GDPR, data, privacy and CCTV policy
December 2024

VERSION CONTROL:

Version ID	Description of Change	Version Sponsor	Policy Owner	Version creation date	Version Approval Date	Next Review Date
1.0	Policy creation (consolidate previous policies)	Adam Killeya, Parish Clerk	Policy & Resources Committee	15/08/24	09/12/2024	September 2027

A Purpose of policy
This policy brings together the council's responsibilities and duties under the General Data Protection Regulation, the Protections of Freedoms Act 2012, and other relevant legislation concerning data and privacy. It outlines how the council will ensure that personal data is processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security. It also outlines the council approach to the use of CCTV; and within its appendices contains the council's privacy notice, public access notice, and data retention statement.

The handling of information is a risk to the council, both financially and reputationally. A breach of regulations or legislation could result in the council facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Such risk can be minimised by maintaining appropriate policies and practices, undertaking an information audit, minimising who holds data protected information, and undertaking training in data protection awareness.

B Roles and responsibilities
GDPR requires continued care by everyone within the council, councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically. This includes the approach use and securing of data, the protection of passwords, the avoidance on inappropriate discussion of data etc.

The Clerk has the responsibility to "manage and respond to Freedom of Information and General Data Protection Requirements" in line with their job description. They shall undertake periodic information audits, manage the information collected by the council, deal with requests, complaints and data breaches, and oversee the safe disposal of information. They shall also ensure that the risks associated with data are included in the council's risk management register.

The Clerk will lead the internal investigation of any breaches; reporting to the Information Commissioners Office within 3 days where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, they will also notify those concerned directly.

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

C Rights under GDPR
Individuals' Rights: GDPR gives individuals rights, with some enhancements to those rights already in place:

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

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

If a request is received to delete information, then the DPO must respond to this request within a month. The DPO has the delegated authority from the Council to delete information. If a request is considered to be manifestly unfounded then the request could be refused.The Parish Council will be informed of such requests.

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

D CCTV

1 Introduction: the council recognises the particular relevance of CCTV to policies around data and privacy. The benefits of CCTV for the prevention and detection of crime must be balanced against an individual's rights of privacy, and unwarranted and excessive use of surveillance technologies has contributed a tougher regulatory landscape. This section is therefore designed to address both the powers and obligations of the Council, and the legislation protecting the rights of individuals, in order to ensure that the Council's use of CCTV and other surveillance technologies is lawful, safe, and reasonable.

2 Powers: the power for a parish council to install CCTV and other surveillance equipment is conferred under Local Government and Rating Act 1997 s.31:

The Council also has a duty to consider crime and disorder implications of their functions, under the Crime and Disorder Act 1998 s.17:

Under Article 8 of the European Charter on Human Rights (enshrined in Human Rights Act 1998 Sch.1), an individual has the *qualified* right to respect for private and family life. These rights are protected through the Protection of Freedoms Act 2012 s.33. The Policy Statement below further addresses the best practice set out in the surveillance camera code.

3 Scope: The purpose of this policy is to enshrine within the Council's practices the amended surveillance camera code of practice 2022, which updates the 2013 code. Under the Protection of Freedoms Act the council is under a duty to have regard to this code when, in exercising any of its functions, it considers that the future deployment or continued deployment of overt surveillance camera systems to observe public places may be appropriate. This will help to ensure that the council meets its statutory obligations, and to ensure that individuals and the wider community have confidence that surveillance cameras are deployed to protect and support them rather than spy on them. This policy also requires the council to consider any new or updated guidance or codes that may be issued in the future.

This policy covers CCTV owned and operated by Burnham Parish Council. *CCTV.* The Council operates systems of CCTV cameras at Burnham Park Hall, the George Pitcher Memorial Ground. and on Footpath 57. It is considering adopting further provision in High Street, and in other areas of Burnham as appropriate and proportionate for the prevention and detection of crime and antisocial behaviour.

In addition, the following may be relevant:

a) New systems of CCTV may be operated by another provider, such as Buckinghamshire Council, and in this instance the council shall satisfy itself that they have appropriate processes and procedures in place.

b) Community Speed-watch. In the past the Council has operated this scheme, which includes the use of a mobile traffic camera for the capture of images of cars exceeding the speed limit, and may do so again. Where the equipment is joint-owned with neighbouring parish councils, and this policy shall not cover the use of the equipment by any of these councils.

c) The Council also employs a contractor for parking enforcement who makes use of ANPR technology; and in appointing such contractors the council shall satisfy itself that they have appropriate processes and procedures in place.

d) The Council may on occasion request to access cameras owned by others, for example to investigate damage to council property. In this instance the council shall act in accordance with the rules and principles contained within this policy.

The Council also operates Motor Vehicle Activated Signs (MAVS) but these do not record individual data and therefore are not covered by this policy.

The following people and organisations are covered by this policy:

a) *Data controller* and *data owner* – meaning Burnham Parish Council.
b) *System manager* – meaning the Parish Clerk.
c) *System user* – meaning such councillors, officers, volunteers, or other individuals authorised to use the surveillance equipment.
d) *Data subject* – meaning any such individual whose personal information is captured by the surveillance equipmen.

4. Principles of operation: In accordance with the *Surveillance Camera Code of Practice 2013* the Council has adopted the following 12 principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
The purposes of the systems listed are for "*the prevention and detection of crime and antisocial behaviour, including traffic offenses, with the civil parish of Burnham*" or *"for the appropriate monitoring and enforcement of parking restrictions and charges".* The systems shall not be used for any other purpose, and there shall be a prohibition on the monitoring of the lawful movements of any individual.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
There are varying and subjective expectations of privacy, and the Council shall not:
a) deploy surveillance camera systems in public places where there is a high expectation of privacy, including toilets and changing rooms;
b) use any forms of audio recording in a public place, other than for the recording of Council and committee meetings
c) use any form of facial recognition or other biometric characteristic recognition system.
The Council shall also undertake a privacy impact assessment for any new form of surveillance it wishes to undertake, and shall regularly review such assessments alongside this policy.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
The Council shall ensure that sufficient signage is in place in all areas covered by any surveillance system, and that this full policy, complaints policy, and other relevant documents are published on its website.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
The *Data Controller* and *Data Owner* shall have overall ownership for the surveillance systems in place, with the *System Manager* having responsibility for ensuring that proper governance arrangements are in place, and ensuring that such arrangements are communicated to and adhered to by any *system users*.

5. Clear rules, policies and procedures must be in place before a surveillancecamera system is used, and these must be communicated to all who need to comply with them.
The *System Manager* will ensure that all system users are aware of the contents of this policy and have sufficient training to safely and securely use the equipment.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
As a default, all images captured shall be deleted without review, unless the *system manager* is satisfied beforehand that there is a legitimate reason, under Principle 1, for it

being accessed and viewed.

a) *CCTV.* Images are stored for up to 30 days, following which they are automatically overwritten.
b) *Community Speedwatch.* Images of cars, including their number plates, are stored during each exercise. The images are then used to extract the number plate for entry into the Police National Computer, following which the images are deleted. Where storage devices are used by other parish councils, any information shall be deleted on return of the device.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

Access to all images by any permitted users is solely for the purposes set out in Principle 1 above. Access to stored images is restricted to the *System Manager*, and other *system users* as follows:

(a) Burnham Park Hall CCTV: Clerk, General Manager, Assistant Manager (no current post), Bookings Supervisor:
(b) Footpath 57 CCTV. Clerk, Deputy or Assistant Clerk
(c) George Pitcher Memorial Ground: Grounds Team, Clerk, Deputy or Assistant Clerk

The Clerk, as system manager, may designated other officers as necessary and proportionate for the above and for any other use of CCTV.

Where footage is extracted for the purposes of passing this to a third party (e.g. the Police or a school for the identification of an offender) the Council shall ensure that this complies with any data protection legislation, and any stipulations in its Data Retention Statement and Privacy Policy. The Council shall also take reasonable steps to ensure the third party has in place practices and procedures to comply with data protection regulations. Where another third party, such as a person whose property has been damaged, requests the disclosure of images, such requests will be approached with care and in accordance with the Human Rights Act 1998, and with a view to the guidance set out in para. 4.7.4-4.7.6 of the *Surveillance Camera Code of Practice 2013*.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

The *System Manager* shall ensure that all CCTV follows the latest standards for the operation and management of CCTV, and that all surveillance equipment meets any such additional standards as made available by the Surveillance Camera Commissioner or their successors.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

The *System Manager* shall follow the guidance as outlined the latest codes of practice.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

The *Data Controller* shall review this policy and privacy impact assessments, along with the number and positioning of all surveillance cameras, in line with the latest code of practice.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then 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.

The *Data Controller* shall ensure that the quality and positioning of any surveillance equipment is such so as to achieve the highest quality and most useful images. Where

images are to be used for law enforcement and criminal proceedings, the Council will ensure that there is an audit trail of all images used, and that such images are available in a readily exportable format without the loss of forensic integrity.

12. ***Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date****.*

This may include the use of automatic number plate recognition (ANPR) or facial recognition systems. However, as stated in 2(c), the Council will not use facial and biometric recognition technology. In addition, the Council does not have, nor does it have any intention of using, a reference database for the purposes of matching data captured from its surveillance systems.

Appendix A: Privacy Notice

Please read our privacy notice carefully as it describes our collection, use, disclosure, retention, and protection of your personal information. This notice applies to the use of any of our services, facilities, website, or other online platform which references this privacy policy. Where you provide us with your personal information in any of the ways described in paragraph 2 below, you agree that we may use it as described in this privacy policy.

1. **Who we are**

The work of Burnham Parish Council includes the management of facilities including parks, playgrounds, green spaces, public toilets, community hall, street furniture, as well as the provision of services for the benefit of the residents and other service users in Burnham. Our work, and this privacy policy, encompasses all our commercial activity including the hiring and hosting of events at *Burnham Park Hall* (also referred to as *Burnham Park*), and the hiring of our green spaces including the *George Pitcher Memorial Ground* (also referred to as the *Cherry Orchard*). This privacy policy includes our websites: www.burnhamparish.gov.uk and www.burnhampark.co.uk and their associated email addresses.

2. **How we collect information**

We will collect information about you and any other party whose details you provide to us when you:

- register to use or attend any of our facilities or services. This may include your name, address, email address, and telephone number. We may also ask you to provide additional information about your preferences;
- place an order using our websites, or third party booking website such as www.eventbrite.co.uk or www.ticketsource.co.uk;
- complete online forms, take part in surveys either using our or a third-party survey website such as www.surveymonkey.co.uk, sign up to newsletters hosted through www.wix.com, post on our message boards, post any blogs, or participate in any other interactive areas that appear on our website or within our facilities;
- interact with us using social media;
- contact us offline, for example by telephone, SMS, email or post.

3. **Cookies**

To make this site simpler, we sometimes place small data files on your computer. These are known as cookies. They improve things by:

- remembering settings, so you don't have to keep re-entering them whenever you visit a new page;
- remembering information you've given so you don't need to keep entering it;
- measuring how you use the website so we can make sure it meets your needs;

Our cookies aren't used to identify you personally. They're just here to make the site work better for you. Indeed, you can manage and/or delete these small files as you wish. To learn more about cookies and how to manage them, visit AboutCookies.org.

We use Google Analytics to collect information about how people use this site. We do this to make sure it's meeting its users' needs and to understand how we could do it better. Google Analytics stores information about what pages you visit, how long you are on the site, how you got here and what you click on. We do not collect or store your personal information (e.g. your name or address) so this information cannot be used to identify who you are. We do not allow Google to use or share our analytics data.

If you intend giving us personal information about someone else, you must ensure that beforehand you have their explicit consent to do so and that you explain to them how we collect, use, disclose, and retain their personal information or direct them to read our privacy notice.

4. **How we use your information**

You agree that we may use your information to:

- provide any information and services that you have requested or ordered;
- compare information for accuracy and to verify it with third parties;
- manage and administer your use of services you have asked us to provide;
- manage our relationship with you (for example, providing you with information on similar services or issues of public or personal interest);
- monitor, measure, improve, and protect our content, website, and services;
- provide you with any information that we are required to send you to comply with our regulatory or legal obligations;
- detect, prevent, investigate, or remediate crime, illegal or prohibited activities, or to otherwise protect our legal rights (including liaison with regulators and law enforcement agencies for these purposes);
- contact you to see if you would like to take part in our community engagement activities (for example, feedback on our facilities or public services);
- deliver joint content and services with third parties which whom you have a separate relationship (for example, other local authority);

After our initial interaction has concluded (i.e. your booking of our facilities has finished, or we have concluded a query), we may retain information about you. This information will be held and used for as long as permitted for legal, regulatory, fraud prevention, and legitimate public interest or commercial purposes.

We may monitor and record our communications with you, including emails and phone conversations. Information which we collect may then be used for training purposes, quality assurance, to record details about our website and services you request from us or ask us about, and in order to meet our legal and regulatory obligations generally.

5. **Sharing your information**

We may share your information with:

- Any local authority or agency acting in the public interest, for the purposes set out in this privacy policy, (e.g. to successfully resolve a issue with one of our facilities or services, or those of another local council);
- third parties used to facilitate payment transactions, for example our bank, or credit card payment provider;
- third parties where you have a relationship with that third party and you have consented to us sending information (for example social media sites);
- fraud prevention agencies;
- law enforcement agencies so that they may detect or prevent crime or prosecute offenders;
- any third party in the context of actual or threatened legal proceedings, provided we can do so lawfully (for example in response to a court order);
- any third party in order to meet our legal and regulatory obligations, including statutory or regulatory reporting or the detection or prevention of unlawful acts;
- external professional advisors and auditors for the purpose of seeking professional advice or to meet our audit responsibilities;

6. **Your information**

If we hold any information about you which is incorrect or if there are any changes to your details please let us know so that we can keep our records accurate and up to date.

You can also contact us if you would like to update your records or see a copy of the information that we hold about you. If you request a copy of your information you will need to pay the applicable statutory fee.

If you withdraw your consent to the use or of your personal information for purposes set out in our privacy notice, we may not be able to provide you with access to all or parts of our website, facilities, or services.

To contact us about any of the above, contact the Parish Clerk on 01628 661381 / clerk@burnhamparish.gov.uk.

7. **Changes to our privacy notice**

We may change our privacy policy from time to time. We will always update the privacy notice on our website, so please try to read it when you visit the website (the 'last updated' reference tells you when we last updated our privacy policy).

8. **Security and storage of information**

We will keep your information secure by taking appropriate technical and organisational measures against its unauthorised or unlawful processing and against its accidental loss, destruction, or damage. We will do our best to protect your personal information but we cannot guarantee the security of your data which is transmitted to our website or to other website, applications, and services via an internet or similar connection. If you believe your account has been compromised, please contact us at the details above.

9. **Other sites and social media**

If you follow a link from our website, or social media platforms to another site or service, this notice will no longer apply. We are not responsible for the information handling practices of third party sites or services and we encourage you to read the privacy policies appearing on those sites or services.

Appendix B: subject access notice
Burnham Parish Council takes your data privacy seriously.

If you wish to find out what information Burnham Parish Council holds about you, please contact us providing your contact details, a brief description of the information you require and enclose proof of your identity. This could be a scanned copy of a household bill plus a photocopy of your passport or driving licence.

To help you and to ensure confidentiality, we ask for any request to be made:

- In writing; to the Clerk at Burnham Park Hall / clerk@burnhamparish.ogv.uk
- With sufficient information to locate the data requested.
- With sufficient evidence to confirm your identity as stated above.

In response to a subject access request individuals are entitled to a copy of the information held about them, both on computer and as part of a relevant filing system. They also have the right to receive a description of why their information is processed, anyone it may be disclosed to, and any information available to you about the source of the data
Burnham Parish Council will respond to requests as quickly as possible. This must be no later than one calendar month, starting from the day we receive the request. If we need something from you to be able to deal with your request (eg ID documents), the time limit will begin once we have received this.

If your request is complex or you make more than one, the response time may be a maximum of three calendar months, starting from the day of receipt.

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

If at any time you feel that we have failed to meet these standards, then please either contact us or make a complaint direct to the Information Commissioner using their website www.ico.org.uk/concern

Appendix C: Data Retention Policy

1. Introduction

The purpose of this statement is to ensure that particular documents (or sets of documents) are dealt with in the correct manner; being retained and disposed of in the correct method and timescale.

This statement gives the Council a system for the management of paper and electronic records. The Parish Clerk is responsible for ensuring all Council documents are managed accordingly.

This policy is based on the National Association of Local Council's Legal Topic Note on Local Council's Documents and Records (LTN 40), to ensure it meets the legal requirements and recommended practice within the sector.

Where the policy refers to 'documents' this includes both paper and electronic copies.

2. Retention of Documents

Certain important documents must be retained for clear reasons such as audit purposes, staff management, tax liabilities, and the eventuality of legal disputes and legal proceedings. Appendix A shows the appropriate document retention periods.

Subject to the above reasons for retaining documents, papers and records will be destroyed if they are no longer of use, relevant, or, in the case of personal information, would breach the rights of the individual under the Data Protection Act 2018 or be contrary to the Council's Privacy Policy. If there is any doubt, the document will be retained until proper advice has been sought.

3. Retention of documents for legal purposes

Most legal proceedings are governed by the Limitation Act 1980 (as amended). This Act provides that legal claims may not be commenced after a specified period. The specified period varies, depending on the type of claim in question. The table below sets out the limitation periods for the different categories of claim.

Category	**Limitation Period**
Negligence and other torts	6 years
Defamation	1 year
Contract	6 years
Leases	12 years
Sums recoverable by statute	6 years
Personal injury	3 years
To recover land	12 years
Rent	6 years
Breach of trust	None

It should be noted that some limitation periods can be extended. Examples include:

- Where individuals do not become aware of damage until a later date
- Where damage is hidden
- Where a person is a child or suffers from a mental incapacity
- Where there has been a mistake by both parties
- Where one party has defrauded another or concealed facts

Where the limitation periods above are longer than other periods specified in this policy, the documentation should be kept for the longer period specified. Some types of legal proceedings may fall within two or more categories; in this instance, the longer period will be observed.

In such circumstances the Parish Clerk will consider the costs of storing relevant documents and the risks of:

- Claims being made
- The value of any such claims
- The inability to defend any such claims should documentation be destroyed

4. Disposal

All Council documents will be handled in the correct manner for their sensitivity. Any document held by the Council offices which contain confidential information will be disposed of by shredding in the Council offices. For large amounts of confidential information, this may be done through a confidential waste disposal service.

Councillors are responsible for ensuring that any confidential Council documentation in their possession is held securely and disposed of in accordance with this statement, either by themselves or by returning the documents to the Council offices. On ceasing to hold their office, councillors must ensure that all documents in their possession are returned to the Council offices.

In an effort to maintain the organisation and efficiency of the workplace and reduce the volume of printing, officers are committed to printing only those documents necessary to have in hard copy, and disposing of those which are not necessary to be kept.

5. Responsibility

The Parish Clerk holds responsibility for ensuring all Council employees are aware of and adhering to the Document Retention Statement, in particular the retention of the documents at Appendix A to the statement.

Document retention periods

Document	Minimum Retention Period	Reason
Minutes and reports	Indefinite	Archive
Scales of fees and charges	6 years	Management
Income and expenditure accounts	Indefinite	Archive
Receipt books of all kinds	6 years	VAT
Bank statements	Last completed audit year	Audit
Bank paying-in books	Last completed audit year	Audit
Cheque book stubs	Last completed audit year	Audit
Quotations and tenders	6 years	Limitation Act 1980
Paid invoices	6 years	VAT
Paid cheques	6 years	Limitation Act 1980
VAT records	6 years (20 years for VAT on rents)	VAT
Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980
Timesheets	3 years	Personal injury
Wages book	12 years	Superannuation
Insurance policies	While valid	Management
Employer Liability Certificates	40 years	Employer's Liability Regulations 1998
Investments	Indefinite	Audit, Management
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management
Personal data of employees	6 years after employment terminates	Recommended practice
Recruitment paperwork	1 year for all except successful candidate	Recommended practice
Accident books/reports	3 years (21 years for children)	RIDDOR
Formal complaints	6 years	Management
FoI / subject access requests received	6 years	Management
Hall, pitch and other booking information	6 years	VAT

Any other items not specified: in general 1 year, unless authorised by the Clerk