Stratfield Mortimer Parish Council Data Protection and Information Technology Policy

Introduction

1 This is the Data Protection and Information Technology Policy of Stratfield Mortimer Parish Council and adopts the definitions in the Council's Policy Guidance and Glossary.

2 The Council provides access to information technology ("IT") to enable Officers and Members (together, "Users") to perform their duties efficiently and securely.

3 The Council also operates systems that collect and/or capture data from Users, other organisations and members of the public (together "Subjects"), and this Policy also addresses how such data is collected, processed and stored, how long it should be retained for, and how it can be accessed.

4 This Policy sets out:

4.1 the Council's expectations for the proper use of IT;

4.2 how the Council will protect data and systems;

4.3 how the Council will store records and calculate retention periods;

4.4 how the Council will operate its CCTV system;

4.5 the responsibilities of Users; and

4.6 the rights of Subjects and how they can seek to access personal information held about them.

5 The aims of this Policy are to:

5.1 ensure that IT and data are used effectively and lawfully;

5.2 protect the Council's data, reputation, and assets;

5.3 set clear standards of acceptable and unacceptable use; and

5.4 set out the consequences of misuse.

Scope of Policy

6 This Policy covers all forms:

6.1 of IT provided by the Council, and/or used/accessed by Users in relation to their duties, including hardware, software, services, and supporting infrastructure used to manage and/or process data;

6.2 of data held by the Council.

Responsibilities

7 Overall responsibility for this Policy rests with the Clerk, who is the Council's IT and Data Protection lead.

8 The Clerk will:

8.1 seek to ensure that Users understand and comply with this Policy;

8.2 ensure that Subjects' access rights are protected and addressed;

8.3 propose necessary amendments to this Policy;

8.4 liaise with any external IT support provider as applicable.

Appendices – Protocols and Notices

9 This Policy contains a number of Protocols, Notices, etc, annexed to this Policy as appendices:

- Appendix 1 - Data Protection Protocol and Privacy Notice;
- Appendix 2 - IT Use Protocol;
- Appendix 3a - Record Retention Protocol;
- Appendix 3b - Table of Record Retention Periods;
- Appendix 4a - CCTV Protocol;
- Appendix 4b - CCTV Privacy Impact Assessment;
- Appendix 5 - Application form for accessing personal information.

Appendix 1 – Data Protection Protocol and Privacy Notice

Data Protection

1 All Users must handle personal data in accordance with this Policy, the Data Protection Legislation, and the six Data Protection Principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality.

2 Council data must not be shared or disclosed to unauthorised persons and must be disposed of securely when no longer required and/or in accordance with the Record Retention Protocol.

Data Protection Protocol and Privacy Notice

3 The Data Controller for Stratfield Mortimer Parish Council is the Council itself.

4 The Council is committed to:

4.1 protecting the personal data it holds in line with the provisions of the Data Protection Legislation; and

4.2 holding personal data securely and for the minimum period necessary.

Data Held/Potentially Held

5 The Council holds details of Councillors, updated following elections or other changes, used for advising Councillors of meetings and other administrative business, paying expenses, and passing on correspondence from residents and enquirers.

6 Some information about Councillors is available on the Website.

7 There is a statutory requirement to publicise a Register of Interests, and to hold a Register of Gifts for Councillors - this information is collected from Councillors and kept updated, and is accessible via the Website.

8 The Council holds employment details, including salary and pension information for all its current Officers, and for past Officers as required. This information is held and retained under statutory provisions and in accordance with statutory timescales.

9 The Council operates a service whereby individuals may sign up to receive communications via email from the council (bulletins and/or general information depending upon what the individual chooses to receive). The names and email addresses of such individuals will be held solely for the purpose in question and deleted upon a request from that individual or their authorised representative.

10 The Council may at times hold contact details for organisations or individuals working with, providing services for, or contracted to, the Council, hiring assets from the Council, or attending Council events. This information will be held solely for the purpose in question, although certain contact details may need to be retained for financial accounting or contractual purposes in accordance with statutory timescales (normally six years from the relevant year of audit).

11 The Council may retain correspondence with speakers, donors, residents, enquirers and other individuals who contact, or are contacted by, the Council in connection with the Council's statutory role. Such correspondence will only be retained for the working life of the information and, in general, not beyond a year. Correspondents should be aware that correspondence may be shared, where appropriate, with Councillors, or advisory parties such as the Berkshire Association of Local Councils and its consultants, or staff within West Berkshire Council.

12 The Council holds contact details for individuals with regards to the Council's cemetery, burial and cremation records. This information will be retained for at least the duration of any Exclusive Right of Interment, and sometimes longer, depending on the circumstances of/demands on the cemetery.

13 The Council may process data in the form of photographs.

14 The Council may hold data in relation to Community Speedwatch. The data will be held for processing purposes only and deleted as soon as uploaded to the Community Speedwatch portal.

15 The Council uses CCTV (see CCTV Protocol).

16 Where minutes and reports, or other similar documents contain personal information, such information is retained for archival purposes as part of the formal records of the Council (see Record Retention Protocol).

17 A separate Privacy Notice regarding the personal data obtained when individuals access the Website can be found at https://www.stratfield-mortimer.gov.uk/website/privacy.

Rights of Individuals

18 Individuals have the right to ask to see the information the Council holds about them, and may object about how their personal information is used, or ask that such personal information is deleted.

19 Any enquiries regarding personal data held by the Council should be made to the Clerk in accordance with Appendix 5 to this Policy.

Appendix 2 – IT Use Protocol

Website

1 The Council's Website shall comply with the relevant Web Content Accessibility Guidelines.

Email and Electronic Communication

2 The Clerk will be supplied with a generic email address (the.clerk@stratfield-mortimer.gov.uk) to ensure data ownership and governance compliance.

3 As set out in the Communications Protocol to the Code of Conduct, *"Councillors and Officers will be provided with a Council Microsoft 365 account and password, including a Council email address (firstname.surname@stratfield-mortimer.gov.uk) which they are required to use in relation to email Communications*".

4 All email correspondence must be professional, accurate, and appropriate for Council business.

5 Emails are subject to disclosure under Freedom of Information and the Data Protection Legislation (see relevant Protocols).

6 Attachments containing personal data must be encrypted or password-protected.

7 Users must not forward chain emails, spam, or offensive material.

Internet Usage

8 Internet access is provided for legitimate Council business.

9 Officers' personal browsing during work hours should be minimal and restricted to break times.

10 Council systems must not be used:

10.1 to access, download, or distribute material that is offensive, illegal, discriminatory, or unrelated to Council business;

10.2 for political activity, gambling, or commercial gain.

11 The Council's firewall and security settings must not be disabled or bypassed.

Software and Licensing

12 Only software approved and licensed by the Council may be installed on Council systems, and copyright and licensing conditions must be respected at all times.

Computer Use and Security

13 Whenever they are in a public place, Users must lock or log off their devices when leaving them unattended.

14 Computers should be shut down at the end of each working day.

15 Council data should be saved to approved cloud storage (eg Microsoft SharePoint) to ensure backup and recovery.

16 Equipment must be protected from public access or interference during meetings and events.

17 Only authorised software may be installed.

Personal Devices (Bring Your Own Device)

18 Officers may only use personal devices for Council business with the prior agreement of the Clerk.

19 Members may use personal devices for Council business subject to the requirements in this Protocol.

20 Personal devices used for Council business must have password protection and encryption enabled.

21 Any personal device used for Council business must be capable of remote data deletion if lost or stolen.

Access Codes and Security

22 Any User using an electronic device or computer for any business relating to the Council shall ensure that anti-virus, anti-spyware and firewall software with automatic updates, together with a high level of security, is used.

23 Access Codes must be kept confidential and never shared except with the Clerk (or the Council Chairman in the Clerk's absence) for business continuity.

24 Passwords must contain at least eight characters and should include a mix of letters, numbers and symbols.

25 Access Codes should be stored in a secure password store or the like, and must be so stored except for:

25.1 any Access Code used by a Bank Signatory to access a Bank Portal using a personal electronic device or computer;

25.2 any Access Code used by a User to access Council emails or systems using a personal electronic device or computer.

26 The password to any secure password store used by Officers shall be placed in an identifiable sealed dated envelope and:

26.1 the envelope shall be handed to, and retained securely, by the Council Chairman; and

26.2 the envelope may only be opened by the Council Chairman in the presence of two other Councillors; in which case:

26.2.1 the relevant Access Code(s) shall be changed as soon as practicable; and

26.2.2 the circumstances leading to the envelope needing to be opened shall be reported to F&GP.

27 If an Access Code is suspected to be compromised, it must be changed immediately and reported to the Clerk.

28 Regular back-up copies of the records on any computer shall be made and shall be stored securely away from the computer in question, and preferably off site.

Training and Awareness

29 The Council will provide induction training on IT security and data protection to all new Officers.

30 Refresher training will be provided as required, particularly when systems or regulations change.

Monitoring and Privacy

31 The Council reserves the right to monitor use of its IT systems for legitimate business purposes, including compliance, security, and performance.

32 Monitoring will be proportionate and consistent with the Data Protection Legislation.

33 If personal use of Council systems is permitted (for example, checking personal email during breaks) that use must comply with this Policy and may be monitored.

Misuse and Disciplinary Action

34 Breaches of this Policy may result in disciplinary action under the Council's Disciplinary Policy - examples include:

34.1 accessing inappropriate websites or material;

34.2 sharing passwords or confidential data;

34.3 attempting to bypass system security;

34.4 installing unauthorised software;

34.5 using IT systems to harass, bully, or abuse others;

34.6 leaving devices unsecured in public places.

35 Serious breaches may be treated as gross misconduct.

Appendix 3a – Record Retention Protocol

Purpose

1 The Council requires a wide variety of records for transacting its business and is committed to retaining such records in a format, and for such periods of time, that enable it to (at least) meet its statutory obligations in respect of records.

2 In addition, this Protocol seeks to:

- ensure the security of records;
- protect personal details and confidential data;
- facilitate legitimate access to information;
- optimise the use of storage space;
- manage the associated costs of record retention; and
- facilitate the destruction of redundant records.

3 The Appendix sets out the minimum retention periods for different records.

Scope

4 This Protocol applies to the Council's records - physical and electronic.

5 This Protocol, and the retention of records, is subject to the overarching requirements of the Data Protection Legislation (eg in relation to the right for individuals to have certain personal data erased).

6 Electronic records will be subject to the same rules of retention and security as physical records unless otherwise stated.

7 Copies of Council records held by Members are not subject to a minimum retention period, but must be destroyed in accordance with the Disposal Part below:

- where required by the Data Legislation;
- when no longer required; or
- at the end of the Member's term of office.

8 The Clerk is responsible for the implementation of the Protocol.

9 Records subject to a statutory period of retention are identified by their associated legislation in Appendix 3b.

Storage

10 Records that are required to be retained in a physical format (contracts, leases, deeds, etc) shall be copied to an electronic format before being stored in accordance with Appendix 3b.

11 Other physical records may be copied to an electronic format and then destroyed if that is the most convenient way of storing them.

Security

12 Physical records containing personal and/or sensitive information will be kept in lockable storage.

13 Electronic records shall be stored on media which is password protected (see IT Use Protocol).

Disposal

14 Redundant records may be destroyed in order to reduce the cost of storage, indexing and handling.

15 Physical records containing personal and/or confidential information will be cross shredded and disposed of as confidential waste.

16 Other physical records will be shredded or recycled as appropriate.

17 Electronic records containing personal and confidential information will be securely deleted.

18 Prior to disposing of computer hardware, memories and data storage will be fully wiped.

Appendix 3b - Table of Record Retention Periods

Category	Record	Minimum Retention Period	Processing Purpose
ADMINISTRATION	Annual Parish Award	Three years	Management
	Applications to Council	Six months from date of application	Management
	Complaints: No resulting policy change Resulting in a policy change	 Three years from last action Five years from last action	Legal obligation
	Consultation Results	Five years from exercise	Consent
	Correspondence & emails - general	Until no longer required	Management
	Correspondence & emails - other	At least six years, then until no longer required	Limitation Act 1980 / Management
	Councillor email accounts	One year following end of term of office	Management
	Historical Information	Indefinite	Historical purposes
	Information from other bodies	Until no longer required	Management
	Newsletters	Indefinite	Interest
	Parish Plans/NDP – final copy	Indefinite	Management & historical purposes
	Planning documents	Until no longer required	Information is held by Planning Authority
	Policies/Procedures	Until revised copy is available	Management & Audit
	Register of Electors	Until no longer required	Management
	Risk Assessments	Until reviewed and updated	Management
	Speed Watch Data	As soon as uploaded to the Community SpeedWatch portal	Management
AUDIT AND FINANCE	Asset Register	Indefinite	Management & Audit

	Bank Paying-in Book	Last completed audit year	Audit
	Bank Statements	Last completed audit year	Audit
	Cheque Book Stubbs	Last completed audit year	Audit
	Hire Forms	Six years	Audit/VAT
	Internal/External Audit Report and Returns	Indefinite	Legal
	Lettings diaries	Six years	Audit/VAT
	Paid invoices	Six years from when the relevant accounts are submitted.	Audit/VAT
	Receipt and Payment Accounts	Indefinite	
	Scale of fees/charges	Six years from when the relevant accounts are submitted.	Audit/VAT
	VAT Records	Six years from when the relevant accounts are submitted, but 20 years for VAT on rents	Audit/VAT
BURIAL GROUNDS	Register of: Burials Purchased Graves Register/plan of grave spaces Memorials Applications for internment Applications for right to erect memorials Disposal certificates Copy certificates of grant of exclusive right of burial	Indefinite	Archives, Local Authorities Cemeteries Order 1977
COMMITTEES	Agendas	Once finished with	Management – no current obligation
	Meeting Papers	Once finished with Six years/until no longer needed	Management

	Meeting Recordings	Until minutes have been approved	No current obligation
	Minutes - approved	Indefinite Six years	Statutory No current obligation
	Minutes - draft	Until minutes have been approved	Management
PERSONNEL	Recruitment records for unsuccessful candidates	Six months after candidate has been notified	Equality Act 2010
	Staff employment records	Duration of Employment plus seven years	Contract
	Staff leave and absence	Two years after action completed	Contract and management
	Staff pension records	Six years from date of last pension payment	Legal/Audit
	Staff payroll records	Six years from when the relevant accounts are submitted	Tax/Audit
	Time sheets	Three years	Audit Personal Injury Limitation Act 1980
PURCHASE MANAGEMENT	Contracts	Six years after contract expired 12 years for contracts under seal	Limitation Act 1980
	Quotations and tenders	Successful: six years after contract expired Unsuccessful: one year	Limitation Act 1980 / Management
STATUTORY and LEGAL	Accident/Incident Report	21 years	Management
	CCTV	30 days unless retained in accordance with CCTV Policy (eg relating to investigation)	Data Protection Act 2018
	Certificate of Employers Liability	40 years from date on which insurance commenced or was renewed	Employers' Liability (Compulsory Insurance) Regulations 1998
	Declaration of Term of Office	Six years	Legal – Members are required to sign

	Deeds	Indefinite	Audit and management
	Freedom of Information Requests	Three years	Legal
	Insurance policies but see below	Seven years after the term of the policy has expired	Legal
	Insurance policy numbers and company names	Indefinite	Management
	Insurance claim	Seven years after all obligations/entitlements are concluded (allowing for the claimant to reach 25 years of age)	Legal
	Leases	12 years	Limitation Act 1980
	Risk Assessments	Whilst valid	Insurance
	Register of Members Interest	Six years	Legal
	Playground equipment inspection reports	Duration of life of equipment plus six years	Limitation Act 1980

Appendix 4a – CCTV Protocol

Introduction

1 The Council:

1.1 has installed a ~~A~~ CCTV (closed circuit television) system ("the System") ~~has been installed~~ on Mortimer Fairground; and

1.2 owns further CCTV devices which it may, from time to time, deploy within the Parish.

2 All such CCTV equipment ("CCTV Equipment") is operated by the Council with the primary purpose of reducing the threat of crime generally and/or~~,~~ protecting Council premises and helping to ensure the safety of users, the general public and staff, in all cases consistent with the respect for the individual's privacy.

3 In operating the CCTV Equipment the Council will comply with:

3.1 the Surveillance Camera Code of Practice (Home Office, November 2021) and/or any update thereof;

~~4~~3.2 any guidance issued by the ICO.

~~2~~4 This Policy includes processes for individuals and organisations to request or be provided with access to data (see Appendix 5) and a Data Privacy Impact Statement (see Appendix 4b).

Processing of personal data

~~3~~5 The lawful basis for processing an individual's personal data is that of a legitimate interest:

~~3.1~~5.1 where processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;

~~3.2~~5.2 under the Data Protection Legislation, where the Council is permitted to use an individual's information because it has a legitimate interest in securing its premises and reducing complaints against Officers;

~~3.3~~5.3 where, if CCTV captures more sensitive information about individuals, the processing is necessary for reasons of substantial public interest, for the prevention or detection of unlawful acts, and/or to carry out a key function as set out in law (s.163, Criminal Justice and Public Order Act 1994).

The System

~~4~~6 The System comprises four deployable cameras located on two poles above the tennis court westside fence at The Fairground, The Street, Mortimer, RG7 3RD. Camera images are not monitored but are recorded and access is only available to limited individuals. Images are captured 24 hours a day, seven days a week, and are kept securely on encrypted cloud-based storage. If images are downloaded, they are stored on password-protected Council systems.

~~5~~7 Signs are prominently placed at strategic points to inform members of the public that the System is in use.

Formatted: c2, No bullets or numbering

Formatted: c2, No bullets or numbering

~~6~~8 Although every effort has been made to guarantee the effectiveness of the System, it is not possible to guarantee that the System will detect every incident taking place within the area of coverage.

~~7 The Council has followed the CCTV guidelines produced by theICO.~~

Purposes

~~8~~9 The CCTV Equipment ~~System~~ will be used for all or any of the following purposes:

- to create a safer community;
- to reduce the fear of crime;
- to reduce the vandalism of property;
- to prevent, deter and detect crime and disorder;
- to gather evidence by a fair and accountable method;
- to assist the council, and the police and other law enforcement agencies with the identification, detection, apprehension, and prosecution of offenders, by examining and using retrievable evidence relating to crime, public order or contravention of the law;
- to deter potential offenders by publicly displaying the existence of CCTV: having cameras clearly sited that are not hidden and signs on display;
- to assist the emergency services to carry out their lawful duties.

Access to images

~~9~~10 Access to images will be restricted to those that need to have access in accordance with the purposes of the CCTV Equipment~~System~~. Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the CCTV Equipment~~System~~ and is limited to the following:

- police and other law enforcement agencies where the images recorded could assist in a specific criminal enquiry and / or the prevention of terrorism and disorder;
- prosecution and safeguarding agencies;
- relevant legal representatives;
- individuals whose images have been recorded and retained (unless disclosure would prejudice criminal enquiries);
- parents/appropriate adults connected to an incident under review and involving someone aged under 18.

~~10~~11 All requests for disclosure should be documented. If disclosure is denied, the reason should be recorded.

Retention

~~11~~12 All footage can be exported if needed to be retained for as part of an investigation.

13 Otherwise:

13.1 ~~,~~ stored images on the System are retained for 30 days - this allows sufficient time and chance to come back to an event that has occurred~~;~~

~~12~~13.2 stored images captured on CCTV Equipment other than the System are overwritten as the storage media becomes full, but are in any event checked and wiped on a regular basis (as the equipment is re-charged); and

~~13~~13.3 CCTV footage is not backed up so, unless exported, it will be overwritten by more recent coverage.

Formatted: c2, No bullets or numbering

Individuals' access rights

14 The Data Protection Legislation give individuals the right to access personal information about themselves, including CCTV images:

14.1 subject to certain exemptions, individuals have a right to be told whether any personal data is held about them;

14.2 they also have a right to a copy of that information in a permanent form, except where the supply of such a copy is not possible or would involve disproportionate effort, or if they agree otherwise - the Council will only give that information if it is satisfied as to the individual's identity;

14.3 if the information would disclose information relating to (an)other individual(s) who can be identified from that information, the Council is not obliged to comply with an access request unless:

- the other individual has consented to the disclosure of information; or
- it is reasonable in all the circumstances to comply with the request without the consent of the other individual(s).

15 An application form for accessing personal information is at Appendix 5.

The Council's rights

16 The Council may deny access to information where the Act allows - the main exemptions relate to information held on the System are where the information may be held for the prevention and detection of crime or the apprehension and prosecution of offenders, and the release of the data would potentially prejudice those purposes.

Data Privacy Impact Assessment

17 The Council's CCTV Data Privacy Impact Assessment ("DPIA") is at Appendix 4b.

18 The purpose of a DPIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. It is recommended in The Surveillance Camera Code of Practice, issued by the Surveillance Camera Commissioner in June 2013 in accordance with s.30(1)(a), Protection of Freedom Act 2012, ("the Code").

19 The Code provides guidance, including 12 guiding principles, on the appropriate use of surveillance camera systems by local authorities and the police.

20 Guidance is based on the ICO's DPIA Handbook, and the four areas highlighted by the ICO as potential areas for loss of privacy in relation to personal data are:

- the privacy of personal information;

- the privacy of the person;
- the privacy of personal behaviour; and
- the privacy of personal communications.

21 'Personal data', as defined by s1 of the 2018 Act, means data which relates to a living individual who can be identified from:

21.1 that data; or

21.2 that data and other information, which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

DPIA - Responsible Person contact details

22 The person qualified to respond to questions regarding the Council's DPIA is the Clerk to the Council, Stratfield Mortimer Parish Council, 27 Victoria Road, Mortimer, Reading, RG7 3SH (the.clerk@stratfield-mortimer.gov.uk).

Appendix 4b – CCTV Privacy Impact Assessment

1	**Why a Privacy Impact Assessment is Required**	
1.1	What is the aim of the surveillance system?	Providing Stratfield Mortimer Parish Council and Thames Valley Police with evidence to take criminal and civil action in the Courts.
		Reducing the fear of crime and providing reassurance to the public.
		Aiding in the detection and prevention of crime (including countering terrorism).
		Assisting with the maintenance of public order.
		Deterring or reducing the incidence of vandalism, graffiti, and other environmental crime.
		Deterring persons from committing crimes and to enhance the opportunities for detecting those who do.
		Improving the safety and security of residents, visitors, and the business community.
		Discouraging anti-social behaviour including alcohol and drug-related elements.
1.2	Who takes legal responsibility under the Data Protection Act?	Stratfield Mortimer Parish Council is the Data Controller at the point of images being recorded. However if any images are released to any of the authorised organisations, then the legal responsibility will be transferred to that organisation in relation to the images that have been released.
1.3	What organisations will have access to CCTV images?	Stratfield Mortimer Parish Council will be the main user of the CCTV system.
		However, Thames Valley Police, other Police Forces and other agencies such as Fire and Rescue Service will be granted access to images from the system if a legitimate request is received.
1.4	What are the benefits to be gained from the system and who will benefit?	Residents, visitors, and businesses will benefit from improved public safety, and reductions in crime.
		CCTV is a proven tool in detecting crimes, and the perpetrators of it. Using CCTV can significantly reduce the time and cost on the Police service in investigating allegations.
		It is known that false allegations are made, and CCTV is also useful in disproving some allegations.

		CCTV captures actual events and is not influenced by interpretation, or events, as seen by people who are under the influence of alcohol or drugs.
1.5	Can CCTV realistically deliver these benefits?	Yes, and consistently so.
2	**Information Flow**	
2.1	How is information collected?	The system captures video pictures, which are transmitted from cameras positioned on the Fairground, Stratfield Mortimer.
		The transmissions are received via Parish Council hardware. Access is via a web link and log in/password. The cameras are equipped with pan, tilt and zoom facilities.
2.2	Where are the real-time images from the camera displayed?	Real-time images will be accessed and displayed via Parish Council hardware.
		Third parties can be granted access to the images via the web link and log in/password, but it is not envisaged that this will be used.
2.3	Who has operational access and ability to move the CCTV camera?	Stratfield Mortimer Parish Council Clerk.
		Thames Valley Police can access live video streams and use of cameras under the Regulation of Investigatory Powers Act. This is controlled by the Parish Council Clerk.
2.4	How are the images recorded?	Each camera signal will be continuously recorded by way of a Digital Video Recorder.
2.5	Where are the recorded images stored?	On hard drives in a locked cabinet.
2.6	How is information used?	Information is used to monitor public safety and prevent and detect crimes.
		Evidence is provided for investigation and enforcement.
		Individuals can request copies of CCTV data which contains their personal information.
		Disclosure of data is covered by internal processes which are fully compliant with relevant legislation and codes of practice.
2.7	How is access gained to the recorded images?	Password controls are in place on the system. Hard copy requests for images will be required.
2.8	How long are the images retained?	30 days on the system. Images from an 'incident' may be stored for longer.

2.9	How is information deleted?	The data management system will automatically delete information after 30 days
2.10	When data is downloaded, or copied for release to a third party how is information recorded?	Memory stick or secure, encrypted cloud-based exchange.
2.11	What processes are in place to ensure that data protection responsibilities are understood by persons receiving the data?	Each request for data by the public must be requested via a signed data release form.
3	**Data Protection Act**	
3.1	Can less privacy intrusive solutions achieve the same objectives?	CCTV is a good solution to achieve the objects set out in 1.1.
3.2	Are images of identifiable individuals required or could the scheme use other technology not capable of identifying individuals?	The system must be capable of identifying individuals, as footage from the system could be used in both criminal and civil court cases.
		If the system did not have this capability, it would not be fit for purpose.
3.3	Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?	The service will remain a 24-hour service for the foreseeable future.
3.4	What future demands may arise for wider use of images and how will you address these?	The benefits of additional cameras will be considered as and when required.
3.5	What are the views of those under surveillance?	The general feeling is that people who are not involved in crime are happy to be in an area that is monitored by CCTV cameras. There are some members of society both law abiding and those who are not, who have issues with being in areas covered by CCTV cameras. By abiding with current legislation, the aim is to show that the CCTV system is only used for crime reduction/ detection purposes and those activities that assist the public.
4	**Human Rights Act**	
4.1	Is the system established on a proper legal basis and operated in accordance with the law?	The system has been established on a proper and legal basis to comply with the Data Protection Act, Human Rights Act and Regulations of Investigatory Powers Act.
4.2	What could we do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?	Regular reviews of camera performance shall be undertaken to justify their need.

4.3	Is CCTV justified in the circumstances?	Yes. Violence, theft, and anti-social behaviour are key areas to address which in turn will reduce the fear of crime thereby creating a safer environment.
4.4	Is it proportionate to the problem that it is designed to deal with?	Yes. CCTV is used to detect crime and complies with the current legislation.
5	**Surveillance Code of Practice**	
5.1	Do you regularly review the system against its objectives?	Yes.
5.2	Is the system being used for any other purpose other than those specified?	No.
5.3	Does signage exist highlighting the use of surveillance cameras?	Signage is installed.
5.4	Does the signage highlight the point of contact?	Signage highlights the point of contact.
5.5	Are all staff aware of their responsibilities?	Yes.
5.6	Can a member of the public request footage?	The procedure for a Data Subject Access Request forms a Protocol to the Council's Data Protection and Information Technology Policy ("the Policy"). CCTV footage can only be supplied for 30 days from the date and time of an incident, after which time the images are automatically overwritten.
6	**Risks**	
6.1	Is the data shared with other organisations?	Yes, for investigation and enforcement.
6.2	Is the system operated in full compliance with: DPA requirements; ICO codes of practice; SCC codes of practice; and Human Rights Act?	Yes.
6.3	Do you have procedures in place to manage risks associated with the use of CCTV cameras	Yes – see the Policy.
7	**Privacy Solutions**	
7.1	Have you identified solutions to address any risks?	As set out in the Policy, the system is operated in line with relevant identified legislation and codes of practice.

Appendix 5 - Application form for accessing personal information

REQUEST FOR ACCESS TO DATA

SECTION 1 - About You

The information requested below is to help us (a) satisfy ourselves as to your identity and (b) find any data held about you.

PLEASE USE BLOCK LETTERS

Title *(tick as appropriate)*	**Mr**		**Mrs**		**Miss**		**Ms**	
Other Title (*Dr, Rev, etc)*								
Surname								
First Name(s)								
Address								
Postcode								
Tel								

SECTION 2 - Proof of Identity

Please provide (or produce to the Parish Office for inspection) two official documents (or certified copies) that, between them, clearly show (a) photo proof of your ID (eg passport or driving licence), and (b) proof of your current address (eg recent bank statement or utility bill).

SECTION 3 - Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form – do you wish to (please delete as necessary):

- View the information and receive a permanent copy [Yes] / [No]
- Only view the information [Yes] / [No]

SECTION 4 - Details

To assist us in finding the information please complete the following:

Request to access CCTV

I am (please tick or complete):

A person reporting an offence or incident	
A witness to an offence or incident	
A victim of an offence	
A person accused or convicted of an offence	
Other – please explain:	

Details of the incident:

Date(s) and time(s) of incident	
Place incident happened	
Brief details of incident:	

Request to access data other than CCTV

Please provide full details of your request, including any names/phrases you wish searched:

Relevant date(s)	
Relevant phrase(s)	
Brief details of/reasons for request:	

SECTION 5 - Declaration

The information I have supplied in this application is correct and I am the person to whom it relates.

Signed: _____ Date: _____

Warning: a person who impersonates or attempts to do so may be guilty of an offence

SECTION 6 - Submission

When you have completed, checked, signed and dated this form, please send or deliver it, together with the required identification documents/certified copies to: **Stratfield Mortimer Parish Council, 27 Victoria Road, Mortimer, RG7 3SH**.

If you have any queries regarding this form, or your application, or any complaint or enquiry about the day-to-day operation of the system please email the.clerk@stratfield-mortimer.gov.uk.

Document control

Version	Date	Editor	Changes	Approved	
				On	By
0.1	21/10/2025	D Davies	Initial draft		
0.2	03/12/2025	G Bridgman	Edit to include various previous policies as protocols		
0.2	08/01/2026		Reviewed by F&GP		
0.3	09/01/2026	G Bridgman	Edit to CCTV Protocol following F&GP		