



Data Protection Update

Autumn 2024

CONTENTS	Page
Update regarding the Data Protection and Digital Information Bill	2
ICO feedback – Cybersecurity Issues	2
Access Controls Policy	3
Heritage data	4
CCTV Requests for images from police and others	5
Surveillance/CCTV Data Protection Impact Assessments	6-7
Appendix One – CCTV Images Request Form Template	8-11

Please Note: This update is advisory in nature, informational in content, and is intended to assist the council to improve their standards of compliance with data protection legislation and best practice; it does not constitute legal advice. It has been based on observations and written and oral information provided by the council's representative(s). This report, however, has been prepared on the strict understanding that the council retains ownership of, and remains responsible for, the compliance with data protection in its workplace. Accordingly, JDH Business Services Ltd will not accept liability for any incident or damages of any kind resulting from the use of, or reliance upon, any information contained in the report.

Data Protection Update 2024

1.) Update regarding the Data Protection and Digital Information Bill

The Data Protection and Digital Information Bill was first introduced during the 2022-23 parliamentary session. This bill had passed a number of sessions of the House of Lords so was due to become legislation. However, this bill was not in any “wash up period” to enact laws prior to the dissolution of Parliament in Summer 2024, so this entire Bill is considered ‘failed’ and was not carried over to the new Parliament and Government. I have seen no articles indicating the Bill is a priority to be re-presented by the new Government. Therefore, all the proposed changes of this failed Bill to the FOIA, DPA 2018 and the Privacy and Electronic Communications regulations (PECR) are currently not going to happen.

2.) ICO feedback – Cybersecurity Issues

The ICO has noted that *‘bolstering online security and keeping systems safe is a must as in recent years, cyber-attacks have been one of the most common incidents affecting organisations, and many of the cyber incidents we see come from phishing. That’s what led to the reprimands issued to organisations.’*

The ICO has issued guidance to avoid similar incidents stating that organisations should:

- Ensure all relevant staff receive training in identifying phishing attacks, which is when attackers attempt to trick people into clicking a bad link that will download malware or into revealing people’s username and password. Organisations should consider tailoring the measures in the NCSC Phishing Attack guidance to their own organisation.
- Implement two-factor or multifactor authentication wherever it is possible to do so – to take the most common example, a password and a one-time token generator. This will be even more important for organisations that handle sensitive personal information.
- Determine and communicate security requirements to a supplier and formalise responsibilities within a contract. As part of this, establish how to seek assurances a supplier has implemented appropriate levels of security. The NCSC supply chain security guidance provides practical examples of how to manage security within a

supply chain.

- Make sure that access to personal information is restored in the event of any incidents, such as by establishing an appropriate backup process. Such recovery measures should be reviewed regularly to ensure they're appropriate in large incidents that pose a risk to people through confidentiality, availability or integrity issues.

3.) Access Controls Policy

As noted above, the ICO considers that cyber-attacks have been one of the most common incidents affecting organisations. Therefore, councils should also review access controls and ensure controls are formalised. Formal access controls support the reduction in risks of cybersecurity attacks and other forms of data breach and can also help support compliance with data protection requirements.

Councils should consider formalising access controls into an adopted policy that sets the rules and restrictions that define who can access the council data, systems, and applications, and how they can access them. Therefore, an effective access controls policy will help minimise accidental or unauthorised access to the council systems, networks, drives, applications, electronic folders and electronic information.

Individuals employed by or under contract to the council should be granted access only to information and information systems that are required to fulfil their duties. Therefore, access control protocols will apply to:

- all employees including temporary and agency workers
- members
- third party organisations who require access to the council's information systems and facilities should also be aware of the contents of this policy (eg. accountancy providers, independent consultants)

An access controls policy should not be designed to be obstructive so there should always be an option for staff who consider the current access controls procedures prevents them from carrying out their duties effectively to discuss the issue with the council clerk. However, the decision of levels of access to information must be based on roles and responsibilities, 'need to know' and segregation of duties and roles.

To ensure continuity of council activity, an access controls policy will need to stipulate the procedures for providing access to systems and specific drives/folders where a staff member is off on sickness or other absence, or extended sickness absence, to permit temporary access, allowing essential council business to continue. The policy will also need to cover the removal of access, for instance, when an officer has resigned.

We have provided a generic template for an Access Controls Policy with this data protection update which could be aligned to the council's particular required controls.

4.) Heritage data

We have noted some councils are commencing initiatives to create heritage archives which may include using information from the community such as photographs, pictures, documents, correspondence with the overall aim of preserving the information as a historical archive.

The DPA 2028 contains provisions for archiving in the public interest which affect the application of the rights of the individual and some of the principles. This is enacted in the Data Protection Act 2018, Sch.2, part 6, para.28. It is important to note that ‘Archiving in the public interest’ is processing to secure the permanent availability of recorded memory, in other words, evidence and information, for a wide range of current and potential future purposes, including enabling:

- research and investigation, including academic, historical or genealogical research
- long-term accountability, such as public inquiries and other official investigations like cold case murder investigations
- the discovery and availability of personal, community and corporate identity, memory and history
- the establishment and maintenance of rights and obligations and of precedent decisions
- educational use
- commercial and non-commercial re-use.

Using the ‘archiving purposes in the public interest’ exemption.

It is important to have a clear definition of what the scope of the council’s archiving function and activity is (as distinct from any other corporate purposes of processing), what it seeks to achieve and sufficient documentation of how this activity is performed. Archive services meeting the national accreditation standard will probably already have policy and procedural documents which meet this requirement. Archive services which do not have clear policies committing them to some form of direct or indirect public access to their holdings, now or in the future, will need to demonstrate in what other ways their archival operations meet a public interest, in addition to any private interests.

Some benefits of the ‘archiving in the public interest’ exemption are conditional upon their use being actually necessary and proportionate for the performance of the archiving function, so services will need to be able to demonstrate and document that this is the case.

Exemptions for archiving in the public interest only apply:

- to the extent that complying with the provisions above would prevent or seriously impair the achievement of the purposes for processing;

- if the processing is subject to appropriate safeguards for individuals' rights and freedoms (see Article 89(1) of the GDPR – among other things, you must implement data minimisation measures);
- if the processing is not likely to cause substantial damage or substantial distress to an individual; and
- if the processing is not used for measures or decisions about particular individuals, except for approved medical research.

As transparency is an important aspect of compliance, services should use a range of means to make clear (particularly to people about whom they hold data) that they are 'archiving in the public interest', for example through the council website. Where personal data collected by a council is being archived this should be included in the council privacy notice. You will need to add the new data category to the council retention policy/schedule and data inventory.

Circumstances in which the 'archiving purposes in the public interest' exemption may not be appropriate are as follows:

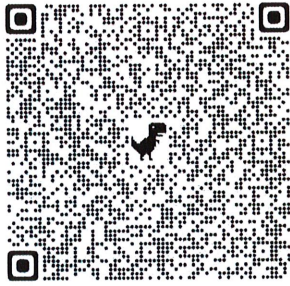
- If the data have been processed to take 'measures or decisions' about the individual,
- there was a clear likelihood that substantial damage/distress would be caused simply by continuing to hold the data
- if the processing was unlawful or unfair

Related data subject rights to have data restricted or rectified (or the broader elements relating to access, portability and objection to processing) are similarly limited by provisions for archiving in the new legislation. However, these provisions apply only to the extent that the archival purpose would be compromised by complying with the request.

5.) CCTV Requests for images from police and others

Sharing information with the Police

This is a permissible reason covered under the DPA 2018 legislation for the prevention or detection of crime or apprehension or prosecution of offenders (DPA 2018 Schedule 2, Part 1, Para 2) (1), (a) & (b)). There is an ICO toolkit that you can apply if you are ever uncertain about the process of sharing data with a law enforcement agency after receiving such a request – please use the QR code to get access to the actual ICO toolkit.



Sharing information with the insurance companies /solicitors

If this relates to a road traffic collision or other incident then an insurance company (or solicitor) could request the footage under Schedule 2, Part 1(5) of the Data Protection Act 2018 ‘Information required to be disclosed by law etc or in connection with legal proceedings’. However, the council should review the requests on a case by case basis, and to help with this you could establish a standard template for the requests of CCTV information by insurers/solicitors which also includes stipulations about the sharing and processing of the data provided. A template CCTV image request form is included in Appendix One.

6.) Surveillance/CCTV Data Protection Impact Assessments

Councils should note that there is a Surveillance Data Protection Impact Assessment template developed jointly by the Surveillance Camera Commissioner (SCC) and the Information Commissioner’s Office (ICO) and there is also associated detailed guidance provided.

Principle 2 of the Surveillance Camera Code of Practice states that the use of a surveillance camera system must take into account its effect on individuals and their privacy.

The Surveillance DPIA Guidance states *‘Processing of personal data using a surveillance camera system will be considered ‘likely to result in high risk to rights and freedoms’ under data protection law. For instance, where it can systematically monitor public spaces on a large scale, or can involve innovative technology or the processing of biometric data. As processing using a surveillance camera system is likely to be high risk you must conduct a DPIA before the system is installed and review it regularly. Carrying out a DPIA means that you can determine whether deployment is lawful, and will also be a record of how you have considered and addressed any risks or wider concerns about your project. This addresses Principle 2 of the Surveillance Camera Code of Practice as well as requirements of data protection law.’*

The DPIA guidance also states there are situations when you must **consider** a DPIA and provides the following examples:

- *When you are introducing a new surveillance camera system.*

- *Before you process any special categories of personal data on a large scale.*
- *If you are considering introducing new or additional technology that may affect individuals' rights and freedoms (e.g. facial recognition technology, automatic number plate recognition (ANPR), audio recording, body worn cameras, unmanned aerial vehicles (drones), megapixel or multi sensor very high-resolution cameras).*
- *If your system involves any form of data matching.*
- *When you are changing the location or field of view of a camera or other such change that may raise privacy concerns.*
- *When you are reviewing your system to ensure that it is still justified. Both the SCC and the ICO recommend that you review your systems regularly, for example as part of annual procedures.*
- *When you change the way you record images and handle, use or disclose information.*
- *When you increase the geographical area captured by your surveillance camera system.*
- *When you change or add an end user or recipient for the recorded information or information derived from it.*

Conclusion

Councils should ensure they are using the latest DPIA template for surveillance/CCTV and applying the joint guidance from the SCC and ICO for both identifying whether processing is high risk and then, if the processing is identified as high risk, completing the detail required in the DPIA template. A copy of both the DPIA template and DPIA guidance has been provided with this data protection update. All assessments by councils as to whether processing is high risk should be clearly documented and retained.

Appendix One

Template Form for requesting access to CCTV images

Please Note the following - The Council must be satisfied that all CCTV requests are genuine and that persons making a request understand their legal obligations in relation to possessing and making use of images recorded on the Council's CCTV system. The requestor should also be clear that copyright of all images remains with the Council and images must not be published or otherwise shown without the specific written permission of the Council. This form is to be used for requesting CCTV data covered by the Data Protection Act 2018, Schedule 2, Part 1, 5(3).

DPA 2018, Schedule 2, Part 1, 5(3)

The listed GDPR provisions do not apply to personal data where disclosure of the data:

(a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights, to the extent that the application of those provisions would prevent the controller from making the disclosure.

Please clearly disclose the Crime Reference / Court Reference/ Claim Reference here:

.....

Please provide the organisation details requested below:

Name	
Address	
Email	
Telephone	

Organisation Name	
-------------------	--

Please provide details of the purpose for which you are requesting this information. Please enter 'yes' or 'no' against each category.

(a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),	
(b) is necessary for the purpose of obtaining legal advice	
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights,	

(PRINT) Name.....

Position.....

Signature of Applicant.....

Date.....

Details of CCTV images requested:

I/we require footage of the camera or cameras that have been recorded for the following location:

Please provide exact details of the location and camera location	

The information I/we require is of footage that was recorded on the following date and time/s:

Enter details of date and any timings that are relevant	Date	Times

In particular I/we are interested in footage that contains the following information:

Enter details of incident or descriptions of persons or vehicles or property.	

In order to assist you in locating the information I/we provide the following supplementary details:

Enter any other relevant information that you feel may assist us to locate the information you have requested.	

1. *Journal of the American Medical Association*, 2000; 283: 2689-2693.

Journal of Management Education 36(7) 809-827

1 0