
    b) If you do not hold any personal data, inform the requestor. If you do hold personal data, continue to the next step.

4. Screen the information
    a) Some of the information you have retrieved may not be disclosable due to exemptions, however legal advice should be sought before applying exemptions.
    Examples of exemptions are:
        - References you have given
        - Publicly available information
        - Crime and taxation
        - Management information (restructuring/redundancies)
        - Negotiations with the requestor
        - Regulatory activities (planning enforcement, noise nuisance)
        - Legal advice and proceedings
        - Personal data of third parties

5. Are you able to disclose all the information?

a) In some cases, emails and documents may contain the personal information of other individuals who have not given their consent to share their personal information with others. If this is the case, the other individual's personal data must be redacted before the SAR is sent out.

6. Prepare the SAR response (using the sample letters at the end of this document) and make sure to include as a minimum the following information:

    a) the purposes of the processing;

    b) the categories of personal data concerned;

    c) 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;

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

    e) 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;

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

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

    h) 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.

    Be sure to also provide a copy of the personal data undergoing processing.

All SAR's should be logged to include the date of receipt, identity of the data subject, summary of the request, indication of if the Council can comply, date information is sent to the data subject.

Sample letters:

Replying to a subject access request providing the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. We are pleased to enclose the personal data you requested.

Include 6(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwisemade available in whole or in part without the prior written consent of the copyrightholder.

Yours sincerely"

Release of part of the personal data when the remainder is covered by an exemption

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. To answer your request we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose *[some/most]* of the personal data you requested. *[If any personal data has been removed]* We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that *[if there are gaps in the document]* parts of the document(s) have been blacked out. *[OR if there are fewer documents enclose]* I have not enclosed all of the personal data you requested. This is because *[explain why it is exempt]*.

Include 6(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwisemade available in whole or in part without the prior written consent of the copyrightholder.

Yours sincerely"

Replying to a subject access request explaining why you cannot provide any of the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject*].

I regret that we cannot provide the personal data you requested. This is because *[explanation where appropriate]*.

[Examples include where one of the exemptions under the data protection legislation applies. For example, the personal data might include personal data is 'legally privileged' because it is contained within legal advice provided to the council or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Your data protection officer will be able to advise if a relevant exemption applies and if the council is going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter the council should set out the reason why some of the data has been excluded.]

Yours sincerely"

3. Consent Form

"Your privacy is important to us and we would like to communicate with you about the Parish Council and its activities. To do so we need your consent. Please fill in your name and address and other contact information below and confirm your consent by ticking the boxes below."

If you are aged 13 or under your parent or guardian should fill in their details below to confirm their consent

Name …… ……

Address …… ……

…… ……

…… ……

Signature …… ……

Date …… ……

Please confirm your consent below. You can grant consent to any or all of the purposes listed. You can find out more about how we use your data from our "Privacy Notice" which is available from our website or from the Council Office or at www.annesleyfelley-pc.org.uk

You can withdraw or change your consent at any time by contacting the council office.

☐ We may contact you to keep you informed about what is going on in the council's area or other local authority areas including news, events, meetings, clubs, groups and activities. These communications may also sometimes appear on our website, or in printed or electronic form (including social media).

☐ We may contact you about groups and activities you may be interested in participating in.

☐ We may use your name and photo in our newsletters, bulletins or on our website, or our social media accounts (for example our Facebook page or Twitter account).

Keeping in touch:

☐ Yes please, I would like to receive communications by email

☐ Yes please, I would like to receive communications by telephone

☐ Yes please, I would like to receive communications by mobile phone including text message

☐ Yes please, I would like to receive communications by social media (for example Facebook, Twitter, Instagram, WhatsApp)

☐ Yes please, I would like to receive communications by post

4. Records Retention Policy

Annesley & Felley Parish Council recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the association. This document provides the policy framework through which this effective management can be achieved and audited.

It covers:

- Scope
- Responsibilities
- Retention Schedule

Scope

This policy applies to all records created, received or maintained by Annesley & Felley Parish Council in the course of carrying out its functions. Records are defined as all those documents which facilitate the business carried out by Annesley & Felley Parish Council and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically. A small percentage of Annesley & Felley Parish Council records may be selected for permanent preservation as part of the Councils archives and for historical research.

Responsibilities

Annesley & Felley Parish Council has a corporate responsibility to maintain its records and record management systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Clerk. The person responsible for records management will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely. Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with Annesley & Felley Parish Council's records management guidelines.

Retention Schedule

The retention schedule refers to record series regardless of the media in which they are stored.

Document	Minimum Retention Period	Reason
Minutes		
Minutes of Council meetings	Indefinite	Archive
Minutes of Committee meetings	Indefinite	Archive
Agendas for Council & Committee meetings	One year	Archive
Employment		
Employment records	6 years after ceasing employment	Management
Payroll information	6 years	Management

Staff references	6 years after ceasing employment	Management
Application forms (interviewed – unsuccessful)	6 months	Management
Application forms (interviewed – successful)	6 years after ceasing employment	Management
Disciplinary files	6 years after ceasing employment	Management
Staff appraisals	6 years after ceasing employment	Management
Finance		
Scales of fees and charges	3 years	Management
Cash Book	6 years	Audit/VAT
Bank statements	Last completed audit year	Audit
Cheque book stubs	Last completed audit year	Audit
Paying In Book stubs	Last completed audit year	Audit
Paid invoices	6 years	Audit/VAT
Paid cheques	6 years	Limitation Act 1980
Payroll records (PAYE & NI)	12 years	HMRC
Petty cash accounts	6 years	HMRC
Budget	6 years	Management
Audited Annual Financial Return	6 years	Audit/Management
Insurance		
Insurance policies	6 years after policy end	Management
Certificates for Insurance against liability for employees	40 years after policy end	Employer's Liability Regulation 1998
Certificates for Public Liability	6 years after policy end	Management
Insurance claim records	6 years after policy end	Management
Health and Safety		
Accident books	3 years from date of last entry	Statutory
Risk assessment	3 years	Management
Cemetery		
Register of Burials	Indefinite	Statutory/Management

Register of Graves	Indefinite	Statutory/Management
Exclusive Right of Burial Deeds	100 years	Statutory/Management
Plan of Grave Spaces	Indefinite	Statutory/Management
Burial Applications	Indefinite	Statutory/Management
Memorial erection applications	Indefinite	Statutory/Management
General Management		
Councillors contact details	Duration of membership	Management
Councillors Declarations of Interests and Acceptance of Office	Duration of membership	Management
Property & Asset Title Deeds, Lease Agreements & Asset Registers	Indefinite	Audit/Management
Contracts	Indefinite	Audit/Management
Grant Applications	6 years	Audit/Management
Precept Request	Current financial year	Audit/Management
Quotations & Tenders	6 years	Audit/Management
Routine correspondence	3 years or end of useful life	Management
Important correspondence	6 years	Management
Email messages	At end of useful life	Management
Allotment Agreements	Indefinite	Archive/Management
Register of Hall Bookings	3 years	Management
Parish Council Newsletters	Indefinite	Archive
Planning Applications	2 years	Management
Planning Applications – controversial developments	4 years	Management
Consent forms	5 years	Management
GDPR Security Compliance form	Duration of membership	Management

5. CCTV Policy

1.0 Introduction

1.1 The purpose of this policy is to provide Annesley & Felley Parish Council (the "Parish Council") with guidance in order to comply with relevant legislation relating to the use of Closed-Circuit Television ("CCTV") at the Annesley Parish Hall.

1.2 The definition of CCTV in this policy is "equipment used to capture and store images, potentially including those of persons".

1.3 The purpose of the CCTV installed 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.

The scheme will be used for the following purposes:

- to monitor the security of premises or equipment;
- to ensure public safety;
- to reduce the vandalism of property and to prevent, deter and detect crime and disorder;
- to assist the Police in the identification, detection, apprehension and prosecution of offenders by examining and using retrievable evidence relating to crime or public order.
- to deter potential offenders by publicly displaying the existence of CCTV, having cameras clearly sited that are not hidden and prominent signs on display
- to assist all emergency services to carry out their duties.

1.4 CCTV will only be installed at premises owned or administered by Annesley & Felley Parish Council. Each installation will need to be justified, normally as a result of incidents where CCTV can be judged to be appropriate in order to deter or prevent future incidents.

1.5 The Parish Council will have due regard to the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. As a relevant authority the Parish Council will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.

1.6 The Parish Council accepts the principles of that data must be:

- fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with these purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary;
- processed in accordance with individuals' rights; and
- held securely;

1.7 Responsibility for the management of the CCTV will lie with the Council.

2.0 Legislative Requirements

2.1 The Parish Council has the power to incur expenditure in respect of CCTV under powers granted by the Local Government and Rating Act 1997, section 31.

2.2 The Parish Council shall comply with all legislation, and resultant codes, apply to gathering and use of data.

2.3 The Parish Council recognises that images captured by CCTV may have to be released following a request made under the DPA Act 2018 ("FOI subject access request") .

3.0 **Roles and responsibilities**

3.1 Day-to-day maintenance and operational responsibility rests with the Parish Council.

3.2 The CCTV installation company may carry out checks of the CCTV and can access the system to carry out essential maintenance repairs when requested by the Parish Council.

3.3 The CCTV system may be viewed by a secure Mobile Phone Application (App) this is to prevent unauthorised persons having access to view any recordings.

3.4 Any breach of this policy shall be investigated by the Clerk to the Council and reported to the Parish Council.

3.5 A CCTV system prevents crime largely by increasing the risk of detection and prosecution of an offender. Any relevant tape or digital evidence must be in an acceptable format for use at Court hearings.

3.6 Only those appointed by the Council may access the cameras, recordings and associated systems, the following points must be understood and strictly observed by those persons:

- they must act with due probity and not abuse the equipment or change the pre-set criteria to compromise the privacy of an individual;
- no public access will be allowed to recordings or the App except with the express approval of the Clerk.
- the Police will be permitted access to recording media if they have reason to believe that such access is necessary to investigate, detect or prevent crime. Any visit by the Police to view images will be logged by them;
- the accuracy of the date/time displayed will be checked on each occasion that the system is accessed;
- digital records and images shall be securely stored to comply with data protection Records and images will normally be erased after a certain period but may be retained for longer because of a known incident and required for the apprehension or prosecution of offenders.
- digital records or images shall not be supplied to the media, except on the advice of the Police. Such a decision will be taken by the Parish Council.
- as records may be required as evidence in a court of law, each person handling a digital record may be required to make a statement to a Police Officer and sign an exhibit label. Any extracted data that is handed to a Police Officer should be signed for by the Police Officer and information logged to identify the recording and showing the Officer's name and police station. The log should also show when such information is returned and/or the outcome of its use;
- any event that requires checking of recorded data should be clearly detailed in the logbook of incidents, including crime numbers if appropriate;
- any damage to equipment or malfunction discovered should be reported immediately to the person responsible for maintenance, and the call logged showing the outcome. When a repair has been made this should also be logged showing the date and time of completion;
- any request by an individual member of the public for access to their own recorded image is subject to a standard fee. The sharing of the CCTV by the Parish Council complicates access rights under the Freedom of Information Act. If such a request is made the council should take advice from the ICO.

4.0 **Accountability**

4.1 Copies of this policy are available in accordance with the Freedom of Information Act, as will be any reports that are submitted to the Parish Council, providing that does not breach security needs.

4.2 Any written concerns or complaints regarding the Parish Council's use of the system will be considered under the Parish Council's existing complaints policy.

4.3 The CCTV system installed and used by the Parish Council does not require to be registered with the Information Commissioner due to its static nature.

4.4 The Parish Council is registered with the Information Commissioner as a data handler.

4.5 One or more signs shall be displayed in the vicinity of where the CCTV is deployed. One or more laminated notice shall be erected providing the following information:

- why CCTV is being used;
- who manages the CCTV;
- contact details for the organisation(s) responsible should anyone want to find out more about the scheme or request access to their CCTV images.

4.6 This policy, together with the continued need for CCTV usage, will be reviewed by the Parish Council.

6. Information Technology Policy

Introduction

The purpose of this policy is to ensure that all employees, councillors and any third parties using Annesley & Felley Parish Council information technology (IT) have a clear understanding of what is and is not permitted. This will ensure the appropriate use of the Council's equipment, safeguard the security of its IT systems and data, and assist compliance with any relevant legislation.

Definitions

Users – councillors, employees and third parties acting on behalf of the Council.
Data – digitally stored information including (but not limited to) documents, copyrighted / copyrightable text, images, personal information, accounting information.
IT hardware/software – includes, but is not limited to computers, internet access, remote access connections, email servers, file storage, webmail, smart phones, telephones, website, mobile phones etc.

Scope

This policy covers the use of IT, both hardware and software, for all councillors, employees and third parties acting on behalf of the Council (Users), and contractors, management and safekeeping of data.
The Council has produced a separate Social Media policy that should be referred to for all Social Media matters.

IT provision

The device, software, data access and services provided remain property of the Council and shall be recorded on the asset register. At the end of any period of holding office, employment with or work for the Council, all equipment must be returned to the Clerk, Chair or Vice-Chair in full working condition. If equipment has been lost or damaged, or not returned within 14 days of leaving office, a charge may be made for its replacement or repair.
Users must comply with all relevant policies, procedures and UK legislation with respect to the use of IT hardware.

All IT provisions should:

- demonstrate value for use of Council money;
- provide value for Council or clerk use, whilst enabling efficient working and not contributing to secondary waste;

- include consideration of cost vs time spent carrying out tasks which could be offset by the use of technology;
- maintain privacy of councillors, Council employees, subcontractors and parishioners;
- adhere to other policies as much as is possible, particularly the GDPR and data retention policies.

A review of the Council's IT requirement should be conducted at least every four years, when council elections take place and new councillors take office, or within three months of new members of staff starting with the Council.
Hardware provided should only be used for Council business and not personal use.

Privacy and data protection

Users must:

- not leave their user accounts logged in on an unattended and unlocked device;
- use suitability secure methods for storing and accessing data and services;
- not perform any unauthorised changes to the IT systems or information; changes must only be made with agreement from the Chair and Clerk or at full Council where applicable;
- not attempt to access or use data or software that they are not authorised to use or access;
- not give or transfer Council data or software to any person or organisation outside the Council without the appropriate authority and reason to do so;
- adhere to the Data Protection Policy and Document Retention Policy;
- comply with all relevant policies, procedures and UK legislation with respect to the use of IT software; if unsure about this then users should check with the Clerk or Chair.

Where users use their own hardware to access Council systems or data they are responsible for ensuring the security of systems and data as per this policy, the Data Protection Policy and the Document Retention Policy.
An email address will be provided to all councillors and Council employees and should be the only address used for official or unofficial Council correspondence.
Personal use is not permitted for any Council provided communication services, software applications (downloaded or software as a service) or data, unless such data is already in the public domain.
Any correspondence undertaken on behalf of the Council on Council provided or personal devices or services, where retained in line with the Retention Policy, should be provided upon request to the Clerk or Chair, particularly, but not limited to the case of a Freedom of Information request.

Passwords and access to systems and services

Ideally passwords should be either a minimum of 10 random letters, numbers or symbols, or four or five random words joined with non-alphanumeric characters.
Where a service offers two factor authentication then this must be used, if possible with a hardware security key or software two factor authentication (e.g. google authenticator) secured by a strong log-in or password.
Where a device is provided for a reasonable period of time to a Councillor or employee of the Council and this device offers biometric authentication, then this should be activated under a Council managed account.

Risk Management

As part of its risk management the Council maintains insurance on the equipment provided.

All equipment must be secured from theft or unauthorised use as far as is practical. When travelling with equipment, it should not be left in an unattended vehicle unless there is no other option, in which case it should be secured out of sight.
Any loss of, or damage to equipment should be reported as soon as possible to the Clerk and Chair and any criminal damage will be reported to the Police.
Any loss of personal data as the result of loss or theft of equipment shall be reported to the Clerk and Chair and Information Commissioner's Office (ICO).
An annual risk assessment should be undertaken regarding use and security of Council IT hardware, software and stored data.

Application of the Policy

Not adhering to the terms set out in this policy may result in disciplinary proceedings.

7. Use Your Own Device (BYOD) Policy

Purpose

The purpose of this policy is to permit Councillors, officers, employees, contractors or authorised third parties to use their own personal devices (smartphones, tablets, laptops, etc.) to access or process council information, while ensuring the security, confidentiality, integrity, and availability of council data and compliance with legal and regulatory obligations (e.g. GDPR, Data Protection Act).

Scope

This policy applies to:
- All Councillors, officers, employees, co-opted members, contractors or third parties who, for the purposes of council business, access email, documents, systems or data using their personal device.
- Any device used to access or process council data, including but not limited to smartphones, tablets, laptops, and desktop computers.

Definitions

- Council Data / Information - Any data or information held or processed by the Council, including personal data, financial data, correspondence, agendas, minutes, reports, etc.
- Personal Device - A device owned (or controlled) by an individual rather than the council.
- Remote Wipe - The ability to erase council data remotely from a device, e.g. in event of loss or theft.

Policy Statement

The council recognises the convenience and flexibility offered by BYOD, but also acknowledges that it introduces risks. This policy sets out the requirements and controls to manage those risks.

Acceptable Use & Conditions

Access and Use
- Council email, documents, systems, or data must only be accessed via approved secure methods.
- Use of personal email accounts for council business is discouraged.
- Devices should not automatically sync or back up council data to personal cloud accounts.
- Council data must not be shared with third-party apps or services without approval.

Security Requirements
- Devices must be protected with a strong password, PIN, or biometric lock.

- Devices must run up-to-date OS patches and security updates.
- Anti-virus/anti-malware software should be installed (where applicable).

Data Storage & Deletion
- Council data stored on a personal device should be minimised.
- Sensitive or personal data should be accessed in “read-only” mode where possible.
- In event of loss/theft/change of device, council data should be wiped.
- On ceasing to be a councillor/officer, individuals must remove all council data.

Loss, Theft, Breach Reporting
- Any loss or theft must be reported immediately to the Clerk.
- Suspected breaches must be reported and devices may need to be inspected.

Monitoring & Compliance
- The council reserves the right to audit compliance.
- Non-compliance may result in revocation of BYOD privileges.

Liabilities & Costs
- The council is not responsible for damage, loss, or repair costs.
- Costs (e.g. mobile data) remain the responsibility of the device owner.

Roles & Responsibilities

- Clerk - Verify compliance, lead investigations.
- Provider - Provide secure access methods, assist with audits, remote wipe.
- Councillors / Officers / Employees/ Users - Comply with policy, secure devices, report breaches.
- Council (as Data Controller) - Ensure compliance with GDPR / DPA and best practice.

Legal & Regulatory Considerations

- The council remains accountable for all personal data processing, even via personal devices.
- Information held on personal devices may be subject to FOI requests.
- Council must ensure appropriate organisational and technical measures are in place.
- Personal devices used for council business may be subject to legal inspection or discovery.

Policy Review

This policy shall be reviewed at least every two years (or sooner if required by changes in legislation, cybersecurity best practice, or council operations).