FLITWICK TOWN COUNCIL

INFORMATION & DATA PROTECTION POLICY.

Adopted by Council: 15 September 2020. Review Date: October 2021

Scope

This Policy consists of a suite of inter-linked policies:

Information and Data Protection Policy
Appendix 1-Information Security Policy
Appendix 2- Data Breach Notification Policy
Appendix 3- CCTV Policy
Appendix 4- Subject Access Policy

Introduction

In order to conduct its business, services and duties, Flitwick Town Council (FTC) processes a wide range of data, relating to its own operations and some which it handles on behalf of partners. In broad terms, this data can be classified as:

- Data shared in the public arena about the services it offers, its mode of operations and other information it is required to make available to the public.
- Confidential information and data not yet in the public arena such as ideas or policies that are being worked up. (*unlikely to be personal or sensitive data under GDPR, but confidential never the less*)
- Confidential information about other organisations because of commercial sensitivity. *(All Confidential* information *which is also Personal information comes under GDPR)*
- Personal data concerning its current, past and potential employees, councillors, and volunteers. (*GDPR applies*)
- Personal data concerning individuals who contact it for information, access its services or facilities or to make a complaint. (*GDPR applies see definition of personal data in 7 below*)
- Data passed to a third party (data processor) who undertakes a service or task for FTC, or we have a legal obligation to inform, or we need to share information with (e.g. Pension provider, HMRC). *(GDPR applies)*
- Data processed on behalf of another organisation such as a Trust of which the Council is a trustee, or community partner. *(GDPR applies if that is personal data)*

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

This Policy is linked to our Quality Policy, Digital and ICT Policy and Data Management Policy which will ensure information considerations are central to the ethos of the organisation.

The Town Council will periodically review and revise this policy in the light of experience, advice from its Data Protection Compliance Officer (DPCO), comments from data subjects and guidance from the Information Commissioners Office.

The Council will be as transparent as possible about its operations and will work closely with public, community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the Town's communities. Details of information which is routinely available is contained in the Council's Publication Scheme (on our Website) which is based on the statutory model publication scheme for local councils.

Protecting Confidential or Sensitive Information

Flitwick Town Council recognises it must at times, keep and process sensitive and personal information about both employees and the public. It has therefore adopted this policy not only to meet its legal obligations but to ensure high standards.

The General Data Protection Regulation (GDPR) 'which became law on 25th May 2018 and the Data Protection Act 2018, will, like the the Data Protection Act 1998 before them, seek to strike a balance between the rights of individuals and the sometimes, competing interests of those such as the Town Council with legitimate reasons for using personal information. The policy is based on the premise that Personal Data must be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data Protection Terminology

Data subject means the person whose personal data is being processed.
That may be an employee, prospective employee, member or prospective member of FTC, or someone volunteering to work with it. It may also be someone transacting with it in some way, or an employee, member or volunteer with one of our clients or partner organisations, or persons transacting or contracting with one of our clients or partners when we process data for them.

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

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

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

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

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

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

Consent is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out

Privacy Notice is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.

Flitwick Town Council processes **personal data** in order to:

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

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

The Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

- Processing is necessary for the performance of a contract or agreement with the individual
- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions
- The individual has consented to the processing
- Processing is necessary in order to pursue the legitimate interests of the data controller.

Particular attention is paid to the processing of any **sensitive personal information** and the Town Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual
- Required by law to process the data for employment purposes
- A requirement in order to protect the vital interests of the individual or another person

Who is responsible for protecting a person's personal data?

The Town Council as a corporate body has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Council has delegated this responsibility day to day to the Town Clerk.

- E mail: RobMcGregor@flitwick.gov.uk
- Phone: 01525 631900
- Correspondence: The Town Clerk, The Rufus Centre, Steppingley Rd, Flitwick, Bedford MK45 1AH

The Town Council has also appointed another senior member of staff, the Communication and Marketing Officer, as a non-statutory Data Protection Compliance Officer to ensure compliance with Data Protection legislation.

- E mail: beverleyjones@flitwick.gov.uk
- Phone: 01525 631900

- Correspondence: Communication & Marketing Officer, The Rufus Centre, Steppingley Rd, Flitwick, Bedford MK45 1AH

FTC has thought carefully about whether or not it is wishes under DPA & GDPR to appoint a formal Data Protection Officer (DPCO) on a voluntary basis. In reaching its conclusion it has considered the guidance issued by Article 29 Working Party and considers that if it were a similar sized private business that it would **not** need to appoint a DPCO for the following reasons:

- Data processing is not a core activity of the Council.
- Its data processing is not of 'large scale', when considering the number of data subjects concerned, the population and number of electors in the town, the volume of data or range of data items, the duration of the processing; and the geographical extent of the processing.
- The Council does not undertake regular or systematic monitoring of data subjects with little infringement on their data subject rights.
- It rarely processes sensitive data and only then on a small group of data subjects.

FTC, as data controller and indeed data processor, remains responsible for compliance with the data protection legislation including the GDPR. All Councillors and staff are expected to apply data protection legislation in their work.

FTC has appointed its Communications and Marketing Officer as '**Data Protection Compliance Officer' (DPCO)**. This title is used to avoid confusion with the GDPR required DPCO, to which specific responsibilities are attached under the legislation.

Diversity Monitoring

Flitwick Town Council may monitor the diversity of its employees, and councillors, in order to ensure that there is no inappropriate or unlawful discrimination in the way it conducts its activities. It may undertake similar data handling in respect of prospective employees. This data will always be treated as confidential. It will only be accessed by authorised individuals within the Council and will not be disclosed to any other bodies or individuals. Diversity information will never be used as selection criteria and will not be made available to others involved in the recruitment process. Anonymised data derived from diversity monitoring will be used for monitoring purposes and may be published and passed to other bodies.

Privacy Notices-Employees and Councillors

The Council will always give guidance on personnel data to employees, councillors, partners and volunteers through a Privacy Notice and ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request. This will be available on our website.

Data Security and Overseas Transfers

The Town Council will ensure the security of personal data. We will make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies.
We will only keep your data for the purpose it was collected for and only for as long as is necessary. after which it will be deleted.

Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personal data shall not be transferred to a country or territory outside the European Economic Areas unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Information provided to us

The information provided (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible for us to contact, respond to or conduct the transaction requested by the individual. By transacting with Flitwick Town Council, individuals are deemed to be giving consent for their personal data provided to be used and transferred for that purpose in accordance with this policy and our Privacy Notice, however in other cases specific written consent will be sought. It is the responsibility of those individuals to ensure that the Town Council is able to keep their personal

data accurate and up to date. The personal information will be not shared or provided to any other third party or be used for any purpose other than that for which it was provided.

We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Privacy Notices-General
The Council will always give guidance on personnel data to members of the public or businesses who transact with us, through a Privacy Notice and ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request. This will be available on our website.

Privacy Notices-Website
The Council will always give guidance on personnel data to anyone using its website or transacting with it by digital means through a Privacy Notice and ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request. This will be available on our website.

Rights of a Data Subject

1) The right to access personal data we hold on you

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request, we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2) The right to correct and update the personal data we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3) The right to have your personal data erased

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4) The right to object to processing of your personal data or to restrict it to certain purposes only

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5) The right to data portability

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6) The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details).

You may access these rights by contacting the Town Clerk

7) The right to lodge a complaint with the Information Commissioner's Office.

- You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

The Council will always give guidance on personnel data to employees through the Employee handbook and through a privacy notice.

The Council will ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Making Information Available

The Publication Scheme is a means by which the Council can make a significant amount of information available routinely, without waiting for someone to specifically request it. The scheme is intended to encourage local people to take an interest in the work of the Council and its role within the community.

In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Council publishes or intends to publish. It is supplemented with an Information Guide which will give greater detail of what the Council will make available and hopefully make it easier for people to access it.

All formal meetings of Council and its committees are subject to statutory notice being given on notice boards, the Website and sent to the local media. The Council publishes an annual programme in May each year. All formal meetings are open to the public and press and reports to those meetings and relevant background papers are available for the public to see. The Council welcomes public participation and has a public participation session on each Council and committee meeting. Details can be seen in the Council's Standing Orders, which are available on its Website or at its Offices.

Occasionally, Council or committees may need to consider matters in private. Examples of this are matters involving personal details of staff, or a particular member of the public, or where details of commercial/contractual sensitivity are to be discussed. This will only happen after a formal resolution has been passed to exclude the press and public and reasons for the decision are stated. Minutes from all formal meetings, including the confidential parts are public documents.

The Openness of Local Government Bodies Regulations 2014 requires written records to be made of certain decisions taken by officers under delegated powers. These are not routine operational and administrative decisions such as giving instructions to the workforce or paying an invoice approved by Council but would include urgent action taken after consultation with the Chairman, such as responding to a planning application in advance of Council. In other words, decisions which would have been made by Council or committee had the delegation not been in place.

The 2014 Regulations also amend the Public Bodies (Admission to Meetings) Act 1960 to allow the public or press to film, photograph or make an audio recording of council and committee meetings normally open to the public. The Council will where possible facilitate such recording unless it is being disruptive. It will also take steps to ensure that children, the vulnerable and members of the public who object to being filmed are protected without undermining the broader purpose of the meeting.

The Council will be pleased to make special arrangements on request for persons who do not have English as their first language or those with hearing or sight difficulties.

Disclosure Information

The Council will as necessary, undertake checks on both staff and Members with the the Disclosure and Barring Service and will comply with their Code of Conduct relating to the secure storage, handling, use, retention and disposal of Disclosures and Disclosure Information. It will include an appropriate operating procedure.

Data Transparency

The Council recognises their responsibility to act in accordance with the Local Government Transparency Code (February 2015). This sets out the key principles for local authorities in creating

greater transparency through the publication of public data and is intended to help them meet obligations of the legislative framework concerning information.

“Public data” means the objective, factual data on which policy decisions are based and on which public services are assessed, or which is collected or generated in the course of public service delivery.

The Code will therefore underpin the Council’s decisions on the release of public data and ensure it is proactive in pursuing higher standards and responding to best practice as it develops.

The principles of the Code are:
Demand led: new technologies and publication of data should support transparency and accountability.

Open: the provision of public data will be integral to the Council’s engagement with residents so that it drives accountability to them.

Timely: data will be published as soon as possible following production.

The Council will display at least the amount of data prescribed in the Code on its website and will often voluntarily exceed this requirement.

Appendix 1. FLITWICK TOWN COUNCIL: INFORMATION SECURITY POLICY

Principles and Purpose
This Policy sets out the Council’s commitment to information security within the Council and provides clear direction on responsibilities and procedures.

Flitwick Town Council is a Data Controller, as defined under the Data Protection Act 2018, and pays the appropriate annual fee with the Information Commissioner’s Office.

PROTOCOLS

System Security Processes and Procedures

The Council will provide and maintain security processes and procedures for all key information systems.

The procedures will uphold the principles of confidentiality, integrity, availability and suitability and be assessed for their impact upon other systems and services.

The security procedures will provide preventative measures to reduce the risks to the system, the information held within the system and the service it supports.

A Continuity plan will be developed and maintained for each system to ensure the principles are sustained and enable the continuation of services following failure or damage to systems or facilities.

The Town Clerk will be responsible for the implementation and promotion of the procedures.

Physical Security

Adequate and practical access controls will be provided in all areas in which personal and business data is stored or used. Unattended rooms should be secured at all times with locked doors as a minimum security requirement.

All documents disclosing identifiable information will be transported in sealed containers e.g. envelopes.

Within their level of authority, staff will be responsible for minimising the risk of theft or vandalism of the data and equipment through common-sense precautions. In particular high value equipment such as, laptop computers, notebooks or mobile phones containing personal or confidential information, should not be left unattended or unsecured and paper records should not be left in public view.

The physical environment in which data and equipment is stored will be suitable and fit for purpose to ensure the safety of the data and equipment.

Logical Security

All computerised information and systems will be regularly backed up to a secure environment.

All computerised information systems will be password controlled and all passwords will be treated with the strictest confidence and users will not divulge their password to any unauthorised person. All sensitive data will be password protected.

Copyright and licences

The Town Clerk is responsible for ensuring all computer software packages and non-electronic media for use within an information environment are used in accordance with the terms and conditions of use as set out in the license agreement.

Disposal and movement of equipment and media

Any media or IT equipment disposed of by the Council will not contain any data or codes that could allow an individual to be identified from it or other confidential information to be accessed. The disposal of equipment will be made under a controlled and documented environment satisfying the requirements of the Data Protection Act 2018 and GDPR.

The disposal of media such as disks and memory sticks must ensure that data cannot be recovered. Disposal of such media through the "everyday" waste collection is not permitted. The Council will implement processes to ensure appropriate disposal of such media.

An inventory of all Council computer equipment will be maintained. Details of any equipment or media disposed of or relocated (other than portable equipment) must be recorded.

Personal Computers

Computer users have responsibility for the security of the equipment in their care and shall not commit any act to compromise the data or Information Security Policy.

Computer users will be made aware of their responsibilities through this policy.

Staff and Councillors' Responsibilities

The Council will make every reasonable effort to ensure that staff and councillors are aware of their responsibilities for the security of information. However, each councillor or member of staff is responsible for ensuring that this Security Policy is adhered to and report any breaches of security.

Incident Reporting

Incidents affecting security must be reported to the Town Clerk as quickly as possible.

Appendix 2. FLITWICK TOWN COUNCIL: DATA BREACH NOTIFICATION POLICY

Aim
Flitwick Town Council is aware of the obligations placed on it by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely.
One such obligation is to report a breach of personal data in certain circumstances and this policy sets out our position on reporting data breaches.

Personal Data Breach
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

The following are examples of data breaches:
a) access by an unauthorised third party;
b) deliberate or accidental action (or inaction) by a data controller or data processor;
c) sending personal data to an incorrect recipient;
d) computing devices containing personal data being lost or stolen;
e) alteration of personal data without permission;
f) loss of availability of personal data.

Breach Detection Measures
The Council has implemented a range of measures to assist it in detecting a personal data breach and will continue to review and refine these.

The Council will ask its IT Support company to make sure all computers and phones are up-to-date, make sure our router is an up-to-date quality model, and the firewall and anti-virus software on each computer is current.

The Council will make regular and documented inspections of physical security of premises, rooms and cabinets and ensure documents with confidential or personal information on not left about.

The Council will require our website host to document what they are doing to detect data breaches (typically hacks) and how they report them to you. The Town Clerk is responsible for this.

Staff are encouraged to regularly check for errors which may result in a data breach and report them to the Town Clerk or DPCO.

The Council will regularly check security monitoring systems should flag up personal data breaches.

Staff will be trained to look for to look for:
- Unusual behaviour from anyone using a system
- Unauthorised insiders trying to access servers and files.
- Anomalies in outbound network traffic.
- Traffic sent to or from unknown locations.
- Excessive consumption.
- Changes in configuration.
- Hidden files.
- Unexpected changes.

Investigation in to suspected breach
In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. All staff are instructed to contact the DPCO immediately a data breach is identified or suspected. This investigation will be carried out by the Data Protection Compliance Officer or other person agreed by the Town Clerk and DPCO, who will make a decision over the severity of risk:

Low Risk: Risk needs to be entered in Breach Register only.

Medium Risk: Breach is required to be notified to the Information Commissioner.

High Risk: Breach will need to be notified to the individual(s) and the ICO

Record of Breaches

The Town Clerk or other nominated officer records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

When a breach will be notified to the Information Commissioner

In accordance with the GDPR, we will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified:

i) a description of the nature of the personal data breach including, where possible:

ii) the categories and approximate number of individuals concerned; and

iii) the categories and approximate number of personal data records concerned.

iv) Contact details of the DPCO.

v) a description of the likely consequences of the personal data breach; and

vi) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

When a breach will be notified to the individual.

In accordance with the GDPR, we will undertake to notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and maybe dependent on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals:

i) a description of the nature of the breach

ii) the name and contact details of the Data Protection Compliance Officer.

iii) a description of the likely consequences of the personal data breach, and

iv) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Appendix 3. FLITWICK TOWN COUNCIL: CLOSED CIRCUIT TELEVISION (CCT) POLICY & CODE OF PRACTICE

CCTV POLICY

INTRODUCTION

The purpose of this policy is to regulate the management and use of the closed-circuit television (CCTV) systems operated by Flitwick Town Council. The CCTV systems are owned wholly by the Town Council.

All cameras are monitored from the Town Council Offices which are streamed wirelessly from separate control units held at each secure location.

This CCTV scheme and policy is operated within the Information Commissioner's Code of Practice for CCTV 2008 and Surveillance Camera Code of Practice 2013 published by the Home Office.

OBJECTIVES OF THE CCTV SCHEME

Along with a range of measures, the CCTV system will be used to:

- monitor and assist visitors to certain Town Council premises
- aid safety and security to all vulnerable members of the community
- reduce the fear of crime
- deter crime and criminality
- aid the detection of crime and the prosecution of offenders
- reduce instances of nuisance and vandalism

STATEMENT OF INTENT

- The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements of the Data Protection Act and the Commissioner's Code of Practice, as well as the Surveillance Camera Codes of Practice 2013 & 2019 published by the Home Office.

- Flitwick Town Council will treat as data all CCTV recordings and relevant information.

- Cameras will be used to monitor activities within the Council and its recreation grounds in line with the objectives of the scheme.

- Static cameras are set as to not focus on private homes, gardens and other areas of private property.

- Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained in writing for directed surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

- Materials or knowledge secured as a result of CCTV will not be released to the media, or used for any commercial purpose, or for the purpose of entertainment. Recordings will only be released under the written authority from the Police, or in respect of a subject access request.

- The planning and design have endeavoured to ensure that the scheme will give maximum effectiveness and efficiency. It is not possible, however, to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

- Warning signs, as required by the Code of Practice of the Information Commissioner will be placed at all access routes to areas covered by the Council's CCTV.

OPERATION OF THE SYSTEM

- The system will be administered by the Town Clerk and other Council staff, in accordance with the principles and objectives expressed in the code.

- The CCTV system will be in operation 24 hours each day, for every day of the year.

- Systems will be checked on a weekly basis to ensure that the system is operating effectively and in particular that the equipment is properly recording and that cameras are functional. The system will be regularly serviced and maintained. Defects will be reported to the servicing company at the earliest convenient opportunity.

CONTROL OF SOFTWARE & ACCESS TO THE SYSTEM

- Access to the CCTV software will be strictly limited to authorised operators with a password.

- Operators must satisfy themselves that all persons viewing CCTV material will have a right to do so.

- The main control facilities will be kept secure.

- Other administrative functions will include controlling and maintaining downloaded digital materials, and maintenance and system access logs.

MONITORING PROCEDURES

- Images from these cameras will be shared with Bedfordshire Police. Access to monitors must be restricted to staff where those areas being monitored are not in public view.

- If covert surveillance is planned or has taken place, copies of the Authorisation Forms, including any Review, must be completed and retained.

DIGITAL IMAGES: PROCEDURES

- Live and recorded materials may be viewed by authorised operators investigating an incident.

- Recorded material may be downloaded from the system in line with the objectives of the scheme.

- Images (stills and footage) may be viewed by the Police for the detection or investigation of crime.

- A record will be maintained of the release of images to the Police or other authorised applicants. A register will be available for this purpose.

- Viewing of images by the Police must be recorded in writing and in the log book. Requests by the Police are allowable under section 29 of the Data Protection Act (DPA) 1998.

- Should images be required as evidence, a digital copy may be released to the Police.

- The Police may require the Council to retain images for possible use as evidence in the future. Such images will be securely stored until they are needed by the Police.

- Applications received from outside bodies to view or release images will be referred to the Town Clerk. In these circumstances, images will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee may be charged appropriate for subject access requests.
- Retention: Images will be retained for only as long as these are required. The system will automatically delete all recordings held on the main control unit after approximately one month.

BREACHES OF THE CODE (including breaches of security)

- Any breach of the CCTV Code of Practice will be investigated by the Town Clerk/ DCPO, in order for him/her to take any appropriate disciplinary action.

COMPLAINTS

- Any complaints about the CCTV system should be addressed to the Town Clerk.

SUBJECT ACCESS AND FREEDOM OF INFORMATION

- The Data Protection Act (DPA) & GDPR provide Data Subjects with a right to data held about themselves, including those obtained by CCTV
- Requests for Data Subject Access should be made in writing to the Town Clerk
- A request for Subject Access will be charged at £10, which is the maximum allowable under the DPA
- A request under the Freedom of Information Act 2000 will be accepted, where such a request is appropriate

CCTV Code of Practice

Introduction and Accountability

Flitwick Town Council has a limited closed-circuit television (CCTV) surveillance system for the purposes of the prevention and detection of crime and the safety and welfare of staff and premises users. The system is owned by Flitwick Town Council and images from the system are strictly controlled and monitored by authorised personnel.

In line with the Home Office 12-point code of conduct the use of the system will:

- always be for the purpose specified which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
- take into account its effect on individuals and their privacy
- have as much transparency as possible, including a published contact point for access to information and complaints
- have clear responsibility and accountability for all surveillance activities including images and information collected, held and used
- have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them
- have no more images and information stored than that which is strictly required
- restrict access to retained images and information with clear rules on who can gain access
- consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
- be subject to appropriate security measures to safeguard against unauthorised access and use
- have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with.
- be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value, when used in pursuit of a legitimate aim.
- be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes.

Operation

- The Town Clerk is responsible for the operation of the CCTV system and for ensuring compliance with this policy. Operations will be delegated to other members of staff. Any concerns in respect of the system's use or regarding compliance with this policy should be addressed to the Town Clerk.

Location

- This code of conduct applies to all CCTV systems operated by the Town Council. Currently CCTV is present at the Millennium Park and the Rufus Centre. It will also encompass all other CCTV images that, in due course, are added to the system, or obtained from CCTV systems operated by which the Town Council have access to.
- The system is operational, and images are capable of being monitored for 24 hours a day throughout the whole year.
- Images captured on camera will be recorded and are held in secure locations. Although every effort has been made in the planning and design of the CCTV system to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.
- For the purposes of the Data Protection Act 2018, the Data Controller is The Flitwick Town Council and the Council is legally responsible for the management and maintenance of the CCTV system. It may however be a Data Processor for images obtained from other images.
- No unauthorised access to the system is allowed at any time. Normal access is strictly limited to authorised staff only. Bedfordshire Police may in future monitor cameras under a separate Memorandum of Understanding.
- In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to access the CCTV system.
- Before granting access to the CCTV system, controllers must satisfy themselves of the identity of any visitor and ensure that the visitor has the appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include their name, department or the organisation they represent, the person who granted authorisation for their visit (if applicable) and the start and finish times of their access to the CCTV system.
- It is recognised that the images obtained comprise personal data and are subject to the law on Data Protection. All copies will be handled in accordance with the procedures
- Recorded images will only be reviewed with the authority of the Town Clerk. Copies of digital images will only be made for the purposes of crime detection, evidence in relation to matters affecting safety, evidence for prosecutions, or where otherwise required by law.
- All staff involved in the operation of the CCTV system will, by training and access to this Policy, be made aware of the sensitivity of handling CCTV images and recordings.
- The Town Clerk will ensure that all staff are fully briefed and trained in respect of all functions; operational and administrative, arising within the CCTV control operation. Training in the requirements of the Data Protection Act and this policy will also be provided.

Recordings

- The system is supported by digital recording facilities which will function throughout operations in real time. As the images are recorded digitally, the process of identifying retrieval dates and times will be computerised. Images will be cleared automatically after a set time.
- Unless required for evidential purposes or for the investigation of crime, recorded images will be retained for no longer than 30 days from the date of recording. However, the Town Council recognises that, in accordance with the requirements of the Data Protection Act, no images should be retained for longer than is necessary. Accordingly, some recorded images may be erased after a shorter period, for example where it can be determined more quickly that there has

been no incident giving rise to the need to retain the recorded images. Digital images will be automatically erased after a set period, which will be no longer than 30 days.

- In the event of the digitally recorded image being required for evidence or the investigation of crime it will be retained for a period of time until it is no longer required for evidential purposes or any investigation into a crime has been completed.

Digital Recording and Access Procedures

- All disks containing images to remain the property of the Town Council.
- Requests by persons for viewing or copying of disks or obtaining digital recordings will be usually be made by prior authority of the Police.
- Requests from the Police will arise in a number of ways, including:
    - requests for a review of recordings in order to trace incidents that have been reported
    - immediate action relating to live incidents, e.g. immediate pursuit
    - for major incidents that occur when images may have been recorded continuously
    - individual Police Officers seeking to review recorded images
- It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes. Users of CCTV will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images. These aspects of the policy reflect Data Protection Principles of the Data Protection Act 2018.
- All requests for access or disclosure will be recorded. The Town Clerk will make decisions on access to recorded images by persons other than Police Officers. Requests by the Police for access to images will not normally be denied and can be made without the above authority, provided they are accompanied by a written request signed by a Police Officer who must indicate that the images are required for the purposes of a specific crime enquiry.
- If access or disclosure is denied, the reasons will be documented.
- If access to or disclosure of the images is allowed, then the following will be documented:
    - the date and time at which access was allowed or the date on which disclosure was made
    - the reason for allowing access or disclosure
    - the extent of the information to which access was allowed or which was disclosed

Photographs and hard copy prints

- Photographs and hard copy prints taken from digital images are subject to the same controls and principles of Data Protection as other data collected. They will be treated in the same way as digital images.
- At the end of their useful life all computer disks, still photographs and hard copy prints will be disposed of as confidential waste.
- This code of practice will be reviewed regularly to assess its implementation and effectiveness and it will be promoted and implemented throughout the Council.

Appendix 4. FLITWICK TOWN COUNCIL: SUBJECT ACCESS POLICY

Introduction

This policy was adopted by the Town Council in order to comply with the requirements of the General Data Protection Regulations (GDPR) and Data Protection Act 2018. Data subjects have the right to access personal data held on them by the Council. Details are set out in the Privacy Notice on the Council's website.

This policy is in place to ensure that internal procedures on handling of Subject Access Requests (SARs) are accurate and complied with and includes:

- Responsibilities (who, what)
- Timing
- Changes to data
- Handling requests for rectification, erasure or restriction of processing.

The Council will ensure that personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered. The Council has implemented standards on responding to SARs.

Upon receipt of a SAR

- The data subject will be informed who at the Council to contact, the Town Clerk.
- The identity of the data subject will be verified and if needed, any further evidence on the identity of the data subject may be requested.
- The access request will be verified, to ensure it is sufficiently substantiated and it is clear to the data controller what personal data is requested. If necessary, additional information will be requested.
- Requests will be verified as to them being unfounded or excessive (in particular because of their repetitive character); if so, the Council may refuse to act on the request or charge a reasonable fee.
- Receipt of the SAR will be promptly acknowledged, and the data subject will be informed of any costs involved in the processing of the SAR.
- Whether the Council processes the data requested will be verified. If the Council does not process any data, the data subject will be informed accordingly. At all times the internal SAR policy will be followed, and progress may be monitored.
- Data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned may be permitted.
- The data requested will be verified to establish if it involves data on other data subjects. This data will be filtered before the requested data is supplied to the data subject; if data cannot be filtered, other data subjects will be contacted to give consent to the supply of their data as part of the SAR.

Responding to a SAR

The Council will respond to a SAR within one month after receipt of the request:

- If more time is needed to respond to complex requests, an extension of another two months is permissible, and this will be communicated to the data subject in a timely manner within the first month;
- If the council cannot provide the information requested, it will inform the data subject on this decision without delay and at the latest within one month of receipt of the request.
- If a SAR is submitted in electronic form, any personal data will be preferably provided by electronic means as well.
- If data on the data subject is processed, the Council will ensure as a minimum the following information in the SAR response:
  - the purposes of the processing;
  - the categories of personal data concerned;
  - the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses

- where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with the Information Commissioners Office (“ICO”);

- If the data has not been collected from the data subject: the source of such data;
- The existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Provide a copy of the personal data undergoing processing.