Andover Town Council

Data Protection Policy and Procedure

Introduction

This policy and procedure provides a framework for ensuring that Andover Town Council ('the Council') meets its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications Regulations 2003 (PECR).

Policy

Purpose

The Council complies with data protection legislation guided by the six data protection principles. These principles require that personal data is:

- processed fairly, lawfully and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.

In addition, the accountability principle requires the Council to be able to evidence compliance with the above six principles and make sure that individuals are not put at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage to the Council, or financial implications due to fines. To meet our obligations, the Council has put in place appropriate and effective measures to make sure it complies with data protection legislation.

The Council's is committed to transparent, lawful, and fair proportionate processing of personal data.

What does this policy include?

The scope of this policy includes information covered by data protection legislation as follows:

- The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.
- Pseudonymised personal data is included, however anonymised data is not regulated by the UK GDPR or DPA 2018, providing the anonymisation has not been done in a reversible way.
- Some personal data is more sensitive and is afforded more protection, this is information related to:
    - race or ethnic origin;
    - political opinions;
    - religious or philosophical beliefs;
    - trade union membership;
    - genetic data;
    - biometric ID data;
    - health data;
    - sexual life and/or sexual orientation; and
    - criminal data (convictions and offences)

How does the Council comply with data protection legislation?

The Council:

- appoints a Data protection Officer (DPO) who is primarily responsible for advising on and assessing the Council's compliance with the UK GDPR and DPA 2018, making recommendations to improve compliance, privacy by design and handling subject access requests. The Council's DPO is M Young who can be contacted at Micha.young@andover-tc.gov.uk.
- publishes a privacy notice on the website and provides timely notices where this is required.
- publishes a cookie notice on the website
- requires all staff to undertake mandatory training on information governance and security which they re-take every year.
- considers personal data breach incidents and sets out the reporting mechanism included below.

- assesses processing of personal data perceived to be high risk, and that needs a Data Protection Impact Assessment (DPIA) to be carried out.
- records our processing activities (ROPAs) and publishes our safeguards policy on law enforcement processing and processing of special category data.
- ensures our contracts and / or service level agreements are compliant with UK GDPR.

What personal information does the Council hold?

The Council holds personal information necessary for the performance of tasks carries out in the public interest or in the exercise of official authority vested in the Council. This includes allotments services, customer services and providing support to Councillors. Details of the data held are set out in the ROPA.

Procedure

Data Protection by Design and Default

When commencing new services, the Council assesses processing of personal data perceived to be high risk to determine if a data protection impact assessment (DPIA) should be carried out. The Council assists staff in ensuring compliance and privacy by design is integral part to any product, project or service we offer.

Data subject access and other information requests

Residents and taxpayers can ask us for personal information we might hold about you. The Council will usually only hold information about you if you've dealt with us before. We typically keep this information for a maximum of two years.

When you contact the Council for information please try to be as clear as possible. This will help us understand and respond promptly to your request. Please specify what you want and supply relevant case numbers, if you have them. We might ask you for clarification if we are not sure what you are looking for. If we hold any information, the Council will provide it unless we think it should be withheld for reasons covered by the exemptions in the legislation.

You can contact the Council:

In person: Office 107, IncuHive, Chantry House, 36 Chantry Street, Andover, SP10 1LS

By email: office@andover-tc.gov.uk

Data breaches

The Council assesses whether we need to report data breaches to the Information Commissioner's Office in line with its guidance as the Regulator of data protection legislation. The Council takes appropriate action to make you as data subjects aware of any breach.

Recording Processing Activities

The Council records and regularly reviews its personal data processing activities. Electronic ROPA are shown at xxxxx (to be added if approved)

Data retention and disposal

The Council maintains and reviews a schedule outlining storage period for all personal data.

Data disposal

The Council has methods of disposal to prevent disclosure of personal data prior to, during or after disposal.

- electronic
- paper

Data access

The Council limits access to personal data to authorised staff only and regularly review users' access rights.

Monitoring

The Council will monitor compliance with this policy via the Data Protection Officer and the Policy and Resources Committee

Review

The Council will regularly review this policy and procedure, at least annually and will also consider any impact of the Data Use and Access Act 2025 as specific provisions are phased in.

Annex A – Privacy notice and cookie statement for customers (NOTE: to be added to the website)

Andover Town Council Privacy and Cookie Policy

UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications Regulations 2003 (PECR).

Andover Town Council ("we", "us", "our", "the Council") is the data controller for the purposes of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1. Who we are and how to contact us

Controller: Andover Town Council

Address: Office 107, IncuHive, Chantry House, 36 Chantry Street, Andover, SP10 1LS

Email: office@andover-tc.gov.uk

Telephone: 01264 335592

Data Protection Officer / lead officer: M Young

2. Scope of this notice

This notice explains how we collect and use personal data when you interact with the Council, including through our website, by email, phone, post, in person, and when you use our online forms and services. It also explains our use of cookies and similar technologies on our website (see section 11).

3. The personal data we collect

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual.

Depending on your relationship with us, we may collect:

- identity and contact details (e.g., name, address, email, phone).
- communications and correspondence.
- service-related information (e.g., applications, enquiries, complaints, bookings, allotments, events).
- financial details for payments, grants or fees.
- records relating to meetings, consultations and statutory functions.
- CCTV images (if operated) and visitor information for Council premises/events.
- website and technical data (IP address, device, logs).

We collect data directly from you, from publicly available sources, from other public authorities and partners where lawful, and from our website and IT systems.

4. Our purposes and lawful bases

We process personal data only where a lawful basis applies. Typical lawful bases include:

- public task: to perform our functions as a local authority and carry out activities in the public interest or under official authority.
- legal obligation: to comply with UK law and our statutory duties for example, as an employer
- contract: to enter into or perform a contract with you (e.g., hire of facilities).
- consent: where you have given clear consent for a specific purpose (e.g., mailing lists). You can withdraw consent at any time.
- legitimate interests: for limited activities not carried out as a public task (e.g., general website administration), balanced against your rights.

If we process special category data (e.g., health) or criminal offence data, we do so only where an additional condition under data protection legislation is satisfied and where necessary for our functions or with your explicit consent.

5. How we use your information

We use personal data to:

- deliver services and fulfil statutory functions;
- manage enquiries, feedback, complaints and requests (including FOI/EIR/Subject Access);
- process applications, bookings, grants and payments;
- manage consultations and democratic processes (e.g., agendas, minutes);
- communicate service updates and information (where appropriate legal basis applies);
- ensure information security, prevent and detect crime and fraud;
- pay salaries, taxes, insurances and expenses; and
- manage our website and digital services.

6. Sharing your information

We may share data with:

- other data controllers such as public authorities and statutory bodies;
- contractors and service providers acting on our instructions (processors);
- professional advisers and auditors; and
- law enforcement and regulators where required.
- community groups
- charities
- other not for profit entities
- agents, suppliers and contractors, for example, to maintain our database software.

Where we use data processors, for example, tenancy agreements, we have written contracts requiring them to keep data secure, act only on our instructions and not use data for their own purposes. We do not sell your personal data. International transfers (if any) will only occur with appropriate safeguards (e.g., adequacy regulations or standard contractual clauses).

7. Retention – how long we keep data

We keep personal data only as long as necessary for the purposes set out in this notice and in line with our Records Retention Schedule (available on request).

Typical retention periods include routine correspondence [e.g., 2 years]; financial records [e.g., 6 years]; meeting records in accordance with statutory requirements. When no longer needed, data is securely deleted or destroyed.

8. Your rights

You have rights to:

- be informed about how we use your data;
- access your personal data;
- rectify inaccurate or incomplete data;
- erase data ('right to be forgotten') in certain circumstances;
- restrict or object to processing;
- data portability (for data you provided to us that we process by consent or contract, where technically feasible);
- object to direct marketing; and
- not to be subject to decisions based solely on automated processing that have legal or similarly significant effects.

To exercise your rights, contact us using the details in section 1.

You also have the right to complain to the Information Commissioner's Office (ICO): ico.org.uk | 0303 123 1113 | Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

9. Security

We take appropriate technical and organisational measures to protect personal data, including access controls, staff training, secure systems, encryption where appropriate, and incident management. We report notifiable personal data breaches to the ICO and affected individuals where legally required.

10. Children and vulnerable people

Where we provide services to children or vulnerable individuals, we apply additional safeguards and obtain consent where required.

11. Cookies and similar technologies (website)

We use essential cookies to make our website work. With your consent, we may also use non-essential cookies (e.g., analytics) to improve our services. Non-essential cookies will not be set unless you enable them via our cookie banner or settings.

11.1 What are cookies?

Cookies are small text files placed on your device that help our site function, remember your preferences, and analyse how the site is used. We also use similar technologies such as pixels and local storage.

11.2 Managing cookie consent

On your first visit, you will see a cookie banner. You can accept or reject non-essential cookies and change your choices at any time via ["Cookie settings" link on the site]. Essential cookies do not require consent.

11.3 Cookies we use

Below is an indicative table. Our cookies may be essential, analytical or functional. Our live cookie list may change as services evolve; the current list and purposes are kept up to date on our website.

Name	Provider	Purpose	Type	Expires
cookie_consent	Council site	Stores your cookie preferences	Essential	12 months
_ga	Google Analytics	Helps us understand site usage (only if you consent)	Analytics	13 months
_gid	Google Analytics	Distinguishes users (only if you consent)	Analytics	24 hours
sessionid	Council site	Maintains secure session for forms	Essential	Session

Embedded content (e.g., maps, videos) may set third-party cookies. Where possible we provide privacy-enhanced modes or ask for consent before loading such content.

11.4 How to control cookies

You can adjust your browser settings to refuse or delete cookies. See help pages for Chrome, Edge, Firefox, Safari and others. Rejecting cookies may affect site functionality.

11.5 Server logs and IP addresses

Our web servers automatically log requests (including IP address, date/time and pages visited) for security and operational purposes. We do not attempt to identify individuals from logs except where required by law or to investigate security incidents.

12. Changes to this notice

We may update this notice from time to time. Significant changes will be highlighted on our website.

13. Contact and complaints

For questions or requests about this notice or your data, contact us using the details in section 1. You may also complain to the Information Commissioner's Office using the details above.

14. Version control

Policy owner: GDPR Officer

Approved by: Full Council

Version: 1.0

Date approved: xxx

Next review: The Council will regularly review this policy and procedure, at least annually and will also consider any impact of the Data Use and Access Act 2025 as specific provisions are phased in.