New Alresford Town Council

Alresford Recreation Centre, The Avenue, Alresford, Hants, SO24 9EP
Tel: 01962 732079. Email: townclerk@newalresford-tc.gov.uk
Website: www.newalresford-tc.gov.uk

Data Protection Policy

Table of Contents

Version Control

Version	Owner	Date approved	Minute Ref	Website updated	Next review
V1	Town Council	15/10/2019	19/158	29/11/2019	01/11/2020

1 Introduction

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.
The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) which came into force in the UK on 25 May 2018.
Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

New Alresford Town Council processes personal data in accordance with General Data Protection Regulations (and Data Protection Act) Article 6 (1) (a) (b) and (e) to:

- fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law.
- pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law.
- monitor its activities including the equality and diversity of its activities
- fulfil its duties in operating the business premises including security
- assist regulatory and law enforcement agencies
- process information including the recording and updating details about its Councillors, employees, partners and volunteers.
- process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint.
- undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council.
- undertake research, audit and quality improvement work to fulfil its objects and purposes.
- carry out Council administration.

Where appropriate and governed by necessary safeguards we will carry out the above processing jointly with other appropriate bodies from time to time.

The Council will adopt procedures and manage responsibly, all data which it handles and will respect the confidentiality of both its own data and that belonging to partner organisations it works with and members of the public. In some cases, it will have contractual obligations towards confidential data, but in addition will have specific legal responsibilities for personal and sensitive information under data protection legislation.

The Council will be as transparent as possible about its operations and will work closely with public, community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the Town's communities. Details of information which is routinely available is contained in the Council's Publication Scheme.

2 Identifying the roles and minimising risk

GDPR requires that everyone within the council must understand the implications of GDPR and that roles and duties must be assigned. The council is the data controller. However, the council is not required to appoint a Data Protection Officer as the council is not deemed to be a public authority under Section 7 (3) of the Data Protection Act 2018 for the purposes of GDPR. A council must adhere to the issuing of privacy statements, dealing with requests and complaints raised and; the safe disposal of information.

GDPR requires continued care by everyone within the council, councillors and employees, in the sharing of information about individuals, whether as a hard copy or electronically. Any breach of the regulations could result in the council facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as high / medium risk to the council (both financially and reputationally). The risk is minimised through technical measures, training and appropriate policies, the council ensures that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure.

3 Data breaches

The Council must conduct an investigation if there is a report of a personal data breach within one month of the alleged incident. Procedures are in place to detect, report and investigate a personal data breach. The ICO will be advised of a breach within 3 days where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council will also have to notify those concerned directly.

Employees, volunteers and members must be careful not to use IT in any way that can be deemed unacceptable conduct, for example the discussion of internal council matters on social media sites could result in reputational damage for the Council and to individuals.

4 Privacy Notices

Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of the Data Protection Act 2018 and the General Data Protection Regulations. The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a council does with their personal information. A privacy notice will contain the name and contact details of the data controller, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a privacy notice must be detailed on the Information Audit kept by the council. The council will adopt a privacy

notice to use, although some changes could be needed depending on the situation, for example where children are involved. All privacy notices must be verifiable.

5 Information Audit

The council must undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the council will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the council undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

6 Individuals' Rights

GDPR gives individuals rights with some enhancements to those rights already in place:

- the right to be informed
- the right of access
- the right to rectification
- the right to edit or erase
- the right to restrict processing
- right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling.

The two enhancements of GDPR are that individuals now have a right to have their personal data erased ('right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

If a request is received to delete information, then the Council must respond to this request within a calendar month.

If a request is considered to be manifestly unfounded then the request could be refused, or a charge may apply. The charge will be as detailed in the council's Freedom of Information Publication Scheme. The Town Council will be informed of such requests.

7 Children

The age when a child can give their own consent is 13. If the council requires consent from young people under 13, the council must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in language that they will understand.

8 Summary

The main actions arising from this policy are:

- The Council must be registered with the ICO.
- A copy of this policy will be available on the Council's website.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices must be issued.

9. Data Protection Terminology

Data subject - is any person whose personal data is being collected, held or processed.

Personal data - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person.
It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, and posts on social networking sites or a computer IP address.

Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data controller - means a person who (either alone or jointly or in common with other persons) (e.g. Town Council) determines the purposes for which and the manner in which any personal data is to be processed.

Data processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organising, adapting or altering it
- retrieving, consulting or using the information or data
- disclosing the information or data by transmission, dissemination or otherwise making it available
- aligning, combining, blocking, erasing or destroying the information or data. regardless of the Technology used.