REPORT OF	Head of Legal and Governance & Monitoring Officer
To:	Full Council
Subject:	Adoption of CCTV Policy
Date:	30th October 2023 **Reference:**

PURPOSE OF REPORT:
To seek approval for adoption of the attached CCTV Policy

1. INTRODUCTION

The Council has various CCTV cameras operating across our sites.

Whilst CCTV is a helpful technology it is also critical that we consider Data Protection Law and ensure that we are compliant in this regard both in the way that we use our systems and, have processes in place when it comes to requests for the footage, and how people can access the footage.

We must show to the public that the Council takes data protection seriously, and how we hold and treat their personal information, which can, in some instances include footage of them captured on CCTV.

By adopting a CCTV policy, we can show staff, councillors and the public that we take our data protection obligations seriously and are transparent.

2. REPORT

The key concepts in data protection law are transparency, fairness, and proportionality. However, the ability to record can be helpful in certain situations such as to protect the public and our staff.

The Policy sets out the fundamental principles such as :-

a) Who the policy applies to;
b) Who is responsible for overseeing the policy;
c) The Council's reasoning for using CCTV;
d) The locations of our CCTV;
e) Retention and erasure of CCTV; and
f) How requests for disclosure can be made

3. IMPLICATIONS

Legal Implications

Failure to have a CCTV policy could put us in breach of Data Protection Law. It makes it clear to our staff, and to the public howe we will hold the data, the reasoning for using CCTV and when we will disclose CCTV footage.

Financial Implications

No financial implications of adopting a CCTV policy, although being in breach of Data Protection Law could put us at risk of non-compliance and subject to action being taken against us together with the imposition of financial penalties for non-compliance.

Human Resources Implications

N/A

Sustainability/Biodiversity Implications

N/A

Equality/Diversity

None directly applicable to this report.

Risk Management

The Council is required to comply with Data Protection Law, and failure to do so could lead to both reputational risk and financial penalties if we do not comply.

Compliance with Policies and Strategies

This complies with our Data Protection Polic.

Data Protection (GDPR) Implications

The Council take Data Protection seriously. Having a policy in place is critical to ensure that the public have assurance that we treat their data with care. Having a policy in place will also give clear guidance to staff as to the limited instances when we will disclose CCTV footage, and ensures we are compliant with Data Protection legislation.

Climate Change

None directly applicable to this report

Ward Member and Lead Member Views

Date of Consultation - 20th October 2023

Cllr Simon Newton, Lead Member for Legal and Democratic Support:

4. CONCLUSIONS

It is necessary for the Council to have a CCTV Policy in place for transparency, fairness and proportionality reasons and to be compliant with Data Protection Legilsation. It is also necessary to have clear protocols in place for Council staff.

5. RECOMMENDATIONS

That Members recommend the adoption of the CCTV Policy.

SUPPORTING INFORMATION

Consultations:	Officers Consulted Senior Management Team Operational Management Team CCTV Team Lance Wrey (Estates) Simon Hoare (Estates) Rachel Gulwell (Estates) Matthew Millichope (Community Safety) Ian McIver (Community Safety)
Contact Officer:	Staci Dorey
Background Papers:	CCTV Policy October 2023

CCTV Policy

October 2023

CONTENTS

CLAUSE

1. About this policy

1.1 We use CCTV cameras to view and record individuals on and around our premises in order to maintain a safe environment for staff and visitors. However, we recognise that the images of individuals recorded by CCTV cameras are personal data which must be processed in accordance with data protection legislation. As a controller, we have registered our use of CCTV with the Information Commissioner's Office (**ICO**) and seek to comply with its best practice suggestions.

1.2 The purpose of this policy is to:

(a) outline why and how we will use CCTV, and how we will process data recorded by CCTV cameras;

(b) ensure that the legal rights of staff, and the public, relating to their personal data, are recognised and respected;

(c) assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence; and

(d) explain how to make a subject access request in respect of personal data created by CCTV.

1.3 This policy has been agreed by Full Council

1.4 This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time subject to agreement by Full Council.

1.5 A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

2. Who does this policy apply to?

2.1 This policy applies to all employees, officers, councillors, consultants, self-employed contractors, casual workers, agency workers, volunteers and apprentices. It also applies to anyone visiting our premises or using our vehicles.

3. Who is responsible for this policy?

3.1 The Senior Management Team has overall responsibility for the effective operation of this policy. The Senior Management Team has delegated responsibility for overseeing its implementation to the Public Health and Community Safety Manager and/or The Head of Legal and Governance (DPO).

3.2 Any questions you may have about the day-to-day application of this policy should be referred to your line manager or the Public Health and Community Safety Manager or The Head of Legal and Governance in the first instance.

3.3 This policy is reviewed annually by the Head of Legal and Governance. We will also review the ongoing use of existing CCTV cameras at least every 12 months to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

4. Definitions

4.1 For the purposes of this policy, the following terms have the following meanings:

CCTV : means fixed and domed cameras designed to capture and record images of individuals and property.

Controllers: are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. We are the controller of all personal data used in our business for our own commercial purposes.

Data: is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data subjects: means all living individuals about whom we hold personal information as a result of the operation of our CCTV (or other surveillance systems).

Data users: are those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy.

Personal data: means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

Processing: is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

Processors: are any person or organisation that is not a data user (or other employee of a controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

Surveillance systems: means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

5. Reasons for the use of CCTV

5.1 We currently use CCTV around our sites as outlined below. We believe that such use is necessary for legitimate business purposes, including:

(a) to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;

(b) for the personal safety of staff, visitors and other members of the public and to act as a deterrent against crime;

(c) to support law enforcement bodies in the prevention, detection and prosecution of crime;

(d) to assist in day-to-day management, including ensuring the health and safety of staff and others;

(e) to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;

(f) to assist in the defence of any civil litigation, including employment tribunal proceedings;

This list is not exhaustive and other purposes may be or become relevant.

6. Monitoring

6.1 CCTV monitors the exterior of the buildings [and both the main entrance and secondary exits]] at the following sites:-

a) Riverbank House, Bideford, Devon, EX39 2QG;

b) Town Hall, Bridge Street, Bideford, Devon, EX39 2HT;

c) Middledock, Appledore, Newquay Street;

d) Appledore Fishdock, Hubbastone Road, Appledore, EX39 1LZ;

e) Cattlemarket Carpark;

f) Caddsdown Business Support Centre, Bideford, EX39 3DX;

g) Barton House Hostel, Barton Tors, Bideford, EX39 4EZ;

h) 26 High Street, Bideford , EX39 2AR

i) Tamar Units, Holsworthy;

j) Torrington Pannier Market, The Square, Torrington, EX38 8HE;

k) Cromlech House;

l) Westcome Dept, Westcombe Lane, Bideford, Devon;

m) 8 Cooper Street, Bideford, Devon (Part of town CCTV system)

n) Victoria Park Nurseries, Bideford, Devon;

o) Bideford Skate Park

p) Sully House

6.2 The Cameras are in use 24 hours a day and this data is continuously recorded.

6.3 Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property.

6.4 Images are monitored by authorised personnel

6.5 Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

7. How we will operate any CCTV

7.1 Where CCTV cameras are placed in the workplace, we will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. The signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

7.2 Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety.

7.3 We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters. Recorded images will only be viewed in designated, secure offices.

8. Use of data gathered by CCTV

8.1 In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

8.2 Given the large amount of data generated by surveillance systems, we may store video footage using a cloud computing system. We will take all reasonable steps to ensure that any cloud service provider maintains the security of our information, in accordance with industry standards.

9. Retention and erasure of data gathered by CCTV

9.1 Data recorded by the CCTV system will be stored digitally using a cloud computing system. Data from CCTV cameras will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. [In all other cases, recorded images will be kept for no longer than 30 days.

9.2 At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

10. Use of additional surveillance systems

10.1 Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a data protection impact assessment (**DPIA**).

10.2 A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

10.3 Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

10.4 No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

11. Covert monitoring

11.1 We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

11.2 In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of The Chief Executive or in his absence The Head of Legal and Governance . The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers/public will always be a primary consideration in reaching any such decision.

11.3 Only limited numbers of people will be involved in any covert monitoring.

11.4 Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

12. Requests for disclosure

12.1 We may share data with partner agencies/organisations where we consider that this is reasonably necessary for any of the legitimate purposes set out above in paragraph 5.1.

12.2 No images from our CCTV cameras will be disclosed to any other third party, without express permission being given by The Chief Executive or Head of Legal and Governance. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

12.3 In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

12.4 We will maintain a record of all disclosures of CCTV footage.

12.5 No images from CCTV will ever be posted online or disclosed to the media.

13. Subject access requests

13.1 Data subjects may make a request for disclosure of their personal information, and this may include CCTV images (**data subject access request**). A data subject access request is subject to the statutory conditions from time to time in place and should be made in writing, in accordance with our Subject Access Policy which can be found within our Data Protection Policy, available on the intranet from your line manager or from the DPO.

13.2 In order for us to locate relevant footage, any requests for copies of recorded CCTV images must be in writing and include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

13.3 We reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so.

14. Complaints

14.1 If any member of staff has any concerns about our use of CCTV, they should speak to their line manager or the HR Department in the first instance.

14.2 Where this is not appropriate, or matters cannot be resolved informally, employees should use our formal grievance procedure.

15. Requests to prevent processing

15.1 We recognise that, in rare circumstances, individuals may have a legal right to request erasure of personal data concerning them or to restrict the processing of their personal data. Any person who considers that these rights apply to them in relation to our use of CCTV should speak to their line manager or the HR Department in the first instance.