Data Protection Documents

Data Protection by Design checklist -	This checklist should be completed for all new processing activities. It helps ensure that data protection is integrated from the outset of any new initiative. While it's not mandatory to retrospectively apply it to activities already listed in the ROPA, it's good practice to review high-risk or sensitive existing processes using the checklist where appropriate
Data Protection Impact Assessment - (DPIA) Procedure	A systematic process that organisations follow to identify, assess, and mitigate the privacy risks of processing personal data—especially when the processing is likely to result in a high risk to individuals' rights and freedoms. A key requirement under Article 35 of the GDPR, used *before* starting any data processing activity that could impact individuals' privacy. It ensures that risks are considered early, and privacy protections are embedded from the beginning.
Data Breach Procedure -	It ensures quick identification, containment, assessment, reporting, and resolution of the breach in a way that complies with legal obligations
Information Transfer Procedure -	A formal process that outlines how data—especially personal or sensitive information—is securely transferred from one party or location to another. This ensures data integrity, confidentiality, and legal compliance during any physical or digital transfer of information. It's especially critical when dealing with personal data
Appropriate Policy Document -	A mandatory internal document required under the UK Data Protection Act 2018 (DPA 2018) when an organisation processes special category or criminal offence data under certain legal conditions. It explains why and how the organization processes this sensitive data, and outlines the safeguards in place to protect individuals' rights. Setting out the legal basis for processing sensitive data, measures to protect the data and individuals' rights and the organisation's data retention and deletion policies It must be in place at the time the processing starts and must be retained for as long as the processing continues.
Data Protection Complaints procedure -	A formal process for individuals to raise concerns about how their personal data is handled—and for organisations to investigate and respond properly

Data Subjects Rights Request Procedure	This outlines the steps an organisation follows when responding to individuals exercising their rights under data protection laws, such as access, rectification, erasure, or objection to processing. Its purpose is to ensure timely, consistent, and lawful handling of requests, protecting individuals' privacy rights and helping the organization remain compliant with regulations like the UK GDPR.
Website Privacy Notice	This is a public statement that explains how an organisation collects, uses, stores, and shares personal data from visitors to its website. Its purpose is to provide transparency, inform users of their data protection rights, and ensure compliance with privacy laws such as the UK GDPR.
Employee Privacy Notice	This informs staff about how their personal data is collected, used, stored, and shared by their employer. Its purpose is to ensure transparency, explain employees' data protection rights, and demonstrate compliance with data protection laws such as the UK GDPR.

Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Fakenham Town Council

DATA PROTECTION BY DESIGN CHECKLIST

VERSION HISTORY

Date	Version Number	Name	Change Description
04/06/2025	0.1	Bulletproof	Initial Document Creation
11/07/2025	0.2	Fakenham Town Council	Document Reviewed
21/07/2026	0.3	Fakenham Town Council	Annual Document Review

THIS DATA PROTECTION BY DESIGN CHECKLIST (DPBD) TEMPLATE IS DESIGNED TO HELP YOU STEP THROUGH THE VARIOUS PROCEDURES NEEDED TO ENSURE ALL ASSESSMENTS AND ACTIONS HAVE BEEN COMPLETED AS REQUIRED BY ARTICLE 25 OF THE GDPR. COMPLETING THE CHECKS AND ACTIONS ON THE CHECKLIST WILL HELP TO ENSURE DATA PROTECTION IS BUILT INTO YOUR PROCESSES.

PROCESSING INFORMATION

Name of processing activity	
Purpose of processing	
Process Owner	

PART ONE: DATA PROTECTION BY DESIGN CHECKLIST

#	Requirement	Example/explanation	Response	Comments
1	Has a lawful basis for processing been identified?	Legal basis includes: Performance of a contract Legal obligation Legitimate Interest Consent Vital Interest performance of a task carried out in the public interest	(Y/N)	Please identify the chosen lawful basis in here. If no lawful basis has been identified, contact your data privacy representative
2	Has all the personal data that is required to carry out this activity/process been identified and checked to make sure no additional personal data is being collected that is not needed?	You should only collect the minimum amount of personal data needed to perform the activity.	(Y/N)	Please list the personal data being collected
3	Have retention periods been identified for this personal data and recorded in the retention policy?	Identify any legal, contractual or regulatory obligations to keep personal data and consider, if none of these apply, what is a reasonable timescale to keep this personal data?	(Y/N)	Please provide retention periods and any associated legal, regulatory or contractual requirements and ensure the document owner of the retention policy has been notified
4	Has a method of removing personal data for this activity/process been identified once the retention period is exceeded?	Identify ways that the data can be removed, preferably automatically. This may involve manual processes as well. Clear records and reminders need to be kept to ensure the data is removed	(Y/N)	Please give details of this method

5	Has a method for keeping the personal data for this activity/process up to date and accurate been identified?	This could involve giving the data subjects access to their data via a portal, conducting regular data cleansing activities, reminding data subjects to inform you of changes	(Y/N)	Please give details of this method
6	Have data flow maps been updated to accommodate the new process/activity	Data flow maps show, by department or function how personal data moves around your organisation and are helpful when dealing with data subject rights requests	(Y/N)	If yes, please provide details of the location of the data map
7	If consent is the lawful basis, have the requirements for consent been met?	If using consent, you must ensure: a) The data subject is giving consent by a clear affirmative action (e.g. ticking a box, signing a document) b) Consent is documented c) The data subject has been provided with clear and transparent information about the resulting processing of their data (via a privacy notice) d) Consent is freely given	(Y/N/N/A)	If Yes, please give details here of how these requirements are being met.
8	If legitimate interest is the lawful basis, has a legitimate interests assessment been carried out?	If you have not conducted an LIA, please use the provided LIA template	(Y/N/N/A)	If yes, please provide details of the LIA and whether it has been signed off by senior management or the DPO (where you have a DPO)
9	If processors are being used has a due diligence check been carried out on the processor?	Processors/service providers who process personal data on behalf of and at the instruction of your organisation should undergo a supplier due diligence check to verify they have suitable	(Y/N/N/A)	If yes, please provide details of the processors and results of the due diligence checks and location of documentation (including all supporting documentation such as security certification)

		security and data privacy protections in place. Use the supplier due diligence checklist and document this		
10	If processors are being used has a contract that meets the requirements of Article 28 been put in place with them	There should be a contract with data processing agreement that clearly outlines the data privacy obligations of the processor in accordance with the requirements of Article 28 of the GDPR	(Y/N/N/A)	If yes, please provide details of the processors and location of the contracts and whether these contracts have been checked by the DPO or legal team
11	If the personal data is transferred to third parties, has the lawful basis for doing so been identified?	See question 1	(Y/N/N/A)	If yes, please indicate which lawful basis has been chosen
12	Is the personal data being processed or transferred to a third country or organisation in a third country?	Third countries are those countries that outside of the UK and do not have an adequacy decision. You can see which countries have an adequacy decision here. If you are transferring personal data to one of these, there will need to be additional safeguards in place such as standard contract clauses	(Y/N/N/A)	If yes, please provide details of the countries the data is being transferred to.
13	If there is special category data being processed as part of this activity, has an article 9 exception been identified for this processing?	Special category personal data includes: Religion, political opinions, ethnic origin, race, trade union membership, philosophical beliefs, genetic data, biometric data, health data, information about the data subject's sex life or sexual orientation. Article 9 exceptions can be identified here	(Y/N/N/A)	If yes, please provide details of the exception identified.

14	Has a Data Protection Impact Assessment (DPIA) been conducted?	DPIAs are needed where the processing or activity is likely to result in a high risk to the rights and freedoms of data subjects. Refer to the DPIA checklist and DPIA template	(Y/N/N/A)	If yes, please provide details of the DPIA (location)
15	Has the relevant privacy notice been updated to include the processing of personal data identified by this activity?	Your DPO or GDPR representative will help with this	(Y/N)	
16	If the source of the personal data is not directly from the data subject, have you identified the source and ensured this has been documented in an Article 14 privacy notice and issued to the data subjects in accordance with Article 14	Your DPO or GDPR representative will help with this	(Y/N/N/A)	
17	If personal data is being stored electronically, can it be exported in a commonly used machine-readable format to comply with the right to data portability?	It should be possible to export data held in a system into a csv, excel, text or other commonly used format to be sent to another controller if the data subject exercises their right to data portability.	(Y/N/N/A)	If yes, please give details
18	If automated decisions (i.e., decisions not made by humans) are made that could have legal implications or similar serious disadvantages for data subjects during the processing, is it ensured that the processing is necessary for the performance of a contract or that consent has been obtained?	Contract and Consent are the two lawful bases that enable data subjects to exercise their right to portability	(Y/N/N/A)	Please indicate the necessity of processing and details of contract or consent if relevant.

19	If automated decisions (i.e. decisions not made by humans) are made that could have legal implications or similar serious disadvantages for data subjects during the processing, is it ensured that the data subject has the right to challenge the decision?	e.g. has the data subject been informed of the automated decision making via the privacy notice and how this will be handled internally?	(Y/N/N/A)	If yes, please give details
20	Can the personal data being used be anonymised or pseudonymised?	Anonymisation means the data can never be used to identify an individual, and if so, the data is no longer personal data and GDPR will not apply. Pseudonymisation does allow the possibility that the data can be used to identify an individual if additional information is provided so GDPR will still apply	(Y/N)	Please provide details.
21	Are there access controls in place to ensure access to the personal data is limited to those that need it?	Access control should be in place to restrict access. This should be configured to ensure people only see the data they need to do their job and no more	(Y/N)	Please provide details
22	Is personal data regularly backed up and data recovery tested?	This is to ensure data can be recovered (loss of access is a data breach) in the event of outage or attacks such as ransomware	(Y/N)	Please provide details
23	Is personal data encrypted at rest and in transit?	Personal data should ideally be encrypted to ensure that in the event of loss, it cannot be accessed. You should encrypt such data in line with your encryption policy	(Y/N)	Please provide details

24	If the new process involves the development of software in-house (or under your control by a third party) has the software been security tested?	Software should be security tested to identify vulnerabilities so they can be addressed before data is processed	(Y/N)	If yes, please provide details of testing and remediation efforts
25	Has the records of processing document been updated to reflect this new activity/process?	The DPO or person responsible for data privacy should update the record of processing with the information you provide	(Y/N)	
26	Have staff had suitable training to understand how the new activity/process works?	Staff should be trained to avoid accidental data breaches through lack of knowledge	(Y/N)	Please provide details of the training

Reviewed at Governance & Finance 21st July 2026

To be reviewed annually

Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Fakenham Town Council

DATA PROTECTION IMPACT ASSESSMENT (DPIA)PROCEDURE

VERSION HISTORY

Date	Version Number	Name	Change Description
05/06/2025	0.1	Bulletproof	Initial Document Creation
11/07/2025	0.2	Fakenham Town Council	Document Review
21/07/2026	0.3	Fakenham Town Council	Annual Document Review

1.0 INTRODUCTION

Fakenham Town Council is fully committed to protecting the personal data of its customers, employees, suppliers and other stakeholders in accordance with the EU and UK GDPR, the UK Data Protection Act 2018 and other privacy legislation. We take data privacy seriously and have initiated a variety of methods and controls to ensure we know how we handle and protect personal data.

As part of this commitment, Fakenham Town Council ensures that all activities that involve the processing of personal data where there may be a high risk to the data subject are subject to data protection impact assessments (DPIAs). The purpose of the assessment is to ensure the risks to the data subject of any processing activities is understood and suitable mitigations have been made prior to processing.

This document outlines the DPIA procedure.

2.0 SCOPE

This scope of this procedure is all processing involving personal data that is carried out by Fakenham Town Council.

3.0 RESPONSIBILITIES

Fakenham Town Council recognises that it has a corporate responsibility to ensure that all data is processed in accordance with any relevant legislation and guidance to which it is subject to.

All individuals covered by the scope of this policy are responsible for ensuring they understand when a DPIA may be needed and instigate one where required.

The Clerk is responsible for conducting the DPIA with the DPO and for instigating the procedure

Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Fakenham Town Council

The Clerk is responsible for conducting the DPIA in partnership with the owner of any new project/system/process that is being considered.

The Clerk is responsible for communication with the Supervisory Authority where required (Prior Consultation as per Article 38)

The Clerk is responsible for making recommendations on whether the processing can proceed.

The Clerk is responsible for the final decision on whether processing will proceed.

The Clerk is responsible for reviewing the DPIA and defining the time scale for review.

4.0 ESTABLISH NEED AND CONTEXT

There are a number of criteria that determine when a DPIA should be carried out. Article 35 of the GDPR states that a DPIA shall be required when the proposed processing involves:

a) Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significant affect the natural person;
b) Processing on a large scale of special categories of data referred to in Article 9(1) or of personal data relating to criminal convictions and offences referred to in Article 10; or
c) A systematic monitoring of a publicly accessible area on a large scale.

In general, Fakenham Town Council specifies that DPIAs are appropriate for projects where one or more of the following applies:

a) Where there is a high risk to the data subject
b) Use innovative technology (in combination with any of the criteria from the European guidelines);
c) Use profiling or special category data to decide on access to services;
d) Profile individuals on a large scale;
e) Process biometric data (in combination with any of the criteria from the European guidelines);
f) process genetic data (in combination with any of the criteria from the European guidelines);
g) Match data or combine datasets from different sources;
h) Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
i) Track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
j) Profile children or target marketing or online services at them; or
k) Process data that might endanger the individual's physical health or safety in the event of a security breach.

If there is uncertainty as to whether it is appropriate to carry out a DPIA, the Clerk should consult with a Date Protection (DPO) Officer for clarification and further guidance. The DPO, in turn, where necessary, may consult

Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Fakenham Town Council

the ICO or other legal representatives for further guidance. If the result of any guidance is inconclusive, the default approach will be to conduct the DPIA.

5.0 PROCEDURE

For any new project involving the processing of personal data, the project leader should

1. Identify the need for the DPIA in accordance with the criteria outlined in section 4.0 of this procedure – if in doubt, consult with the (Project Manager)
2. Create a DPIA using the DPIA template provided
3. Complete as much of the DPIA as possible
4. Refer to the Clerk for support on completing the rest of the DPIA
5. Risks will be assessed according to the likelihood and impact scales defined in the DPIA template
6. Once completed, the Clerk will review the DPIA and make recommendations on whether processing can proceed. The Clerk will also recommend a review period for the DPIA
7. Where the residual risk of processing is high, the Clerk will refer the DPIA to the ICO for prior consultation. This will involve providing the ICO with the following information:
    a. Details of the respective responsibilities of the controller, joint controller and processors (where applicable)
    b. Purpose and means of processing
    c. The controls that will be implemented to protect the data
    d. Contact details of the Clerk
    e. A copy of the DPIA
8. The final decision for processing will be made by the Clerk. Where the Clerk overrules the recommendations of the DPO, this will be documented in the DPIA
9. Processing must not start until the Clerk has approved it.
10. The Clerk will review the DPIA in accordance with the review period and at least annually. The review period will be recorded in the DPIA log.

Reviewed at Governance & Finance 21st July 2026

To be reviewed annually

Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Fakenham Town Council

DATA BREACH PROCEDURE

VERSION HISTORY

DATE	VERSION NUMBER	NAME	CHANGE DESCRIPTION
04/05/2025	V0.1	Bulletproof	Initial Document Creation
11/7/2025	0.2	Fakenham Town Council	Document Review
21/07/2026	0.3	Fakenham Town Council	Annual Document Review

1. INTRODUCTION

A data breach procedure creates a framework for all staff at Fakenham Town Council who hold and processes personal data in relation to employees, members and contractors. As a council we pride ourselves on the security and lawful handling of personal data including special category data. At Fakenham Town Council we process data in accordance with the relevant legal requirements, namely General Data Protection Regulation 2016/679; the UK Data Protection Act 2018 and all relevant EU and UK data protection legislation. As a council we ensure that care is taken to protect personal data from incidents (either committed accidentally or deliberately) and to avoid a data breach that could compromise security. Any compromise to the confidentiality, integrity, or availability of information we hold, in terms of breach of may result in harm to individual(s), reputational damage, a detrimental effect on service provision, amount to legislative noncompliance, and/or financial costs.

2. DEFINITION OF DATA BREACH

A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted, or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:

- Loss or theft of personal data and/or equipment on which data is stored
- 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
- Hacking attack
- Cyber attack
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Flawed data destruction procedures.

3. RESPONSIBILITIES

Fakenham Town Council recognises that it has responsibility to ensure that all Fakenham Town Council data is processed in accordance with any relevant legislation and guidance to which it is subject to.

All individuals covered by the scope of this policy are responsible for reporting actual, suspected, threatened or potential data breaches and for assisting with investigations as required, particularly if urgent action must be taken to prevent any or further damage.

The Clerk is responsible for drawing up guidance on access to information, including data protection and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely management of incidents.

Failure to comply with the policy may result in an administrative fine for Fakenham Town Council by the information commissioner's office (ICO) and/or disciplinary action against individuals under Fakenham Town Council procedures.

4. PERSONAL DATA BREACH NOTIFICATION: GENERAL POINTS

When a personal data breach is suspected, it is the responsibility of the employee or Councillor who identifies the breach to report this to the Clerk immediately to ensure the breach can be dealt with within the timescales required.

All data breaches, regardless of their severity and impact will be recorded in the council data breach register.

In the event of a data breach, employees must not speak to third parties or the press without permission from the Clerk. Any questions from third parties related to any suspected or actual data breach should be passed to the Clerk.

If there is doubt as to whether a data breach should be reported to the ICO and/or data subject, the Clerk should seek guidance from the ICO.

5. PERSONAL DATA BREACH NOTIFICATION: DATA CONTROLLER TO SUPERVISORY AUTHORITY

When the personal data breach or suspected data breach affects personal data that is being processed by Fakenham Town Council as a data controller, the following actions are performed by the Clerk:

1) Fakenham Town Council must establish whether the personal data breach should be reported to the Supervisory Authority.

2) In order to establish the risk to the rights and freedoms of the data subject affected, the Clerk must assess the risks in accordance with the guidelines outline in section 9.0 of this document and, where required, using the ICO tool here.

3) The Supervisory Authority must be notified (see here) with undue delay but no later than in 72 hours, if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.

Any possible reasons for delay beyond 72 hours must be communicated to the Supervisory Authority. The Clerk will send Notifications to the Supervisory Authority that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Breach Response Team Leader/ Data Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach

6. PERSONAL DATA BREACH NOTIFICATION: DATA CONTROLLER TO DATA SUBJECT

The Clerk must assess if the personal data breach is likely to result in high risk to the rights and freedoms of the data subject in accordance with the guidelines outlined in section 9 of this document. If there is a high risk, Fakenham Town Council must notify, without undue delay, the affected data subjects. The notification to the data subjects must be written in clear and plain language and include:

- The name and contact details of any data protection officer you have, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.
- If possible, Fakenham Town Council should give specific and clear advice to individuals on the steps they can take to protect themselves, and what Fakenham Town Council is able to do to help them. Depending on the circumstances, this may include such things as:
  - forcing a password reset;
  - advising individuals to use strong, unique passwords; and
  - telling them to look out for phishing emails or fraudulent activity on their accounts.

If, due to the number of affected data subjects, it is disproportionately difficult to notify each affected data subject, Fakenham Town Council must take the necessary measures to ensure that the affected data subjects are notified by using appropriate, publicly available channels.

7. PERSONAL DATA BREACH NOTIFICATION: DATA PROCESSOR TO CONTROLLER

Where Fakenham Town Council acts as a processor, any data breach identified must be reported, without undue delay to the controller(s) of the personal data. Information relating to relevant controllers of personal data will be found on the Records of Processing Activities (Processor) document. Information to provide to the controller should include:

- The date and time the breach was identified
- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Clerk
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any mitigating measures the controller needs to take

8. PERSONAL DATA BREACH NOTIFICATION: NOTIFICATION OF OTHER THIRD PARTIES

Fakenham Town Council is responsible for checking with sectoral regulations of the relevant parties that should be notified following a severe data breach. Significant cyber incidents may also need to be reported to the National Cyber Security Centre, more details can be found here.

Data breaches that may lead to individuals being victims of fraud should be reported to Action Fraud the UK's national fraud and cybercrime reporting centre.

It may also be necessary to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

9. GRADING THE PERSONAL DATA BREACH

Any incident must be graded according to the significance of the breach and the likelihood of serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation.

Likelihood grade	Likelihood of adverse effect	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred.	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Severity Grade	Severity of the adverse effect on Individuals	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach.
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred.	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be sending an email containing personal data about an employee to the wrong recipient.
3	Potentially some adverse effect.	An adverse effect may be release of confidential information into the public domain leading to embarrassment.
4	Potentially Pain and suffering/ financial loss.	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. A person is at risk of harassment or violence from exposed information.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence. Specific risk information for tailored response is wrong or not available.

9.1 BREACH ASSESSMENT GRID

This operates on a 5 x 5 basis with anything other than “grey breaches” being reportable. Incidents where the grading results are in the red are advised to notify data subjects.

s

Severity (Impact)	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood that citizens' rights have been affected (harm)				

Reviewed at Governance & Finance 21st July 2026

Ratified at Full Council 29th July 2026

To be reviewed annually

Fakenham Town Council

Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Appropriate Policy Document

for the Processing of Special Categories of Personal Data and Criminal Offences Data

Version History

DATE	VERSION NUMBER	NAME	CHANGE DESCRIPTION
12/06/2025	0.1	Bulletproof	Initial Document Creation
2/7/25	0.2	Fakenham Town Council	Document Review
21/07/26	0.3	Fakenham Town Council	Annual Document Review

CONTENTS

Purpose 3
Special Categories Data 3
What is special category data? 3
Special Category Data We Process 3
Criminal Offences Data 3
What is Meant by Criminal Offences Data? 3
Criminal Offences Data We Process 3
This Appropriate Policy Document 4
Conditions for Processing Special Category Data 4
How We Comply with the Data Protection Principles 4
Procedures for Ensuring Compliance with the Principles 5
Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. 5
Principle 2 - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. 5
Principle 3 - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. 5
Principle 4 - Personal data shall be accurate and, where necessary, kept up to date. 5
Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. 6
Principle 6 - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against personal data breaches. 6
Retention and Erasure Policies 6
Review Date 6
Further Information 6

Purpose

Fakenham Town Council. As part of its core services, employment, and recruitment functions, process special category data in accordance with the requirements of Article 9 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018') and criminal offences data in accordance with Article 10 of the GDPR and Schedule 1 of the DPA 2018.

This 'Appropriate Policy Document' sets out how we will protect special category data. We have this document in place to explain the basis on which we process this data and to demonstrate that our processing is compliant with principles set out in the GDPR and DPA 2018.

Special Categories Data

What is special category data?

Special Category Data under Article 9 of the UK GDPR covers processing in relation to data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of identifying a person, data concerning health, or a person's sex life or sexual orientation. This is collectively referred to as 'special category data'. This definition is also read to include nationality and disability information.

Special Category Data We Process

We process some special category data as part of our recruitment processes and, where necessary, in the course of employment to meet our obligations under laws such as the Equality Act 2010, or to verify that candidates are suitable for employment or continued employment. This type of data includes information relating to 'right to work' criteria (residency status etc.), needs, adaptations, and adjustments.

Special category data may be shared with the pension provider in the form of health information, disability information, and nationality/ residency/ citizenship information where this is required for the fair, lawful, and accurate provision of the pension product.

Special category data in the form of health information will be processed as part of sick pay and maternity pay.

Relevant special category data may be used as part of conduct and capability and disciplinary processes.

Criminal Offences Data

What is Meant by Criminal Offences Data?

Criminal Offences Data under Article 10 of the UK GDPR covers processing in relation to data revealing criminal convictions information, Disclosure and Baring Service (DBS) checks and reports, allegations data, observations (e.g., CCTV) that reveals that offences may have been committed. This is collectively referred to as 'criminal offences data'.

Criminal Offences Data We Process

We process some criminal offences data as part of our recruitment processes and, where necessary, in the course of employment to meet our obligations, or to verify that candidates are suitable for employment or continued employment. This type of data includes information relating to 'right to work' criteria checks, references from other employers, and the like.

Criminal offences data may be captured as part of allegations of wrongdoing on the part of the council, its employees, or others. It may be included in CCTV and other surveillance, in investigation reports, complaint forms, disciplinary processes, reports to law enforcement, the courts, or insurance providers. Some criminal offences data may be shared back with complainants.

This Appropriate Policy Document

The Data Protection Act 2018 Schedule 1 Paragraph 39 requires an appropriate policy document to be in place for the processing of special category data for the purposes of employment setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.
This document exists to fulfil our obligations in relation to Schedule 1 Parts 1, 2, and 3.
This information supplements our Employee Privacy Notice and Candidate Privacy Notice.

Conditions for Processing Special Category Data

We process special category data under Article 9 of the GDPR. Examples of our processing of such data include pre-employment checks and declarations by an employee in line with contractual obligations. The lawful bases we rely on to process such data are Article 6(b) performance of contract and Article 6(c) complying with our legal obligations to carry out statutory checks and in case the data is taken in the course of recruitment.
The conditions that we rely on under Schedule 1 of the Data Protection Act 2018 include:

- Schedule 1 Part 1 – Employment, social security and social protection: We process the data for the purposes of performing or exercising Employment, social security and social protection our obligations or rights under employment law.
- Schedule 1 Part 2
    - Legal proceedings
    - Equality of opportunity or treatment
    - Preventing or detecting unlawful acts
    - Protecting the public against dishonesty
    - Preventing fraud
    - Suspicion of financing terrorism or money laundering
    - Insurance
    - Occupational pensions
- Schedule 1 Part 3 – Consent: We may also process such data with the consent of the individual provided that it fulfils the requirements of a valid consent such as being freely given, informed, specific.

How We Comply with the Data Protection Principles

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer when required
- Taking a ‘data protection by design and default’ approach to our activities
- Maintaining documentation to support our processing activities
- Adopting and implementing data protection policies
- ensuring we have written contracts in place with our data processors
- Implementing appropriate security measures in relation to the personal data we process

- Carrying out data protection impact assessments for our high-risk processing

We regularly review our accountability measures and update or amend them when required.

Procedures for Ensuring Compliance with the Principles

When processing data, we meet the requirements of the data protection principles, as set out in data protection legislation:

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

We will process special category data only if we have a legal basis for processing and, in addition, if one of the specific processing conditions specified in the Schedule 1 of the DPA 2018 relating to special category data, applies.

In the case where we seek consent, we abide by the strict rules governing gaining and recording consent. No data subject will be compelled to provide written consent. Giving consent will always be an affirmative decision made by free will and will not be a contractual condition. Consent will be recorded as the condition for processing, and it may be withdrawn at any time.

We will inform the data subjects on how special category data is used when the data is collected. This information is set out in the Employee Privacy Notice and Candidate Privacy Notice.

Principle 2 - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

We process special category offence data for the purposes outlined above and in compliance with the legal conditions for processing. We do not use personal data for purposes that are incompatible with the original purpose.

Principle 3 - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

We collect and retain the minimum amount of information necessary to achieve the purposes outlined above. The information we process is necessary for and proportionate to our purposes. We do not collect any personal data that is irrelevant to, or over and above our identified need.

Principle 4 - Personal data shall be accurate and, where necessary, kept up to date.

We take the reasonable steps to ensure that the personal data we hold is up to date and accurate. Special category data will be obtained directly from applicants, staff and other data subjects or from external sources that we are entitled to assume will provide accurate information, such as the Disclosure and Barring Service.

We will erase or rectify inaccurate data that we hold without delay in accordance with our Data Protection Policy where an individual notifies us it that their personal data has changed or is otherwise inaccurate, or if it is otherwise found to be inaccurate. If we decide not to erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

We only keep personal data for as long as we need it, and then we dispose of it securely. These retention periods are detailed in the Council's Retention Schedules. At the end of the relevant retention period, the Council erases or securely destroys special category data.

Principle 6 - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against personal data breaches.

The Council has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data.

Electronic information is processed within our secure network. Hard copy information is processed within our secure premises. Our electronic systems and physical storage have appropriate access controls applied.

The Council has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Retention and Erasure Policies

Our retention and erasure practices concerning special category data are set out in the Council's Retention Schedule.

Review Date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed annually or revised more frequently if necessary. Where necessary, this policy will be amended to ensure that it remains up to date and accurately reflects the Council's approach to processing special category data.

Further Information

If you require further information or have a question about our handling of special category data, you can contact Fakenham Town Council.

- Email: info@Fakenhamtowncouncil.gov.uk
- Phone no: 01328 853653
- Address: Fakenham Town Council, Fakenham Connect, Oak Street, Fakenham, Norfolk, NR21 9DY

Reviewed at Governance & Finance 21st July 2026
To be reviewed annually

Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Fakenham Town Council

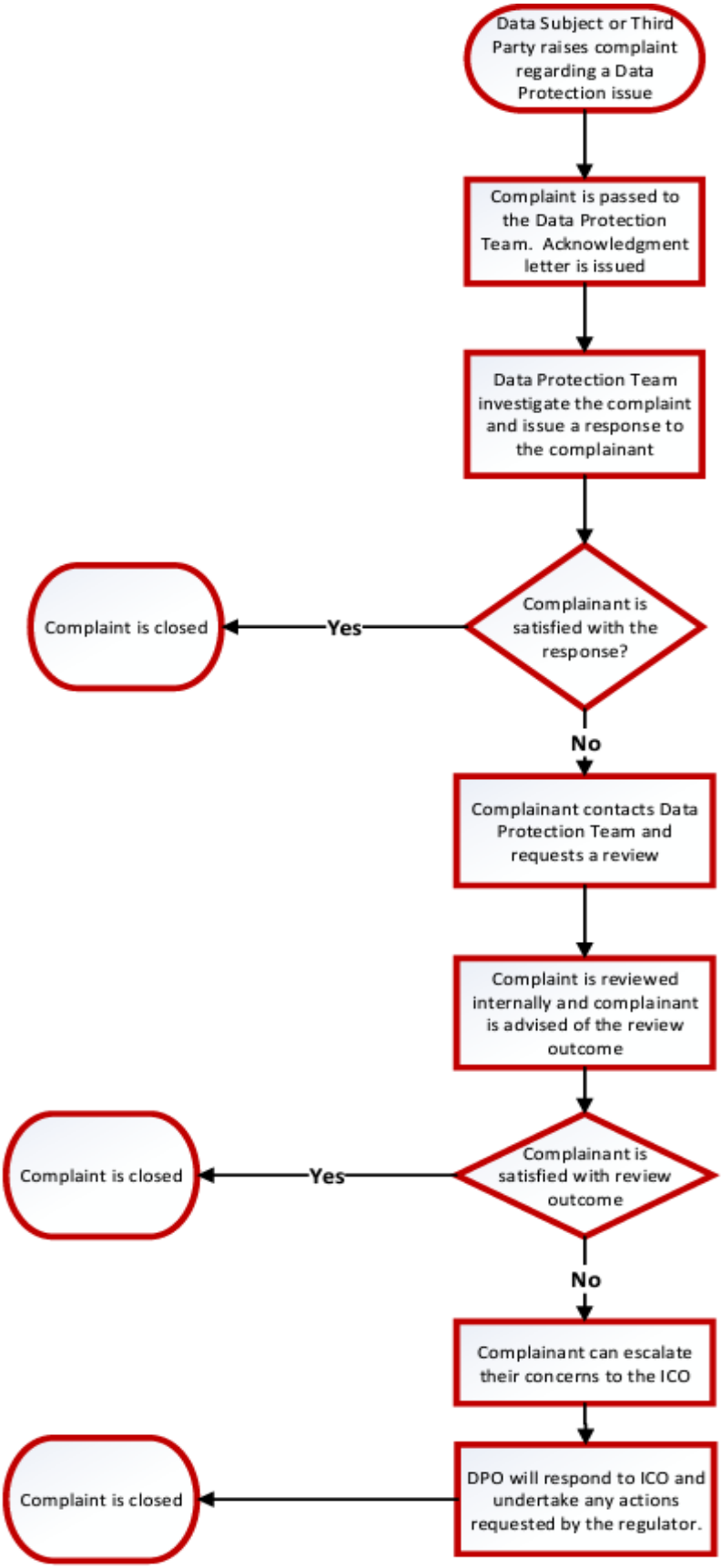
Data Protection Complaints procedure

Version History

DATE	VERSION NUMBER	NAME	CHANGE DESCRIPTION
11/06/2025	0.1	BulletProof	Initial Document Creation
11/07/2025	0.2	Fakenham Town Council	Document Reviewed
21/07/2026	0.3	Fakenham Town Council	Annual Document Review

CONTENTS

1 Introduction 3
2 Who Are Data Subjects? 3
3 Data Subjects' Rights 3
4 What Is A Complaint 3
5 Scope 3
6 Responsibilities 4
7 Making A Complaint 4
8 Investigation And Complaints Outcome 4
9 Review 4
10 Independent External Review 5
11 Manifestly Unfounded, Abusive, Vexatious Or Excessive Correspondence And Complaints Independent External Review 5
12 Use Of Data From Complaints 6


Data Subject or Third Party raises complaint regarding a Data Protection issue
Complaint is passed to the Data Protection Team. Acknowledgment letter is issued
Data Protection Team investigate the complaint and issue a response to the complainant
Complainant is satisfied with the response?
Yes
Complaint is closed
No
Complainant contacts Data Protection Team and requests a review
Complaint is reviewed internally and complainant is advised of the review outcome
Complainant is satisfied with review outcome
Yes
Complaint is closed
No
Complainant can escalate their concerns to the ICO
DPO will respond to ICO and undertake any actions requested by the regulator.
Complaint is closed

1 INTRODUCTION

- The General Data Protection Regulation ("GDPR"), the Data Protection Act 2018 ("DPA 2018"), and the Privacy and Electronic Communications Regulations ("PECR") (together, the "Data Protection legislation"), give data subjects and applicable third parties rights in relation to personal data. This procedure details how Fakenham Town Council (FTC) will respond to complaints from data subjects and third parties relating to the use of personal data.

2 WHO ARE DATA SUBJECTS?

- Data subjects are any natural living individuals whose personal data Fakenham Town Council processes (collects, obtains, stores, retains, disposes of etc.). Data subjects can include Employees, members, contractors, members of public etc.

3 DATA SUBJECTS' RIGHTS

- Under Data Protection legislation, data subjects have the right to the following and these rights can be exercised at any time:
    a. information about the processing of their data (GDPR Articles 12-14, and Recitals 58-62),
    b. access their own personal data (GDPR Articles 12 and 15, and Recital 63),
    c. correct personal data (GDPR Article 16),
    d. erase personal data, also known as the right to be forgotten (GDPR Article 17, and Recitals 65 and 66),
    e. restrict data processing (GDPR Article 18),
    f. object to data processing, including direct marketing (GDPR Article 21, and Recitals 69 and 70),
    g. receive a copy of their personal data or transfer their personal data to another data controller (data portability, GDPR Article 20, and Recital 68),
    h. not be subject to automated decision-making and rights in relation to profiling (GDPR Article 22, and Recital 71), and i. be notified of a data security breach (GDPR Article 34, and Recital 86).

4 WHAT IS A COMPLAINT

- A complaint is an expression of dissatisfaction about Fakenham Town Council's handling of a data subject's personal data or the data of the individual they represent. This can also include dissatisfaction with how Fakenham Town Council has responded to a previous data request, such as those detailed under 1.3.

5 SCOPE

- This procedure addresses complaints made by data subjects regarding the use of their personal data. Complaints may be made in relation to any aspect of Fakenham Town Council's processing of personal data including individual rights requests.

- This procedure also addresses complaints made by third parties in relation to the Council's use of personal data. These may be for example in relation to the Council's response to a data related request from a third party, such as the Police or Local Government Agencies.

- This procedure should also be followed for complaints in relation to use of personal data for direct marketing and/or profiling activity.

6 RESPONSIBILITIES

- The Clerk has overall responsibility for this procedure and all relevant members of staff have been made aware of the procedure and have received appropriate training.

- All Employees/Staff are responsible for ensuring that any complaints that are made in relation to this procedure are reported to the (Info@Fakenhamtowncouncil.gov.uk, and for cooperating with in reviewing these complaints.

- Fakenham Town Council will review this procedure from time to time (and at least on an annual basis) to ensure that its provisions continue to meet our legal obligations and reflect best practice.

7 MAKING A COMPLAINT

- Data subjects and third parties may make a complaint relating to the Council's use of personal data. Complaints should be sent directly to the team via email to ~~at~~ Info@Fakenhamtowncouncil.gov.uk or by post to Fakenham Town Council, Fakenham Connect, Oak Street, Fakenham, Norfolk, NR21 9DY. A member of the team will normally acknowledge the complaint within 5 working days. Fakenham Town Council reserves the right to extend the period we need for response if deemed a necessity.

- Although a complaint may be brought up at any time, there may be limits as to what the ~~company~~ council can do in historic cases.

- Fakenham Town Council will only accept a complaint from a data subject's representative, if the representative provides the data subject's written consent authorising the representative to act on the data subject's behalf in relation to the complaint.

- If there is any doubt about the identity of the complainant, the team will first seek to verify the data subject's identity or third party's entitlement to act on behalf of the individual. The forms of identification that are acceptable from a data subject are as follows; Passport, Driving Licence, or for third parties the identification requirements will vary dependent on their relationship to the data subject. Therefore these will be assessed on a case-by-case basis.

8 INVESTIGATION AND COMPLAINTS OUTCOME

- Once all identification requirements have been met, the investigation will be carried out normally within one month. If further clarification is required from the complainant or more time is required for the response to be completed, Fakenham Town Council will inform the complainant prior to the original deadline.

- The complaint outcome will be communicated to the complainant in writing, normally.

9. REVIEW

- If the complainant does not agree with the outcome, they can request a review of the decision. This request must be made within 1 month of the original decision being communicated and should be sent to the team via email Info@Fakenhamtowncouncil.gov.uk or by post to Fakenham Town Council, Fakenham Connect, Oak Street, Fakenham, Norfolk, NR21 9DY. The decision will be internally reviewed by the team responsible or responsible person normally within one month from the receipt of the request for Review.

- Once the internal review has been completed, Fakenham Town Council will communicate the outcome in writing, normally by email.

10 **INDEPENDENT EXTERNAL REVIEW**

- If the complainant remains dissatisfied, they can escalate their complaint to the Information Commissioner's Office (the "ICO"). Information about how to make a complaint to the ICO can be found here: https://ico.uk/make-a-complaint/

- In order to respond independently to the complaint, a Data Protection Officer may be appointed and the Data Protection Officer will investigate the complaint based on the information provided by the ICO. This may necessitate access to personal data and other information held with Fakenham Town Council. The cooperation of any staff members able to assist with the investigation will be required. The reason for the investigation may need to be disclosed to the relevant staff members.

- The Data Protection Officer will draft and submit a response to the ICO in consultation with the business's key stakeholders.

11. **MANIFESTLY UNFOUNDED, ABUSIVE, VEXATIOUS OR EXCESSIVE CORRESPONDENCE AND COMPLAINTS INDEPENDENT EXTERNAL REVIEW**

- In some scenarios we can refuse to handle the complaint. This will be when a complaint is deemed to be manifestly unfounded, abusive, vexatious or excessive. Each complaint will be considered on a case-by-case basis. The following factors will be taken into consideration:
    a. the data subject has explicitly stated that they intend to cause disruption (whether in the complaint, or in other correspondence), and has threatened individuals.
    b. the data subject has made unsubstantiated accusations against individuals, and is persisting in those accusations;
    c. the data subject is targeting particular individuals, against whom they have a personal grudge.
    d. the data subject makes frequent complaints intended to cause disruption; and
    e. the data subject continues to repeat the substance of previous complaints which have already been investigated.

- Where a complaint is deemed to be manifestly unfounded, excessive, abusive or vexatious, Fakenham Town Council will contact the individual and in a reasonable timeframe explain to them:
    a. the reasons for refusing to consider the complaint;
    b. their right to make a complaint to the ICO; and
    c. their right to pursue their data subject rights through a judicial remedy.

12. **USE OF DATA FROM COMPLAINTS**

- Fakenham Town Council will collect data on complaint outcomes at each stage of this procedure and any complaints submitted by complainants to any regulators (including the ICO) and use the data: a) internally for reporting, evaluation, learning and training; and b) externally for discussion with regulators.

- Your personal data and sensitive personal data ('Personal Data') as defined by the Data Protection Act 2018 (the "DPA") may be disclosed to Fakenham Town Council's members of staff and regulators only for the purpose of dealing with your complaint, or a complaint arising out of it and/or implementing any recommendations. Personal Data will not be shared with any other third parties unless Fakenham Town Council has your express consent, has a statutory obligation to do so, or is otherwise permitted to do so under the DPA.

Reviewed at Governance & Finance 21st July 2026

To be reviewed annually

Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Fakenham Town Council

Data Subject Rights Request Procedure

Version History

Date	Version Number	Name	Change Description
05/06/2025	0.1	Bulletproof	Initial Document Creation
19/08/2025	0.2	Fakenham Town Council	Document Review
21/07/2026	0.3	Fakenham Town Council	Annual Document Review

CONTENTS

1. Purpose 2
2. Scope 2
3. Data subject rights by lawful basis 2
4. Data subject rights request procedure 2
4.1 General points 2
4.2 Responsibilities 3
4.3 Right to withdraw consent 4
4.4 Right to be informed 4
4.5 Right of access 5
4.6 Right of rectification 6
4.7 Right to erasure 6
4.8 Right to restrict processing 7
4.9 Right to data portability 8
4.10 Right to object 9
4.11 Rights in relation to automated decision making and profiling 10
4.12 The right to complain 12

1. Purpose

The purpose of this procedure is to define what steps need to be taken when a data subject exercises one or more of the rights, they are granted under the Data Protection Act 2018/EU-GDPR/UK-GDPR.

2. Scope

The scope of this procedure will extend to all data subject rights requests made to The Fakenham Town Council.

3. Data subject rights by lawful basis

The following should be used as a guide to which rights of the data subject are relevant to each basis of lawful processing. The assumption made is that all personal data is being lawfully processed and personal data are necessary for the purposes for which they processed.

Data Subject Right	Lawful Basis					
	Consent	Contractual	Legal Obligation	Vital Interests	Public Interest	Legitimate Interest
Withdraw consent	Yes	No	No	No	No	No
Be Informed	Yes	Yes	Yes	Yes	Yes	Yes
Access	Yes	Yes	Yes	Yes	Yes	Yes
Rectification	Yes	Yes	Yes	Yes	Yes	Yes
Erasure	Yes	No	No	No	No	Yes
Restrict Processing	Yes	Yes	Yes	Yes	Yes	Yes
Data Portability	Yes	Yes	No	No	No	No
Object	N/A	No	No	No	Yes	Yes
Automated decision making and profiling	N/A	No	No	Yes	Yes	Yes

4. Data subject rights request procedure

4.1 General points

The following points apply to all data subject rights requests described in this document. Please see Article 12 of the GDPR for the full text.

1. Information will be provided to the data subject in a concise, transparent, intelligible, and easily accessible form using clear and plain language, for any information addressed specifically to a child.
2. Information will be provided to the data subject in writing, electronically, or by other means agreed.
3. The identity of the data subject must be established in relation to any request to exercise their rights. Where necessary Fakenham Town Council may request further information to establish the

identity of the data subject. If the identity cannot be established, the data subject rights request will be refused.

4. Where the data subject is being represented by a third party, the authorisation to act on behalf of the data subject must be verified in relation to any request to exercise rights on behalf of the data subject. Fakenham Town Council may request further information to establish this and, if this authorisation cannot be established, the data subject rights request will be refused.
5. If it is decided that Fakenham Town Council will not action the request, the data subject must be informed without delay and at the latest within one calendar month of the request. The reason for not acting and the right for the data subject to complain to the Supervisory Authority must be provided to the data subject.
6. Fakenham Town Council will not charge for data subject rights requests unless they are manifestly unfounded or excessive, in particular because of their repetitive character. However, the onus is on Fakenham Town Council to demonstrate this is the case. If a request is unfounded or excessive, Fakenham Town Council can decide not the action the request or charge a reasonable fee considering the administrative costs of providing the information.
7. Where Fakenham Town Council is acting as a processor, the Clerk will record the details of the data subject rights request, it will inform the controller without undue delay and provide support to the controller, where required, to satisfy the request.

4.2 Responsibilities

ACTIVITY	DESCRIPTION	RESPONSIBLE ROLE
Identifying data subject rights request	Handling the initial request, taking contact details and passing this on to the Clerk	All staff
Log data subject rights request and confirm receipt	Recording the request in the appropriate data subject rights request register and confirm receipt to data subject	All staff
Confirm the identity of data subject or third party acting on their behalf has authorisation to do so	Confirming the data subject is who they say they are, or the third party can provide evidence of authorisation to act for the data subject.	All staff
Evaluate validity of the request	Testing whether request is manifestly unfounded or excessive. Testing whether the request is reasonable and lawful – in relation to rights to rectification, restriction and objection.	Clerk
Confirming any charges or refusal to data subject	If the request is manifestly excessive or unfounded it can be charged for or refused.	Clerk
Communicating any extension to the one-month deadline and reasons why	If the request is going to be complex and is going to take longer than 1 calendar month, the data subject must be informed within one calendar month of their original request	Clerk
In the event of an access request, compiling requested information	Gathering personal data for request	Clerk
In the event of an access request, reviewing the compiled data	Identifying what needs to be provided to the data subject and redacting data that cannot be disclosed	Clerk

In the event of a rectification request, requesting evidence of the correct information	E.g. asking for proof of address	Clerk
In the event of requests other than access, ensuring requested action is taken	e.g. erasing data, making rectification, removing data subject from mailing list, stopping processing if consent is withdrawn	Clerk
In the event of an access request ensuring the information is provided to the data subject	This should be provided in a secure way by the means preferred by the data subject	Clerk
In the event of an access request, confirming the data subject has received the data	Confirming that the data is received and the access request is now closed	Clerk
Collating documentation and completing data subject rights register	Ensuring a complete record of the request is kept (where necessary) and recorded in the rights register	Clerk

4.3 Right to withdraw consent

Data subjects have the right to withdraw consent where the lawful basis for processing is identified as consent. There are two consent scenarios that may arise at Fakenham Town Council as follows:

Scenario 1

If consent was provided electronically via a tick box or similar, withdrawal of consent will not require this procedure as the data subject will be able to withdraw consent themselves.

Scenario 2

Where the data subject cannot withdraw consent electronically (e.g. if they have signed a document) they will need to contact Fakenham Town Council to exercise their right.

The steps for the procedure are as follows:

1. Identify a request to withdraw consent has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Clerk of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request (Clerk)
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject. (All Staff)
5. Verify the lawful basis used is consent, if not then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Clerk0
6. Record the request in the Rights Request Log. (Clerk)
7. Notify relevant parties internally and externally of request and ask them to stop processing immediately. (Clerk)
8. Respond to data subject/third party to confirm the request has been addressed and processing stopped in accordance with their wishes. (Clerk)
9. Complete the Rights Request Log. (Clerk)

4.4 Right to be informed

The right to be informed is satisfied by ensuring at the point where personal data is collected from the data subject or third party, the data subject is informed about the use of this and their rights by means of a data

privacy notice. As such, this is a right that will not be requested after processing has begun as the data subject's right to be informed would have been satisfied before this point.

4.5 Right of access

In principle, the Council will not normally disclose the following types of information in response to a Data Subject Access Request however, the decision of disclosure rests with the Clerk and each case must be reviewed on its own merits:

Information about other people – A Data Subject Access Request may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted unless the individuals involved consent to the disclosure of their data.

Repeat requests – Where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six-month period of the original request will be considered a repeat request, and the Council will not normally provide a further copy of the same data.

Publicly available information – The Council is not required to provide copies of documents which are already in the public domain.

Opinions given in confidence or protected by copyright law – The Council does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by copyright law.

Privileged documents – Any privileged information held by Council need not be disclosed in response to a DSAR. In general, privileged information includes any document which is confidential (e.g. a direct communication between a client and his/her lawyer) and is created for the purpose of obtaining or giving legal advice.

The steps for the procedure are as follows:

1. Identify a request for access has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Clerk of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request and get specific information about what data they wish to access and how they wish to be provided with the Data. (Clerk)
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject. (Clerk)
5. Verify that the request meets one of the above conditions, does not fall into any exceptions (see ICO guidance here) and is not manifestly unfounded or excessive. If it doesn't meet the conditions, there is an exception, or the request Is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Clerk)

This Information will need to include:

- The reasons the council is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Verify whether Fakenham Town Council is a controller or processor for the information requested. If Fakenham Town Council is a processor, identify the controller(s) and inform them immediately of the request and provide full details of the data subject and the request. Inform the data subject that their request has been passed to the data controller and provide the data subject with contact details for the controller. (Clerk)
7. Record the request in the Rights Request Log. (Clerk)
8. If Fakenham Town Council is a Controller, identify the relevant internal departments where the personal data requested is handled and gather relevant data in relation to the request. (Clerk)
9. Once the data requested is compiled, review the data to ensure data about any other data subjects is either redacted, or appropriate consent to disclose is obtained from that data subject. Also review the data in line with possible exemptions to disclosure in accordance with the ICO guidance here .(Clerk)
10. Compile the data for the data subject in the format requested (taking into consideration the need to secure this data in transmission to the data subject. (Clerk)
11. Contact the data subject and provide a copy of Fakenham Town Council's privacy notice along with the data requested (in a secure format). Ask the data subject to confirm receipt of the data. (Clerk)
12. Update the Rights Request Log with the latest information. (Clerk)

4.6 Right of rectification

Regardless of the lawful basis of processing, data subjects have the right to have personal data that is inaccurate corrected and to complete information that is incomplete.

This procedure applies where data subjects are unable to update/correct their own data e.g. through a customer portal/website.

The steps for the procedure are as follows:

1. Identify a request to update/correct/complete Information, obtain contact details of the data subject/ third party. (All Staff)
2. Contact data subject/third party to acknowledge request. (All Staff)
3. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject. (Clerk)
4. Ascertain changes required and ask for evidence of the change e.g. change of address - utility/council tax bill etc. (Clerk)
5. If there is a question over the accuracy or necessity of the changes being requested by the data subject (e.g. the request Is unfounded, excessive, or is asking to change factual Information), this should be escalated to the Clerk and the request handed to them for further Investigation. In this scenario, the Clerk should, if required, request to restrict all processing of this data subject's personal data until the question Is resolved.
6. Make changes and confirm these to the data subject/third party. As the data subject to confirm they are now happy with the changes. (Clerk)

4.7 Right to erasure

The right to erasure Is a conditional right and only applies where the following applies:

- The personal data is no longer necessary for the purpose which it was originally collected or processed for;
- Fakenham Town Council is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent.

- Fakenham Town Council is relying on legitimate interests the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing.
- Fakenham Town Council is processing the personal data for direct marketing purposes and the individual objects to that processing.
- Fakenham Town Council has processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- Fakenham Town Council must do it to comply with a legal obligation; or
- Fakenham Town Council has processed the personal data to offer information society services to a child.

The steps for the procedure are as follows:

1. Identify a request for erasure has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Clerk of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request. (All Staff)
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject. (Clerk)
5. Verify that the request meets one of the above conditions, does not fall into any exceptions (see ICO guidance here) and is not manifestly unfounded or excessive. If it doesn't meet the conditions, there is an exception, or the request is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Clerk)

This information will need to include:

- The reasons the council is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Record the request in the Rights Request Log (Clerk)
7. Identify third parties that the personal data involved has been shared with e.g. controllers, processors. (Clerk)
8. Notify relevant parties internally and externally of request and ask them to remove the data requested (remember this may require removal from backups) immediately.(Clerk)
9. Once erasure Is confirmed by all relevant parties, notify the data subject that their data has been erased as per the request. Ask the data subject to confirm receipt. (Clerk)
10. Update the Rights Request Log with the latest information. (Clerk)

4.8 Right to restrict processing

The right to restrict processing is a conditional right and data subjects can only exercise this right where:

- The individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the UK GDPR) and the individual opposes erasure and requests restriction instead;
- You no longer need the personal data, but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- The individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

The steps for the procedure are as follows:

1. Identify a request for restriction has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Clerk of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request and confirm the details of the request i.e. identify the reason for the request to restrict processing, what processing activities they want to restrict etc. (Clerk)
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject. (Clerk)
5. Verify that the request meets one of the above conditions and is not manifestly unfounded, or excessive. If it does not meet the conditions, or the request is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Clerk)

This information will need to include:

- The reasons the council is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Record the request in the Rights Request Log (Clerk).
7. Identify third parties that the personal data involved has been shared with e.g. controllers, processors and request they restrict processing until notified otherwise. (Clerk)
8. Notify relevant internal parties of the need to restrict processing. Agree on a method of restricting processing which could Include. (Clerk)

- Temporarily moving the data to another processing system;
- Making the data unavailable to users;
- Temporarily removing published data from a website; or
- Storing personal data somewhere to avoid erasure in a case where the data subject has asked to restrict processing for the purpose of retaining data beyond the time Fakenham Town Council would normally retain it.

9. Once restriction is confirmed by all relevant parties, notify the data subject that data processing has been restricted and will not resume until they inform Fakenham Town Council that processing can resume (if required). (Clerk)
10. Update the Rights Request Log with the latest information. (Clerk)

4.9 Right to data portability

The right to data portability gives individuals the right to receive personal data they have provided to Fakenham Town Council in a structured, commonly used and machine-readable format (e.g. XML, CSV, JSON). It also gives them the right to request that Fakenham Town Council transmits this data directly to another controller.

Data subjects can exercise this right where:

- The lawful basis for processing this information is consent, or for the performance of a contract; and
- Processing is carried out by automated means (i.e. excluding paper files).

The data required to be provided for this right only applies to personal data provided by the data subject e.g. name, address, email address etc AND personal data relating to the observation of an individual's activities e.g. search history, raw data processed by connected objects, location data.

The steps for the procedure are as follows:

1. Identify a request for data portability has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Clerk of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request and confirm the details of the request i.e. Identify what personal data they require, if there is a particular format they would like it in and whether they want the data transferred securely to another controller and, if so, contact details of that controller. (Clerk)
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject. (Clerk)
5. Verify that the request meets one of the above conditions and is not manifestly unfounded or excessive. If it does not meet the conditions, or the request is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Clerk)

This Information will need to include:

- The reasons the council is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Record the request in the Rights Request Log. (Clerk)
7. Notify relevant parties of the request and provide details of what data is to be extracted and the format requested by the data subject. (Clerk)
8. Extract the data and provide to the relevant parties. (Clerk)
9. Check the data to ensure there is no information that should not be disclosed to the data subject. (Clerk)
10. Provide the data to the data subject, or their nominated controller by a secure method e.g. secure file transfer, encrypted email, SFTP upload to the controller etc. (Clerk)
11. Confirm with the data subject that the data requested has been received by them or the new controller. (Clerk)
12. Update the Rights Request Log with the latest Information. (Clerk)

4.10 Right to object

Article 21 of the UK GDPR gives individuals the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent Fakenham Town Council from processing their personal data.

An objection may be in relation to all the personal data Fakenham Town Council holds about an individual, or only to certain information. It may also only relate to a particular purpose Fakenham Town Council is processing the data for.

The right to object only applies in certain circumstances. Whether it applies depends on the purposes for processing and the lawful basis for processing.
Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

Individuals can also object if the processing is for:

- A task carried out in the public interest;
- The exercise of official authority vested in Fakenham Town Council; or
- Legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute.

If the processing is for scientific or historical research, or statistical purposes, the right to object is more limited.
Refer to the ICO guidance on the full details of the limitations associated with this right here.

Note, the following does not apply if the user expresses their wish to object to direct marketing by clicking "unsubscribe" on marketing emails. In this situation, their objection will be recorded automatically and they will be removed from mailing lists to prevent any further marketing emails being sent. The minimal amount of data will be kept ensuring the objection is noted.

The steps for the procedure are as follows:

1. Identify a request to object to processing has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Clerk of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request and confirm the details of the request i.e. what exactly are they objecting to. (Clerk)
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject. (Clerk)
5. Verify that the request meets one of the above conditions and is not manifestly unfounded or excessive. If it does not meet the conditions, or the request is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Clerk)

This Information will need to include:

- The reasons the council is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Record the request in the Rights Request Log. (Clerk)
7. Identify third parties that the personal data involved has been shared with e.g. controllers, processors and request they cease processing and confirm this has been done. (Clerk)
8. Notify relevant internal parties of the need to cease processing and confirm this has been done. (Clerk)
9. Once processing has ceased and is confirmed by all relevant parties, notify the data subject that data processing has ceased. (Clerk)
10. Update the Rights Request Log with the latest Information. (Clerk)

4.11 Rights in relation to automated decision making and profiling

Where Article 22(1) applies, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

In this situation, processing can occur where processing is:

- Necessary for entering into or performance of a contract between an organisation and the individual;
- Authorised by law (for example, for the purposes of fraud or tax evasion); or
- Based on the individual's explicit consent.

In this situation, Fakenham Town Council needs to ensure data subjects can:

- Obtain human intervention;
- Express their point of view; and
- Obtain an explanation of the decision and challenge it.

Rights associated with automated decision making and profiling can be complex. The Clerk should refer to the ICO guidance here and seek the advice of the ICO/data privacy lawyers, if required.

The steps for the procedure are as follows:

1. Identify a request to object to exercise rights in relation to automated decision making and/or profiling has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Clerk of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request and confirm the details of the request i.e. what processing activities are involved. Details of why the data subject wishes to challenge any automated decision making should be obtained. (Clerk)
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject. (Clerk)
5. Verify that the request is relevant and that automated decision making and/or profiling with legal effects (or similarly significant effects) is taking place and the request is not manifestly unfounded or excessive. If the request is not relevant or is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Clerk)

This Information will need to include:

- The reasons the council is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Record the request in the Rights Request Log. (Clerk)
7. If the request is valid, the Clerk should identify any relevant internal or external parties involved in the processing and obtain details of the automated decisions making/profiling to discuss with the data subject. They should also identify a suitably qualified person who is authorised to intervene and overrule an automated decision.
8. The Clerk should discuss the process in depth with the data subject, explaining the decision-making process, how the decision was made etc. The data subject should be given the option to obtain human intervention and challenge the decision.
9. If the data subject wishes to obtain human intervention, the suitably qualified person identified as one that could overrule an automated decision should be asked to review the decision and document their findings and decision.

10. The data subject should be made aware of the human intervention, the decision-making process and the outcome. They should also be reminded of their rights to make a complaint to the ICO, or another supervisory authority. This should be made in writing. (Clerk)
11. Update the Rights Request Log with the latest Information. (Clerk)

4.12 The right to complain

The General Data Protection Regulation gives Data Subjects (natural living human beings) the right to complain about a business they believe to be mishandling personal data to the Information Commissioners Office (The ICO https://ico.org.uk/).
Complaints can contribute to the following eventualities:

- Fines under GDPR
- Unannounced audits
- Reputational damage

Fakenham Town Council is committed to protecting personal data and complying with the GDPR. This includes being transparent and handling customer complaints seriously. Fakenham Town Council enables data subjects to exercise their right to complain, either directly to the council, or to the Information Commissioner, by providing details of how to complain on the Privacy Notice.

Data subjects can complain to Fakenham Town Council or the ICO about:

- How their personal data has been processed
- How their request to exercise their rights has been handled
- How any complaints have been handled

They can also appeal against any decision made following a complaint.

All complaints made will be directed to the Clerk for resolution and will be resolved within one calendar month of receipt.

The steps for the procedure are as follows:

1. Complaint will be sent to the Clerk, any email complaints will automatically be routed to the Clerk, but telephone enquiries will be routed manually (All staff).
2. Notify the Clerk of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of complaint and confirm the details of the complaint. (Clerk)
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject. (Clerk)
5. Record the request in the Rights Request Log. (Clerk)
6. Investigate the complaint. (Clerk)
7. Respond to the data subject with findings/decisions and make them aware that they can exercise their right to complain to the Supervisory Authority (ICO) along with their contact details. (Clerk)
8. Update the Rights Request Log with the latest Information (Clerk)

Reviewed at Governance & Finance 21st July 2026
Ratified at Full Council 29th July 2026
To be reviewed annually

Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Fakenham Town Council

Website Privacy Notice

Contents

1. Introduction 2
2. Why we Collect your personal information 2
3. Lawful Basis Of Processing Information 2
4. What Information we collect and where from 2
5. How Long we Keep Information For 3
6. Security of personal information 3
7. Children's information 3
8. Your individual rights 3
9. Consent 5
10. Failure To Provide Personal Information 5
11. Cookies 5
12. Automated Decision Making 5
13. Transfers To Third Parties 6
14. Transfers Outside Of The UK 6
15. Right to complain 6
16. Additional information 7
18. Policy Review and Amendments 7

1**. Introduction**

We, Fakenham Town Council, take the protection of your personal data very seriously and strictly adhere to the rules laid out by data protection laws and the General Data Protection Regulation (GDPR-UK).

This privacy notice gives you information on how we collect and process your personal data through your use of this site and any data you may provide if you contact us regarding our products and services.

2. **Why we Collect your personal information**

We collect your personal data for one of the following purposes:

- To manage communications between you and us
- Where we need to perform the contract, we have entered into with you
- To provide you with information you have requested or which we may feel may be of interest to you
- To ensure the safe operation of our website and to monitor the performance of our website
- For marketing and advertising purposes
- To respond to your queries

3. **Lawful Basis Of Processing Information**

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where:

- The data subject (you) has given consent to the processing activity taking place.
- If the processing is necessary for the performance of a contract
- If the processing is necessary for compliance with a legal obligation to which the controller is subject
- If the processing in necessary for the purpose of the legitimate interest pursed by us or our partners

Where legitimate interest is identified as a lawful basis, we will undertake a legitimate interest assessment which is a three-part test covering:

The purpose test – to identify the legitimate interest
Necessity test – to consider if the processing is necessary for the purpose identified
Balancing test – considering the individual's interests, rights or freedoms and whether these override the legitimate interests identified.

4. **What Information we collect and where from**

We collect personal information from you, for example, if you request information, call us, contact us, use any of our services, you provided us with the information. The categories of

personal information that we may collect, store and use about you include:

- Name, personal or business address, personal or business telephone number, personal or business email address.
- Traffic data, location data, weblogs and other communication data
- IP address and website activity including tracking cookies
- Financial data such as Account Statements, Bank account details.

5. **How Long we Keep Information For**

We pride ourselves on ensuring that your personal data is only retained for the period that we need it for, or in accordance with laws, regulations and professional obligations that we are subject to. All personal information collect has a defined retention period. If you would like to find out how long your information is being retained, please see "additional information", section 16 of this policy.

6**. Security of personal information**

We take the responsibility for protecting your privacy very seriously and we will ensure your data is secured in accordance with our obligations under the Data Protection laws. We have in place technical and organisational measures to ensure personal information is secured and to prevent your personal data from being accessed in an unauthorised way, altered or disclosed. We have in place a robust access control policy which limits access to your personal data to those employees, contractors and other third parties who only have a business need to know. The processing of your personal data will only take place subject to our instruction.

We have policies and procedures in place to handle any potential data security breaches and data subjects, third parties and any applicable regulators will be notified where we are legally required to do so.

We have ensured that all employees have had data protection training. If you would like more details of the security we have in place, please see "additional information", section 16 of this policy.

7. **Children's information**

We do not knowingly collect information on children. If we have collected personal information on a child, please contact us immediately using the details in section 16, so we can remove this information without any undue delay.

8. **Your individual rights**

In this section, we have summarised the rights that you have under General Data Protection Regulation. Some of the rights are complex, and not all the details have been included in our

summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

Your principal rights under General Data Protection Regulation are:

- Right to Object
- Right of Access
- Right to be Informed
- Right to Rectification
- Right to Erasure
- Right to Restrict Processing
- Right to Data Portability

- The right to object
  You can exercise this right if:
  - Processing relies on legitimate interest
  - Processing is for scientific or historical research
  - Processing includes automated decision making and profiling
  - Processing is for direct marketing purposes
- The right of access
  - You or any third party acting on your behalf with your authority may request a copy of the personal data we hold about you without charge.
  - We will ask to verify your identity or request evidence from the third party that they are acting on your behalf before releasing any personal data we hold about you.
- The right to be informed
  We are required, to provide clear and transparent information to you about how we process your personal data. This privacy notice addresses this right.
- The right of rectification
  - If you believe the personal data we hold about you is incorrect or incomplete you have the right to correct this and you may exercise this right along with the right to restrict processing until these corrections are made.
- The right to erasure
  - If there is no legal basis or legitimate reason for processing your personal data, you may request that we erase it.
- The right to restrict processing
  - You may ask us to restrict the processing of your personal data. This means we will still hold it but not process it. This is a conditional right which may only be exercised when:
  - Processing is unlawful
  - We no longer need the personal data, but it is required for a legal process

    - You have exercised your right to object to processing and require processing to be halted while a decision on the request to object is made.
    - If you are exercising your right to rectification
- The right to data portability
    - You can request that your personal data is transferred to another controller or processor in a machine-readable format if:
    - Processing is based on consent
    - Processing is by automated means (i.e. not paper based)
    - Processing is necessary for the fulfilment of a contractual obligation
- Right to object automated decision making or profiling
    - You can request to obtain human intervention
    - You can express your point of view
    - You can obtain an explanation of the decision reached after an assessment
    - You can challenge such decisions

If you have any question about these rights, please see "additional information", section 16 of this policy.

9**. Consent**

Where you have given consent for processing, or explicit consent in relation to the processing of special category data, you have the right to withdraw this consent at any time, but this will not affect the lawfulness of processing based on consent before its withdrawal.

10. **Failure To Provide Personal Information**

Where we need to collect personal data by law or in order to process your instructions or perform a contract we have with you and you fail to provide that data when requested, we may not be able to carry out your instructions or perform the contract we have or are trying to enter into with you. In this case, we may have to cancel our engagement or contract you have with us, but we will notify you if this is the case at the time.

11. **Cookies**

Our website uses cookies. Please see our website for further details of the cookies used.

12. **Automated Decision Making**

Your personal data is not used in any automated decision making (a decision made solely by automated means without any human involvement) or profiling (automated processing of personal data to evaluate certain conditions about an individual).

13. **Transfers To Third Parties**

Fakenham Town Council may disclose your personal data, listed in section 4 to some third parties to help us deliver our services/products. All third parties are contractually bound to protect the personal data we provide to them. We may use several or all of the following categories of recipients:

- Suppliers and contractors for the performance of any contract we enter into with them or you
- Third parties that support us to provide products and services e.g. IT support, cloud-based software services, providers of telecommunications equipment)
- Payment service providers
- Recruitment service providers
- Professional advisors e.g. lawyers, auditors
- Web analytics and search engine provider to ensure the continued improvement and optimisation of our website.

14**. Transfers Outside Of The UK**

In this section, we provide information about the circumstances in which your personal data may be transferred and stored in countries outside the UK.

We may share personal information to third parties outside of the UK. Any personal information transferred will only be processed on our instruction and we ensure that information security at the highest standard would be used to protect any personal information as required by the Data Protection laws.

Where personal data is transferred outside of the UK to a country without an adequacy decision, we will ensure appropriate safeguards are in place prior to the transfer. These could include:

- Standard Contractual Clauses with the UK Addendum
- International Data Transfer Agreement
- Binding Corporate Rules
- An exception as defined in Article 49 of the EU GDPR

For more information about transfers and safeguarding measures, please contact us using the information in section 16.

15. **Right to complain**

We take complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading, or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

If you are not happy with how we have handled your personal data you have the right to make a complaint, please contact us via email on Info@Fakenhamtowncouncil.gov.uk

Alternatively, you can contact us:

Fakenham Town Council
Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY

Full details of the procedure can be found in our Data Protection Complaints procedure

~~Alternatively, you can make a~~ You may make a complaint to the Information Commissioner's Office after the complaint has been investigated by the Council if you are still not satisfied.

~~**By Post:** Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF~~

By Website: Click Here

By Email: Click Here

By Phone: 0303 123 1113 (Local rate) or 01625 545 745 (National rate)

16. **Additional information**

Your trust is important to us. That is why we are always available to talk with you at any time and answer any questions concerning how your data is processed. If you have any questions that could not be answered by this privacy policy or if you wish to receive more in-depth information about any topic within it, please contact our team via email on Info@Fakenhamtowncouncil.gov.uk.

18. Policy Review and Amendments

We keep this Policy under regular review.

This Policy was reviewed at Governance & Finance on ~~19/08/2025~~ 21st July 2026

To be reviewed annually

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Fakenham Town Council

Employee Privacy Notice

Contents

1. Introduction 2
2. Why we Collect your personal information 2
3. Lawful Basis Of Processing Information 2
4. What Information we collect and where from 3
4.1 Special Category Data 3
4.2 Third Party Collection of Personal Data 4
5. How Long we Keep Information For 4
6. Security of personal information 4
7. Children's information 4
8. Your individual rights 5
9. Consent 6
10. Failure To Provide Personal Information 6
11. Cookies 6
12. Automated Decision Making 6
13. Transfers To Third Parties 6
14. Transfers Outside Of The UK 7
15. Right to complaint 7
16. Additional information 8
17. Policy Review and Amendments 8

1. Introduction

We, The Fakenham Town Council (hereinafter referred as "FTC"), take the protection of your personal data very seriously and strictly adhere to the rules laid out by data protection laws and the General Data Protection Regulation (GDPR-UK).

This privacy notice gives you information on how we collect and process your personal data at recruitment, during employment and after your employment with us.

If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the us using the contact information in section 16 of this privacy notice.

2. Why we Collect your personal information

We collect your personal data for one of the following purposes:

- To manage communications between you and us
- To record and manage absence, sickness and other types of leave as required
- To process your payroll
- To follow our recruitment process and determine eligibility for the advertised role
- To check your eligibility to work
- To ensure we are able to support you with any disabilities you may have
- Where we need to assess your ability to work (occupational health)
- To ensure we can contact your next of kin in the event of an emergency
- To validate your qualifications and employment history
- To comply with UK employment and tax laws
- For monitoring performance and assessing progress
- To fulfil our legal obligations
- Managing access to council services
- For provision of providing training to staff
- For future referencing
- For life and medical insurance purposes
- For following our grievances and disciplinary internal policies
- To pay your expenses

3. Lawful Basis Of Processing Information

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where:

- The data subject (you) has given consent to the processing activity taking place.
- If the processing is necessary for the performance of a contract
- If the processing is necessary for compliance with a legal obligation to which the controller is subject
- If the processing in necessary for the purpose of the legitimate interest pursed by us or our partners.

Where legitimate interest is identified as a lawful basis, we will undertake a legitimate interest assessment which is a three-part test covering:

The purpose test – to identify the legitimate interest

Necessity test – to consider if the processing is necessary for the purpose identified

Balancing test – considering the individual's interests, rights or freedoms and whether these override the legitimate interests identified.

4. What Information we collect and where from

We collect personal information from you, for example, if you register to our website, request product information, call us or use any of our services. The categories of personal information that we may collect, store and use about you include:

- Name, address, telephone number, email.
- Bank details, P60, SSP information
- Payroll records
- Pension benefits information
- Your country of birth, nationality.
- Date of birth
- Passport details, Driving license, national insurance number.
- Employment history (records including hours of work, commencement date, training records, probation length, employee reference number, job titles, contracts, appraisal details, CV, covering letters, references, disciplinary and grievance records)
- Qualifications & Training history
- Next of kin details
- Emergency contact details
- Marital status
- Leave dates
- Absence information
- Student loan information
- Copies of your CV and covering letters
- Audit logs of use of computer and telephone systems
- Photographs

4.1 **Special Category Data**

We collect the following special category data from you:

- Sickness details
- Disability details
- Health details (including sickness details, GP fit note, maternity risk assessment with expected due date, disability information for reasonable adjustment, type of injury in case of accidents on work premises)

We will only process special category data where we have an Article 9 exception allowing us to do so, in this case, this is processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment as per Article 9 Paragraph 2b of the GDPR and the Data Protection Act 2018, schedule 1 condition 1.

4**.2 Third Party Collection of Personal Data**

We may also collect your data through Third Parties such as recruitment websites and consultants if you applied for a role via these methods. Additionally, we may collect information from former employers, background check providers and credit refence agency.

During the course of your employment, we may collect other related employment data such as sickness or medical records from your GP, treating physician or occupational health advisor.

5. How Long we Keep Information For

We pride ourselves on ensuring that your personal data is only retained for the period that we need it for, or in accordance with laws, regulations and professional obligations that we are subject to. All personal information collect has a defined retention period, which is in-line with our retention policy. If you would like to find out how long your information is being retained, please see "additional information", section 16 of this policy.

6. Security of personal information

We take the responsibility for protecting your privacy very seriously and we will ensure your data is secured in accordance with our obligations under the Data Protection laws. We have in place technical and organisational measures to ensure personal information is secured and to prevent your personal data from being accessed in an unauthorised way, altered or disclosed. We have in place a robust access control policy which limits access to your personal data to those employees, contractors and other third parties who only have a business need to know. The processing of your personal data will only take place subject to our instruction.

We have policies and procedures to handle any potential data security breaches and data subjects, third parties and any applicable regulators will be notified where we are legally required to do so.

We have ensured that all employees have had information security and data protection training. If you would like more details of the security we have in place, please see "additional information", section 16 of this policy.

7. Children's information

We do not knowingly collect information on children. If we have collected personal information on a child, please contact us immediately using the details in section 15, so we can remove this information without any undue delay.

8. Your individual rights

In this Section, we have summarised the rights that you have under General Data Protection Regulation. Some of the rights are complex, and not all the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

Your principal rights under General Data Protection Regulation are:

- Right to Object
- Right of Access
- Right to be informed
- Right to Rectification
- Right to Erasure
- Right to Restrict Processing
- Right to Data Portability

- The right to object

  You can exercise this right if

  - Processing relies on legitimate interest
  - Processing is for scientific or historical research
  - Processing includes automated decision making and profiling
  - Processing is for direct marketing purposes
- The right of access
  - You or any third party acting on your behalf with your authority may request a copy of the personal data we hold about you without charge.
  - We will ask to verify your identity or request evidence from the third party that they are acting on your behalf before releasing any personal data we hold about you.
- The right to be informed

  We are required, to provide clear and transparent information to you about how we process your personal data. This privacy notice addresses this right.
- The right of rectification
  - If you believe the personal data we hold about you is incorrect or incomplete you have the right to correct this and you may exercise this right along with the right to restrict processing until these corrections are made.
- The right to erasure
  - If there is no legal basis or legitimate reason for processing your personal data, you may request that we erase it.
- The right to restrict processing

    - You may ask us to restrict the processing of your personal data. This means we will still hold it but not process it. This is a conditional right which may only be exercised when:
    - Processing is unlawful
    - We no longer need the personal data, but it is required for a legal process
    - You have exercised your right to object to processing and require processing to be halted while a decision on the request to object is made.
    - If you are exercising your right to rectification
- The right to data portability
    - You can request that your personal data is transferred to another controller or processor in a machine-readable format if:
    - Processing is based on consent
    - Processing is by automated means (i.e. not paper based)
    - Processing is necessary for the fulfilment of a contractual obligation

If you have any question about these rights, please see "additional information", section 16 of this policy.

9. Consent

Where you have given consent for processing, or explicit consent in relation to the processing of special category data, you have the right to withdraw this consent at any time, but this will not affect the lawfulness of processing based on consent before its withdrawal.

10. Failure To Provide Personal Information

Where we need to collect personal data by law or in order to process your instructions or perform a contract we have with you and you fail to provide that data when requested, we may not be able to carry out your instructions or perform the contract we have or are trying to enter into with you. In this case, we may have to cancel our engagement or contract you have with us, but we will notify you if this is the case at the time.

11. Cookies

Our website uses cookies. Please see our website for further details of the cookies used.

12. Automated Decision Making

Your personal data is not used in any automated decision making (a decision made solely by automated means without any human involvement) or profiling (automated processing of personal data to evaluate certain conditions about an individual).

13. Transfers To Third Parties

FTC may disclose your personal data, listed in Section 4 to some third parties to help us perform our day-to-day activities. All third parties are contractually bound to protect the personal data we provide to them. We may use several or all of the following categories of recipients:

- Suppliers and contractors for the performance of any contract we enter into with them or you
- Third parties that support us to provide products and services e.g. IT support, cloud-based software services, providers of telecommunications equipment)
- Payment service providers
- Recruitment service providers
- Professional advisors e.g. lawyers, auditors
- Web analytics and search engine provider to ensure the continued improvement and optimisation of our website.

14. Transfers Outside Of The UK

In this section, we provide information about the circumstances in which your personal data may be transferred and stored in countries outside the United Kingdom (UK).

We may share personal information to third parties outside of the UK. Any personal information transferred will only be processed on our instruction and we ensure that information security at the highest standard would be used to protect any personal information as required by the Data Protection laws.

Where personal data is transferred outside of the UK to a country without an adequacy decision, we will ensure appropriate safeguards are in place prior to the transfer. These could include:

- Standard Contractual Clauses with the UK Addendum
- International Data Transfer Agreement
- Binding Corporate Rules
- An exception as defined in Article 49 of the EU GDPR

For more information about transfers and safeguarding measures, please contact us using the information in section 16.

15. Right to complaint

We take complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading, or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact us via email on Info@Fakenhamtowncouncil.gov.uk

Alternatively, you can contact us:

Fakenham Town Council
Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9HA

01328 853653

Alternatively, you can make a complaint to the Information Commissioner's Office:

By Post:

Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

By Website: Click Here

By Email: Click Here

By Phone: 0303 123 1113 (Local rate) or 01625 545 745 (National rate)

16. Additional information

Your trust is important to us. That is why we are always available to talk with you at any time and answer any questions concerning how your data is processed. If you have any questions that could not be answered by this privacy policy or if you wish to receive more in-depth information about any topic within it, please contact us via email on Info@Fakenhamtowncouncil.gov.uk

17. Policy Review and Amendments

We keep this Policy under regular review.

Policy Reviewed at Governance & Finance ~~19th August 2025~~ 21st July 2026

To be reviewed annually

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.