Arlesey Town Council

DATA Protection Policy

June 2023

Adopted: 20/06/23

Contents

Document Control

Organisation	Arlesey Town Council
Title	Data Protection Policy
Creator	Town Clerk
Source	LCPAS
Approvals	ATC – 20th June 2023
Distribution	All Staff and Council Members
Review date	Annual Review – June 2024

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description

1 Purpose

1.1 Information is a major asset that Arlesey Town Council has a duty and responsibility to protect.

1.2 The purpose and objective of this Information Protection Policy is to specify the means of information handling and transfer within the Council.

2 Scope

2.1 The Data Protection Policy applies to all Councillors, Committees, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Arlesey Town Council purposes.

2.2 Information takes many forms and includes:

- hard copy data printed or written on paper
- data stored electronically
- communications sent by post / courier or using electronic means
- stored tape or video
- speech

3 Information Storage

3.1 All electronic information will be stored on centralised facilities and/or managed storage providers, to allow regular backups to take place.

3.2 Information will not be held that breaches the Data Protection Act (2018) or formal notification and guidance issued by Arlesey Town Council. All personal identifiable information will be used in accordance with the Caldicott Principles.

3.3 Records management and retention policy will be followed.

3.4 Staff should not be allowed to access information until line managers are satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

3.5 Databases holding personal information will have a defined security and system management policy for the records and documentation.

3.6 This documentation defined in 3.5 will include a clear statement as to the use, or planned use of the personal information, which is cross-referenced to the Data Protection Notification.

3.7 Files which are listed by Arlesey Town Council as a potential security risk should not be stored on the network, except for in designated application storage areas. To facilitate this Arlesey Town Council will implement an electronic File security solution.

4 Disclosure of Information - Computer and Paper Based

4.1 The disclosure of personal information reported to other than Data Control Officer (Clerk) and Chairman of Council is forbidden. If there is suspicion of a Member or employee treating confidential Council information in a way that could be harmful to the Council or to the data subject, then it is be reported to the Data Control Officer (Clerk) who will take appropriate action.

4.2 Do not remove printed information from premises without the express consent of the information owner. Consent will only be given in exceptional circumstances.

4.3 Protectively marked, personal or sensitive documents are not to be left unattended and, when not in use, are to be locked away and accessed only by authorised persons.

4.4 Disposal methods for waste computer printed output and other media must be in accordance with Arlesey Town Councils disposal policy.

4.5 Distribution of information should be via the most secure method available.

5 Disclosure of Information – Telephone, Fax and E-mail

5.1 Where this involves the exchange of sensitive information then the following procedures will be applied.

6 Telephone calls:

6.1 Verify the identification of members before disclosing information. If in doubt, return their call using a known telephone number.

6.2 For external callers, verify their identity and their need to know the requested information. Telephone them back before releasing information and ask the caller to provide evidence of their identity (passport, driving license, household utility bill).

6.3 Ensure that you are authorised to disclose the information requested.

6.4 Ensure that the person is entitled to be given this information.

6.5 Ensure that the information you give is accurate and factual.

7 Fax transmissions:

7.1 Fax should not be used to transmit personal or sensitive information.

8 Disclosure of information by email:

8.1 Staff and members are to be mindful that personal or sensitive information is at risk if sent outside of the Council's network.

8.2 Staff and members are to be mindful that If an e-mail is sent to an address that is not a Council domain address the email will be delivered through the public network and the message may be left at several locations on its journey and could be deliberately intercepted. Standard disclaimer MUST be added to the bottom of every email sent.

8.3 Email should not be used for sending personal or sensitive information unless technical measures are in place to keep the message secure.

8.5 The sender should be satisfied of the identity of the recipient, if in doubt the email should not be sent and alternative methods should be used.

8.6 No identifiable personal information should be included when sending on emails, unless appropriate consent of the sender has been obtained.

9 Sharing of Personal Information

9.1 Information relating to individuals shall not be shared with other authorities without the agreement of the Data Control Officer.

9.2 Staff should be aware of their responsibilities to be able to justify the sharing of information and to be able to maintain security when transferring information in person, by email, phone or post.