14)

Attleborough Town Council
"Whistleblowing" Policy
(Making a Disclosure in the Public Interest)

Introduction

Attleborough Town Council is committed to the highest standards of openness, probity and accountability.

An important aspect of accountability and transparency is a mechanism to enable staff and other members of the Council to voice concerns in a responsible and effective manner. It is a fundamental term of every contract of employment that an employee will faithfully serve his or her employer and not disclose confidential information about the employer's affairs. Nevertheless, where an individual discovers information which they believe shows serious malpractice or wrongdoing within the organisation then this information should be disclosed internally without fear of reprisal, and there should be arrangements to enable this to be done independently of line management (although in relatively minor instances the line manager would be the appropriate person to be told).

The Public Interest Disclosure Act, which came into effect in 1999 and updated in May 2013, gives legal protection to employees against being dismissed or penalised by their employers as a result of publicly disclosing certain serious concerns. The Council has endorsed the provisions set out below so as to ensure that no members of staff should feel at a disadvantage in raising legitimate concerns.

It should be emphasised that this policy is intended to assist individuals who believe they have discovered malpractice or impropriety. It is not designed to question financial or business decisions taken by the Council nor should it be used to reconsider any matters which have already been addressed under harassment, complaint, disciplinary or other procedures. Once the "whistleblowing" procedures are in place, it is reasonable to expect staff to use them rather than air their complaints outside the Council.

Scope of Policy

This policy is designed to enable employees of the Council to raise concerns internally and at a high level and to disclose information which the individual believes shows malpractice or impropriety. This policy is intended to cover concerns which are in the public interest and may at least initially be investigated separately but might then lead to the invocation of other procedures e.g. disciplinary. These concerns could include

- Financial malpractice or impropriety or fraud
- Failure to comply with a legal obligation or Statutes
- Dangers to Health & Safety or the environment
- Criminal activity
- Improper conduct or unethical behaviour
- Attempts to conceal any of these

Safeguards

i. Protection

This policy is designed to offer protection to those employees of the Council who disclose such concerns provided the disclosure is made:

- in good faith
- in the reasonable belief of the individual making the disclosure that it tends to show malpractice or impropriety and if they make the disclosure to an appropriate person (see below). It is important to note that no protection from internal disciplinary procedures is offered to those who choose not to use the procedure. In an extreme case malicious or wild allegations could give rise to legal action on the part of the persons complained about.

ii. Confidentiality

The Council will treat all such disclosures in a confidential and sensitive manner. The identity of the individual making the allegation may be kept confidential so long as it does not hinder or frustrate any investigation. However, the investigation process may reveal the source of the information and the individual making the disclosure may need to provide a statement as part of the evidence required.

iii. Anonymous Allegations

This policy encourages individuals to put their name to any disclosures they make. Concerns expressed anonymously are much less credible, but they may be considered at the discretion of the Council.

In exercising this discretion, the factors to be taken into account will include:

- The seriousness of the issues raised
- The credibility of the concern
- The likelihood of confirming the allegation from attributable sources

iv. Untrue Allegations

If an individual makes an allegation in good faith, which is not confirmed by subsequent investigation, no action will be taken against that individual. In making a disclosure the individual should exercise due care to ensure the accuracy of the information. If, however, an individual makes malicious or vexatious allegations, and particularly if he or she persists with making them, disciplinary action may be taken against that individual.

Procedures for Making a Disclosure

On receipt of a complaint of malpractice, the member of staff who receives and takes note of the complaint, must pass this information as soon as is reasonably possible, to the appropriate designated investigating officer as follows:

- Complaints of malpractice will be investigated by the CEO & Town Clerk unless the complaint is against the CEO & Town Clerk or is in any way related to his/her actions. In such cases, the complaint should be passed to the Chairman/Mayor for referral.
- In the case of a complaint, which is any way connected with but not against the Chairman/Mayor, the CEO & Town Clerk will nominate a Member to act as the alternative investigating officer.
- Complaints against the CEO & Clerk should be passed to the Chairman who will nominate an appropriate investigating officer.
- The complainant has the right to bypass the line management structure and take their complaint direct to the Chairman. The Chairman has the right to refer the complaint back to management if he/she feels that the management without any conflict of interest can more appropriately investigate the complaint.

Should none of the above routes be suitable or acceptable to the complainant, then the complainant may approach one of the following individuals who have been designated and trained as independent points of contact under this procedure. They can advise the complainant on the implications of the legislation and the possible internal and external avenues of complaint open to them:

Monitoring Officer, Breckland District Council
Trade Union Representative
Citizens Advice

If there is evidence of criminal activity then the investigating officer should inform the police. The Council will ensure that any internal investigation does not hinder a formal police investigation.

Timescales

Due to the varied nature of these sorts of complaints, which may involve internal investigators and / or the police, it is not possible to lay down precise timescales for such investigations. The investigating officer should ensure that the investigations are undertaken as quickly as possible without affecting the quality and depth of those investigations.

The investigating officer, should as soon as practically possible, send a written acknowledgement of the concern to the complainant and thereafter report back to them in writing the outcome of the investigation and on the action that is proposed. If the investigation is a prolonged one, the investigating officer should keep the complainant informed, in writing, as to the progress of the investigation and as to when it is likely to be concluded.

All responses to the complainant should be in writing and sent to their home address.

Investigating Procedure

The investigating officer should follow these steps:

- Full details and clarifications of the complaint should be obtained.
- The investigating officer should inform the member of staff against whom the complaint is made as soon as is practically possible. The member of staff will be informed of their right to be accompanied by a trade union or other representative at any future interview or hearing held under the provision of these procedures.
- The investigating officer should consider the involvement of the Council auditors and the Police at this stage and should consult with the Chairman / Chief Executive
- The allegations should be fully investigated by the investigating officer with the assistance where appropriate, of other individuals / bodies.
- A judgement concerning the complaint and validity of the complaint will be made by the investigating officer. This judgement will be detailed in a written report containing the findings of the investigations and reasons for the judgement. The report will be passed to the Chief Executive or Chairman as appropriate.
- The Chief Executive / Chairman will decide what action to take. If the complaint is shown to be justified, then they will invoke the disciplinary or other appropriate Council procedures.
- The complainant should be kept informed of the progress of the investigations and, if appropriate, of the final outcome.
- If appropriate, a copy of the outcomes will be passed to the Council Auditors to enable a review of the procedures.

If the complainant is not satisfied that their concern is being properly dealt with by the investigating officer, they have the right to raise it in confidence with the Chief Executive / Chairman, or one of the designated persons described above.

If the investigation finds the allegations unsubstantiated and all internal procedures have been exhausted, but the complainant is not satisfied with the outcome of the investigation, the Council recognises the lawful rights of employees and ex-employees to make disclosures to prescribed persons (such as the Health and Safety Executive, the Audit Commission, or the utility regulators), or, where justified, elsewhere.

Adopted: 1 August 2016
Reviewed: Attleborough Town Council Meeting 13 May 2019

14)

Attleborough Town Council

FREEDOM OF INFORMATION ACT POLICY & PROCEDURE

Attleborough Town Council supports the principle of openness, transparency and accountability and will continue to improve access to information.

1 Introduction

This Freedom of Information Policy ensures that the Council acts in compliance to the Freedom of Information Act 2000 (FOIA).

The aim of this Policy is to:

- Promote a more open council;
- Promote a better informed public debate;
- Improve public confidence in operations of the council;
- Improve decision making to promote accountability;
- Improve regulation;
- Increase public participation to enhance democracy;
- Promote the FOIA, in terms of accuracy and objectivity; and
- Improve information management.

2 Legislation or Executive Summary

The FOIA provides public access to information held by the Council. It does this in two ways:

- The Council is obliged to publish certain information about their activities; and
- Members of the public are entitled to request information from the Council.

The Act covers any recorded information held by a public authority. The Act does not, however, give people access to their own personal data - these requests should be made under the Data Protection Act 1998.

The Council seeks to demonstrate its commitment to all aspects of the FOIA and will continue to promote its values and ensure that the Council is compliant with legislation.

3 Requests for Information

A request for information under the FOIA must be;

- In writing;
- State the name of the applicant and an address for correspondence; and
- Describe the information requested.

4 Fees

Wherever possible, the Council will provide information free of charge. However, in some cases this is not possible. We are entitled to charge for information under Section 9 of the FOIA and the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004, the Council will issue an appropriate fee notice which must be paid within 3 months. If no payment is received we will close the request for information.

5 Time of Compliance

The Council aims to comply with requests for information as quickly as possible. Section 10 of the FOIA states that a public authority must respond to a request promptly and, in any event, no later than the twentieth working day following the date of receipt. Working day means any day other than Saturday, Sunday, or bank holidays. The time for compliance is subject to change if:

- The Council seeks clarification under Section 1(3) of the FOIA;
- There is a need for an extension to consider the Public Interest Test under Section 10(3) of the FOIA; or
- A fees notice is issued under Section 9.

6 Appropriate Limit

Under Section 12 of the FOIA the Council does not have to comply with requests where the cost of compliance exceeds the appropriate limit. Section 12 applies if the following factors would cost the Council more than four hundred and fifty pounds or 18 hours of officer time:

- Determine whether the information is held;
- Locating the information;
- Retrieving the information; and
- Extracting the information.

Under Section 13 of the FOIA and the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 the Council is able to charge for the cost of disbursements.

7 Vexatious or Repeated Requests

Under Section 14, the Council will not comply with vexatious requests where there is a strong likelihood that such requests are being made to intentionally cause disproportionate or unjustified levels of disruption, irritation, or distress.

The Council will not comply with a request where it has received an identical or similar request from the same individual unless a reasonable interval has elapsed between compliance with the original request and the current request.

8 Advice & Assistance

In compliance with Section 16 of the FOIA, the Council will provide advice and assistance in response to all requests for information as far as reasonably practicable.

9 Refusals

In some cases, the Council may refuse requests for information under Section 17 of the FOIA. The Council may issue a refusal notice for the following reasons;

- Information is not held; or
- An exemption applies (see Part II of the FOIA).

In some cases, we may not hold the information requested - it may be that it is held by another party. If possible, the Council shall provide the requestor with information to re-direct the request. However, for Data Protection reasons the Council will not transfer the requestor's request.

10 Exemptions

There may be certain circumstances under which the Council is not obliged to release information. The Council may decide to apply exemptions under Part II of the FOIA. The exemption, if relied upon, will be explained thoroughly in the Council's refusal notice under section 17.

Some exemptions are 'absolute', which means that the exemption applies to any information falling within a defined type. Other exemptions are 'qualified' and require a public interest test to be applied. The Council will ensure that the public interest test is carried out for each of the qualified exemptions. If an exemption is applied, it will be authorised by the Proper Officer.

11 Internal Review

If a requestor is unhappy with a decision that the Council has made, or with the information provided by the Council, it may request an internal review.

The Council's internal review comprises one stage, an independent review by the Chairman of the Council, or deputy chairman if the Chairman is not available. The Council has 20 working days to complete the review and respond to the requester. Additional time may be requested if the review is particularly complex (the requester shall be notified in such cases).

The Personnel Committee will periodically review Freedom of Information requests and report any issues to the full Council. They will also ensure appropriate staff are trained to handle these requests.

12 Data Protection

A request for information may relate to personal data of the requestor or third parties. The Council may refuse the request if to disclose information in relation to third parties would be an actionable breach of confidence or would breach one or more of the data protection principles.

In cases where the request relates to personal data of the requestor, the authority will refuse under Section 40(1) and shall ask for the request to be submitted as a Data Subject Access request under the Data Protection Act 1998 Section 7. This process is detailed within the Council's Data Protection Policy.

13 Information Commissioner

The Council will consult with the Information Commissioner when required. The Council will refer to Commission guidance and ensure that it is compliant with any good practice that the Commissioner promotes. The Commissioner will investigate complaints in relation to Freedom of Information requests.

14)

Attleborough Town Council

DATA PROTECTION POLICY

Attleborough Town Council is committed to protecting the rights and freedoms of data subjects and the safe and secure processing of their data, in accordance with the Data Protection Act and the General Data Protection Regulation (GDPR).

1 Introduction

The Council holds personal data about our employees, clients, suppliers, customers, and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our employees understand the rules governing their use of the Personal Data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The Council is committed to acting responsibly in ensuring continued and effective implementation of this policy and expects all its employees to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

2 Definitions

Purpose	Description
Business	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll andbusiness development purposes. Business purposes include the following: • Compliance with our legal, regulatory and corporategovernance obligations and good practice; • Gathering information as part of investigations by regulatorybodies or in connection with legal proceedings or requests; • Ensuring business policies are adhered to (such as policies covering email and internet use); • Operational reasons, such as recording transactions, trainingand quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking; • Investigating complaints; • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments;

	• Monitoring staff conduct, disciplinary matters; • Marketing our business; and • Improving services.
Personal Data	Personal date means any information relating to an identified or identifiable natural person (data subject); and identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, CV and photo or film images.
Special Categories of Personal Data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data Controller	Data 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; where the purposes and means of such processing are determined by law.
Data Processor	Processor means a natural or legal person, public authority, agency or other agency or other body, which processes personal data on behalf of the controller.
Processing	Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Supervisory Authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office (ICO).

3 Scope

This policy applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means (i.e. paper or photographic records) that form part of filing system or are intended to form part of a filing system.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time.

Who is responsible for this policy?

The Clerk has overall responsibility for the day-to-day implementation of this policy. Please contact the Clerk for further information about this policy if it is required.

4 Principles

The Council will make every effort possible to comply with these principles. The Principles are:

- Lawful, Fair, and Transparent

  Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

- Limited for its Purpose

  Data can only be collected for a specific purpose.

- Data Minimisation

  Any data collected must be necessary and not excessive for its purpose.

- Accurate

  The data we hold must be accurate and kept up to date.

- Retention

  We cannot store data longer than necessary.

- Integrity and Confidentiality

  The data we hold must be kept safe and secure.

- Accountability and Transparency

  The Council will ensure accountability and transparency in all our use of personal data and we will record how we comply with each principle. Our employees are responsible for keeping a written record of how all the data processing activities they are responsible for comply with each of the principles. The written record will be kept up to date and will be approved by the Data Protection Officer (DPO).

  All our employees are responsible for understanding their particular responsibilities to ensure we meet the following data protection obligations:

  - Fully implement all appropriate technical and organisational measures;
  - Maintain up to date and relevant documentation on all processing activities;
  - Conducting Data Protection Impact Assessments; and
  - Implement measures to ensure privacy by design and default, including:
    - Data minimisation;
    - Pseudonymisation;
    - Transparency;
    - Allowing individuals to monitor processing and
    - Creating and improving security and enhanced privacy procedures on an ongoing basis.

5 Our Procedures

Fair and Lawful Processing

We will process personal data fairly and lawfully in accordance with individual rights under the first principle. This generally means that we will not process personal data unless the individual whose details we are processing has consented to this happening.

Lawful Basis for Processing Data

We will establish a lawful basis for processing data. It is the responsibility of each employee to check the lawful basis for any data they are working with and ensure all of their actions comply the lawful basis. At least one of the following conditions will apply whenever we process personal data:

- Consent

  We hold recent, clear, explicit, and defined consent for the individual's date to be processed for a specific purpose.

- Contract

  The processing is necessary to fulfil or prepare a contract for the individual.

- Legal Obligation

  We have a legal obligation to process the data (excluding a contract).

- Vital Interests

  Processing the data is necessary to protect a person's life or in a medical a situation.

- Public Function

  Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

- Legitimate Interest

  The processing is necessary for our legitimate interests. This condition does not apply legitimate interest. Deciding which condition to rely on if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which Condition to Rely On

In making an assessment, we will first establish that the processing is necessary. This means the processing will be a targeted, appropriate way of achieving the stated purpose.

We recognise that that more than one basis may apply, and we will rely on what will best fit the purpose.

We will consider the following factors:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?

- Are we in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are we able to stop the processing at any time on request, and have we factored in how to do this?

As part of our commitment to the first principle we shall document this process to show that we have fully considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We will also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This will occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

Any employee who is responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, must have this approved by the DPO.

6 Special Categories of Personal Data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection.

This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination.

The special categories include information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health; and/or
- sexual orientation.

In most cases where we process special categories of personal data, we will obtain the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data will comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity will cease.

7 Responsibilities

The Council's responsibilities are:

- To analyse and document the type of personal data held;
- To check procedures to ensure they cover all the rights of the individual;
- To identify the lawful basis for processing data;
- To ensure that the consent procedures are lawful;
- To implement and review the procedures to detect, report and investigate personal data breaches;
- To store data in safe and secure ways; and
- To assess the risk posed to individual rights and freedoms should data be compromised.

The responsibilities of individual members of staff are:

- To fully understand their data protection obligations;
- To check that any data processing activities they are dealing with comply with our policy and are justified;
- To not use data in any unlawful way;
- To not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through their actions;
- To ensure that the data used is accurate and consent has been given if applicable;
- To comply with this policy at all times; and
- To raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

Responsibilities of the Data Protection Officer

- To keep the Council updated about data protection responsibilities, risks and issues;
- To review all data protection procedures and policies on a regular basis;
- To arrange data protection training and advice for all staff members and members;
- To answer questions on data protection from staff, M embers and other stakeholders;
- To respond to individuals who wish to know which data is being held on them by us;
- To check with and approve third parties that handle the Council's data any contracts or agreement regarding data processing;
- To ensure all systems, services, software and equipment meet acceptable security standards;
- To check and scan security hardware and software regularly to ensure it is functioning properly;
- To research third -party services, such as cloud services the Council is considering using to store or process data;
- To approve data protection statements attached to emails and other marketing copy;
- To address data protection queries from clients, target audiences or media outlets; and
- To co-ordinate with the staff who undertake marketing activities to ensure all marketing initiatives adhere to data protection laws and the Council's Protection Policy.

Accuracy and Relevance

We will ensure that any personal data we process is accurate, adequate, relevant, and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If they believe that information is inaccurate, they should record the fact that the accuracy of the information is disputed and inform the DPO.

Data Security

We will keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing Data Securely

- In cases when data is stored on printed paper, it shall be kept in a secure place where unauthorised personnel cannot access it.
- Printed data shall be shredded when it is no longer needed.
- Data stored on a computer shall be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks will be encrypted or password protected and locked away securely when they are not being used.
- The DPO will approve any cloud used to store data.
- The DPO will approve any third-party applications that are used to store information.
- Servers containing personal data will be kept in a secure location, away from general office space.
- Data will be regularly backed up in line with the Council's backup procedures.
- All servers containing sensitive data will be approved and protected by security software.
- All possible technical measures will be put in place to keep data secure.

Data Retention

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring Data Internationally

There are restrictions on international transfers of personal data. We will not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DPO.

8 Rights of Individuals

Individuals have rights to their data which we will respect and comply with to the best of our ability. We will ensure individuals can exercise their rights in the following ways:

Right to be Informed

- Providing privacy notices which are concise, transparent, intelligible, and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

Right of Access

- Enabling individuals to access their personal data and supplementary information.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

Right to Rectification

- We will rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This will be done without delay, and no later than one month.

Right to Erasure

- We will delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

Right to Restrict Processing

- We will comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We will retain enough data to ensure the right to restriction is respected in the future.

Right to Data Portability

- We will provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We will provide it in a commonly used, machine -readable format, and send it directly to another controller if requested.

Right to Object

- We will respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We will respect the right of an individual to object to direct marketing, including profiling.
- We will respect the right of an individual to object to processing their data for scientific and historical research and statistics.

Rights in Relation to Automate Decision Making and Profiling

- We will respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

9 Privacy Notices

When to supply a privacy notice.

A privacy notice will be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice will be provided within a reasonable period of having obtained the data, which mean within one month.

If the data is being used to communicate with the individual, then the privacy notice will be supplied at the latest when the first communication takes p lace.

If disclosure to another recipient is envisaged, then the privacy notice will be supplied prior to the data being disclosed.

What to include in a privacy notice?

Privacy notices will be concise, transparent, intelligible, and easily accessible. They will be provided free of charge and will be written in clear and plain language, particularly if aimed at children.

The following information will be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the data protection officer;
- The purpose of processing the data and the lawful basis for doing so;
- The legitimate interests of the controller or third party, if applicable;
- The right to withdraw con sent at any time, if applicable;
- The category of the personal data (only for data not obtained directly from the data subject);
- Any recipient or categories of recipients of the personal data;
- Detailed information of any transfers to third countries and safeguards in place;
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period;
- The right to lodge a complaint with the ICO, and internal complaint procedures;
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject);
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject; and
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject).

10 Subject Access Requests

What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information, which means the information, which should be provided in a privacy notice.

How we deal with subject access requests.

We will provide an individual with a copy of the information the re quest, free of charge. This will occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. Extension of the deadline must be approved by the DPO.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

Once a subject access request has been made, an employee must not change or am end any of the data that has been requested. Doing so is a criminal offence.

Data portability requests.

We shall provide the data requested in a structured, commonly used, and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We will provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This shall be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and express permission must be sought from the DPO first.

11 Right to Erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed;
- Where consent is withdrawn;
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed or otherwise breached data protection laws;
- To comply with a legal obligation; and/or
- The processing relates to a child.

How we deal with the right to erasure.

We will only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For archiving purposes in the public interest, scientific research, historical research, or statistical purposes;

- For public health purposes in the public interest; and/or
- The exercise or defence of legal claims.

If personal data that needs to be erased has been passed onto other parties or recipients, we will contact them and inform them of their obligation to erase the data. If the individual asks, we will inform them of those recipients.

The right to object.

Individuals have the right to object to their data being used on grounds relating to their particular situation. We will cease processing unless:

- We have legitimate grounds for processing which override the interests, rights, and freedoms of the individual; and/or
- The processing relates to the establishment, exercise, or defence of legal claims.

We will inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We will offer a way for individuals to object online.

The right to restrict automated profiling or decision making.

We will only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry in to or performance of a contract;
- Based on the individual's explicit consent; and otherwise authorised by law.

In these circumstances, we will:

- Give individuals detailed information about the automated processing;
- Offer simple ways for them to request human intervention or challenge any decision about them; and
- Carry out regular checks and user testing to ensure our systems are working as intended.

12 Third Parties

Using third party controllers and processors.

As a data controller and data processor, we will have written contracts in place with any third-party data controllers and/or data processors that we use. The contract shall contain specific clauses which set out our and their liabilities, obligations, and responsibilities.

As a data controller, we shall only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

As a data processor, we will only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Contracts

Our contracts shall comply with the GDPR contractual clauses and where applicable, the requirements set out by the ICO. Our contracts with data controllers and/or data processors will set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts will include terms that specify:

- Acting only on written instructions;
- Those involved in processing the data are subject to a duty of confidence;
- Appropriate measures will be taken to ensure the security of the processing;
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR;
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments;
- Delete or return all personal data at the end of the contract;
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations; and
- Nothing will be done by either the controller or processor to infringe on GDPR.

13 Criminal Offence Data

Criminal record checks.

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and will be treated as such. The DPO must approve a criminal record check before it is carried out.

14 Audits, Monitoring & Training

Data Audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. We will conduct regular data audits as defined by the DPO and normal procedures and will on occasions request an audit to be carried out by the Information Commissioners Office.

These audits will provide an assessment of whether the Council is following good data protection practice and will look at whether the Council has effective controls in place alongside fit for purpose policies and procedures to support its data protection obligation. The resulting report will be presented to the full Council and will make recommendations on how to make improvments, if necessary.

Monitoring

Each member of staff and Councillor shall observe this policy and comply with it at all times. The DPO has overall responsibility for this policy. Attleborough Town Council will keep this policy under review and amend or change it as required. Any breach of this policy shall be notified to the DPO.

Training

Each member of staff will receive adequate training on provisions of data protection law specific for their role. If a member of staff moves roles or responsibilities, new GDPR training, relevant to the new role or responsibilities will be provided.

15 Reporting Breaches

Any breach of this policy or of data protection laws will be reported as soon as practically possible. As soon as it becomes aware of a breach, Attleborough Town Council has a legal obligation to report any data breaches to the Information Commissioner's Office within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures.

This allows us to:

- Investigate the failure and take remedial steps if necessary;
- Maintain a register of compliance failures; and
- Notify the Information Commissioner's Office of any compliance failures that are material either in their own right or as part of a pattern of failures.

Failure to comply.

We take compliance with this policy very seriously.

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action, which may result in dismissal.