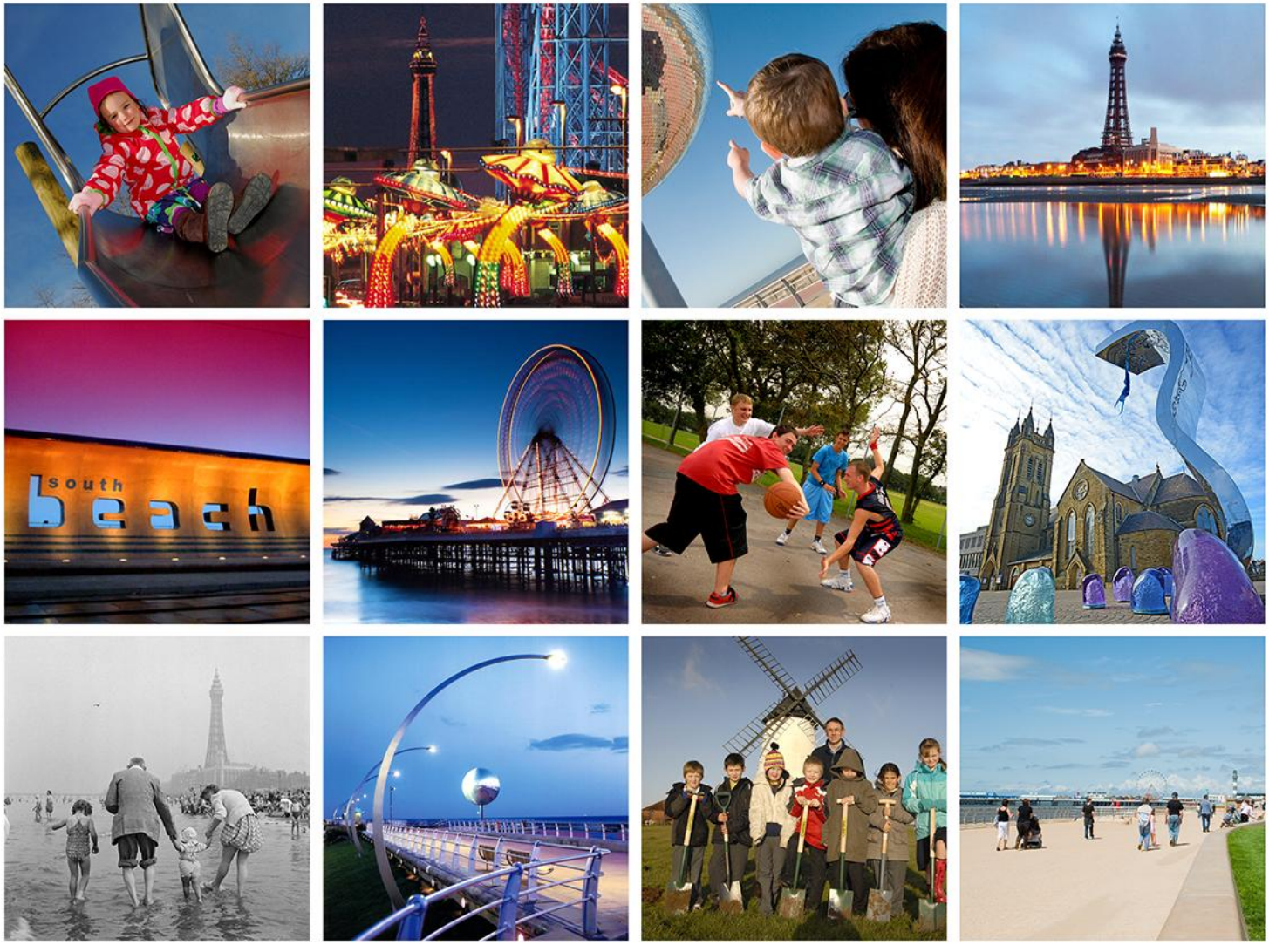
North Western Inshore Fisheries and Conservation Authority (NW IFCA)

Data Protection Audit Report

Audit Date	December 2025
Auditor	Mr Jonathan Pickup, Data Protection Officer
In Attendance	Mark Taylor, Chief Executive Officer Joe Moulton, Head of Enforcement Alison Nicholson, Head of Administration

Blackpool Council



NW IFCA – Data Protection Audit Report

Contents

NW IFCA – Data Protection Audit Report

1. Introduction

1.1 The EU General Data Protection Regulation (GDPR) was implemented in May 2018 for members of the European Union. Following Brexit, the 'UK GDPR' now sits alongside an amended version of the Data Protection Act 2018 as the two primary pieces of data protection legislation in the United Kingdom. The Data (Use and Access) Act 2025, which is currently being implemented, has made slight amendments to the UK GDPR.

1.2 The purpose of this review is to ensure that the Company complies with data protection legislation and best practise provided by the Information Commissioner's Office (ICO), the UK Regulator for data protection and information rights.

1.3 Article 5 of the UK GDPR sets out seven core principles, which all organisations need to comply with:

1. Principle (a) – lawfulness, fairness and transparency
2. Principle (b) – purpose limitation
3. Principle (c) – data minimisation
4. Principle (d) – accuracy
5. Principle (e) – storage limitation
6. Principle (f) – integrity and confidentiality
7. Accountability principle

1.4 Failure to comply with these principles may result in enforcement action being taken against the Company by the ICO. Such enforcement action can include undertakings, audits, prosecution, or monetary penalties. In addition to regulatory action, the GDPR stipulates that any person who has suffered material or non-material damage as a result of an infringement of this Regulation has the right to receive compensation from the controller or processor for the damage suffered.

1.5 The GDPR also provides the following rights for individuals, including visitors and employees.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

1.6 In addition to the primary pieces of data protection legislation, the Privacy and Electronic Communications Regulations (PECR) provide specific privacy rights in relation to marketing. The North Western Inshore Fisheries and Conservation Authority (NW IFCA) is also a public authority for the purposes of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

2. Acknowledgements

2.1 The Data Protection Officer (DPO) would like to thank the Chief Executive Officer, the Head of Enforcement, and the Head of Administration for their contributions to the audit process.

2.2 Please note that, as this is the first formal review, it is likely that a number of recommendations will arise. This should not be seen as a reflection on the organisation's commitment to compliance with data protection legislation.

3. Overview Summary

3.1 This report provides a comprehensive review of the North Western Inshore Fisheries and Conservation Authority's (NW IFCA) data protection compliance, It focuses on governance, individual rights, data security, retention, and data sharing.

3.2 The NW IFCA is correctly registered with the Information Commissioner's Office (ICO) and has appointed Blackpool Council as its Data Protection Officer (DPO). Governance related recommendations include updating the ICO registration with the DPO's details, enhancing the Data Security Policy, and ensuring policy distribution to all staff. The importance of maintaining a comprehensive Record of Processing Activities (RoPA) and regular reviews is highlighted. Consideration is also given to the emerging use of Artificial Intelligence (AI).

3.3 The Authority maintains several privacy notices accessible via its website, covering a range of data processing activities. However, there is a need to ensure these notices are up to date, reflect current practices, and are provided to data subjects at the point of data collection. Additional recommendations include the creation of workforce privacy notices and formalising procedures for handling subject access requests and other individual rights.

3.4 There hasn't been any previous personal data breaches recorded by the NW IFAC, but the report notes the occurrence and appropriate management of a recent cyber incident. Nonetheless, there are recommendations for adopting a formal personal data breach procedure, improving staff awareness, and ensuring regular bespoke data protection training is undertaken. Due diligence in third-party processor arrangements and ongoing cyber-security awareness are also emphasised.

3.5 It is advised to implement a clear Records Management Policy and Retention Schedule to ensure compliance with the GDPR. Data sharing, particularly with bodies such as Lancashire Constabulary, should be governed by formal agreements to clarify roles and responsibilities and reinforce accountability. Communications with stakeholders are conducted on a consent basis and are considered compliant with both PECR and GDPR.

3.6 In summary, while NW IFCA demonstrates commitment to data protection compliance, several recommendations are put forward to strengthen governance, enhance staff awareness, ensure up-to-date documentation and policies, and formalise key data protection processes. These steps will help the Authority maintain robust data protection standards and demonstrate ongoing compliance with statutory obligations.

4 Findings

4.1 Accountability and Governance

4.1.1 The Data Protection (Charges and Information) Regulations 2018 require the North Western Inshore Fisheries and Conservation Authority (NW IFCA) and other organisations that process personal data to pay a data protection fee to the ICO. The Data Protection Officer (DPO) can confirm that the Authority is registered with the ICO (Z6486920), and that its registration is due to expire on 18 March 2026. The tier 2 registration is the correct tier, as the organisation employs more than 10 but fewer than 250 individuals. Registration details should include the name and contact information of the DPO.

4.1.2 The Information Commissioner's Office (ICO) has advised that, if the DPO function is provided by an external organisation, the details of that organisation should be published. It is recommended that the registration be updated to include Blackpool Council's details as the DPO **(Recommendation 1).**

4.1.3 The UK GDPR introduces a duty for you to appoint a DPO if you are a public authority or body, or if you carry out certain types of processing activities. DPO's assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO). The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

4.1.4 The Authority has appointed Blackpool Council to act as its DPO, and relevant post holders possess appropriate qualifications in data protection. As a local authority, Blackpool Council is adequately resourced. To meet the requirement of reporting to the highest management level, it is recommended that this report be issued to the Chief Executive and tabled at a relevant Board meeting **(Recommendation 2).**

4.1.5 The NW IFCA has a 'Data Security Policy' published on its website, making it accessible to employees and other stakeholders. However, awareness of this policy appears to be limited. The 'Data Security Policy' was last reviewed on 12/12/2023. A core policy in data protection is important as it demonstrates the Authority's commitment towards data protection and outlines the responsibilities of individual employees. The DPO has reviewed the content of the policy and found that its detail is limited. Therefore, it is recommended that the policy be replaced with a more comprehensive version, which can be provided by the DPO **(Recommendation 3).**

4.1.6 Once the policy has been updated, it is recommended that it be distributed to all employees and incorporated into the induction process. This approach will ensure that every employee is fully aware of their responsibilities **(Recommendation 4)**.

4.1.7 In recent years, Artificial Intelligence (AI) has emerged and become increasingly prevalent in everyday life. The potential application of AI at NW IFCA was briefly discussed, and, at present, it is anticipated that there will be limited use in the immediate future, with ChatGPT cited as the only example. While some organisations have implemented standalone AI policies, it was agreed that, for now, incorporating a dedicated section on AI within the revised Data Protection Policy is proportionate. There are many benefits and efficiencies to be gained from the use of AI; therefore, the policy position is not to prohibit its use, but rather to ensure that appropriate governance and controls are in place regarding the use of AI to process personal data.

4.1.8 Article 30(1) of the UK GDPR requires that the 'controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.' Documenting processing activities is not only a legal requirement, but it also supports robust data governance and enables NW IFCA to demonstrate compliance with other aspects of the UK GDPR. The NW IFCA confirmed it does not currently have a Record of Processing Activities (RoPA). It is recommended that the management team complete the Information Commissioner's Office (ICO) template RoPA to comply with the requirements of Article 30 **(Recommendation 5).** This will then need to be reviewed regularly to ensure it remains accurate and up to date.

4.1.9 Data protection impact assessments (DPIA) are a tool to help identify and minimise the data protection risks of new projects. They are part of the accountability obligations placed on organisations by the GDPR and are an integral part of the 'data protection by default and by design' approach. The Company has not previously completed any data protection impact assessments. It is therefore recommended that retrospective assessments be completed for core systems, such as the C-Front system and body-worn cameras, using a template provided by the DPO **(Recommendation 6).**

4.1.10 Article 28(3) of the GDPR stipulates that 'processing by a processor shall be governed by a contract or other legal act under domestic law'. Ordinarily, this includes a data protection clause setting out each party's obligations and a processing schedule that records specified information, such as the data categories, type of data subjects, duration of processing etc. The Authority should review its existing agreements such as with C-Front to ensure it is complying with this obligation **(Recommendation 7).**

4.1.11 Part 3 of the Data Protection Act 2018 only applies to competent authorities processing personal data for criminal law enforcement purposes. There are additional rules which apply to 'sensitive processing' of some specified types of particularly sensitive data. Sensitive processing is defined in section 35(8) and if this occurs one of the conditions in Schedule 8 must apply. Once the RoPA is completed, a determination is required from the DPO whether the requirements of Part 3 apply **(Recommendation 8).**

4.2 Individual Rights

4.2.1 Individuals have the 'right to be informed' about the collection and use of their personal data. This is a fundamental transparency requirement under the GDPR and is commonly referred to as 'privacy information'. The default position is that, wherever possible, such information should be provided to the data subject at the point at which their personal data is collected.

4.2.2 The NW IFCA has a public facing privacy notice on its website and this covers the following purposes:

- issue and manage fishing permits.
- provide you with information relevant to the fisheries you are involved with.
- manage fisheries sustainably.
- enforce fisheries regulations.
- select and recruit staff.

4.2.3 This is complemented by several versions of individual privacy notices, each titled as follows:

- GDPR Privacy Notice Vessel owners
- GDPR Privacy Notice Permit Holders
- GDPR Privacy Notice Drone
- GDPR Privacy Notice Catch Returns
- GDPR Privacy Notice Body Worn video

- NWIFCA Protocol Body Worn Video Information
- GDPR Privacy notice Photo consent

4.2.4 According to the website, these public-facing privacy notices were last updated on 13/12/2023. As they are available on the website, the notices are accessible to data subjects; however, given the time that has elapsed, it is not clear whether data subjects were directed to the notices at the point when their personal data was collected, for example, during the completion of an application form. It is recommended that a review of each notice is undertaken to assess whether it is still reflective of practice, contains the required information, and is embedded in processes to ensure that data subjects are furnished with a copy **(Recommendation 9).**

4.2.5 In addition to processing the personal data of members of the public and customers, the Authority, of course, processes the personal data of its employees. In terms of personal data categories, this is often more sensitive, as it includes financial information for payroll purposes and may contain special category data, such as health information. With regard to the right to be informed, employees possess the same entitlements under the GDPR, and the Authority should provide information concerning how their personal data is processed. Currently, this is not happening; therefore, it is recommended that a fit-for-purpose workforce privacy notice be created and implemented **(Recommendation 10).** It is standard practice to have a separate notice for recruitment, which will include unsuccessful candidates, and then a comprehensive notice for employees, with the latter incorporated into the induction process.

4.2.6 Under the UK GDPR, individuals have several information rights, including the right of access, rectification, erasure, restriction of processing, data portability, the right to object, and rights related to automated decision-making or profiling.

4.2.7 The most common of these is the right of access which is contained within Article 15 of the GDPR, often referred to as 'subject access', which enables individuals to obtain a copy of their personal data, along with other supplementary information. Data controllers must comply with a subject access request (SAR) without undue delay and, at the latest, within one month of receiving the request. If the request is considered complex, this period can be extended to three months. Reasonable searches must be undertaken, and information can only be withheld if an exemption applies. The ICO has produced detailed guidance for organisations, which is designed to assist organisations in complying with their obligations.

4.2.8. The right of access was discussed further as part of the audit, and the DPO was advised that the Authority has previously received a very small number of requests, and? there being no reason to suggest these were not actioned appropriately. Although the Data Protection Policy contains brief references to this matter, it is recommended that the Authority implement a standalone right of access procedure **(Recommendation 11).** This will help raise awareness of this right and assist employees should a request be received.

4.2.9 There has been no formal requests received under the remaining 'individual rights' that are afforded to individuals under the GDPR, including the right to rectification and erasure.

4.3 Data Security

4.3.1 Article 5(1) (f) of the UK GDPR concerns the 'integrity and confidentiality' of personal data. It requires personal data should be processed in a manner that ensures appropriate security of the

personal data, with appropriate measures being both organisational and technical.

4.3.2 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Personal data breaches create risk of regulatory action by the ICO (including monetary penalties), reputational risk and place individuals at risk of harm or distress. Also, Individuals who have suffered harm or distress as a result of the Company's failure to comply with the GDPR can also seek financial compensation; this right is contained within Article 82 of GDPR and creates an additional financial risk. Personal data breaches can occur in various forms, with the most common being emails sent to the wrong individual; however, they can also include minor verbal disclosures or large-scale cyber-attacks that can paralyse organisations.

4.3.3 It was reported that prior to the audit there had been no recorded personal data breaches within the preceding two year period, but since the date of the audit there has been a cyber incident. The DPO was informed of the incident in a timely manner and appropriate actions were taken as a result, in conjunction with the Authority's IT providers. These included identifying the source of the attack, containing the risk through the application of appropriate technical measures, communicating effectively with stakeholders, and considering appropriate notifications.

4.3.4 When a personal data breach has occurred, the DPO must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk a notification needs to be undertaken to the ICO within 72 hours. It is important organisations have clear procedures in place to ensure personal data breaches are reported to the DPO in a timely manner to make this assessment. It is also important that relevant information is recorded in a personal data breach register, that a thorough investigation is undertaken to identify the cause, that any risks are mitigated, and that measures are put in place to reduce the likelihood of a recurrence. It is recommended that a personal data breach procedure be adopted, which includes a standard reporting form **(Recommendation 12).** This procedure then needs to be circulated to employees to ensure they are aware of what constitutes a personal data breach and what to do in the event of one occurring **(Recommendation 13).**

4.3.5 Regular data protection training is important for raising awareness of the obligations placed on the NW IFCA by the GDPR, mitigating the likelihood of a personal data breach, and, in the event of a breach, is a key factor for the ICO when considering whether enforcement action is appropriate. According to the ICO's best practice, data protection training should be completed annually, but must be undertaken at least once every two years as a minimum.

4.3.6 Currently, new employees are required to complete a mandatory set of courses on the Breathe HR system, which includes a module entitled 'General Data Protection Regulation'. The introduction to this module states that it should take fifteen minutes to complete. Additionally, there is a small set of questions that users are required to answer upon completion. As a result, a large percentage of the workforce have not received training within the last two years, and for those who have, it has been relatively brief. It is therefore recommended that the current training be supplemented by bespoke training delivered by the DPO, to take place at least every two years **(Recommendation 14).**

4.3.7 Article 28(1) of the GDPR requires data controllers 'shall use only processors providing sufficient guarantees' around the security of personal

data, which in practice means NW IFCA should complete due diligence before engaging in to contracts with third parties. Cloud hosted solutions present unique security risks and the National Cyber Security Centre (NCSC) has developed cloud security principles for organisations to consider. The DPO has created a specific 'Due Diligence Form' that incorporates organisational measures and also the principles referred to above. It is recommended said form is adopted immediately and retrospectively completed for any high-risk processors **(Recommendation 15).**

4.3.8 The sole biggest risk to all organisations at present is the risk of a successful cyber-attack, with the recent cyber incident at the Authority. Attacks are constantly increasing in volume and sophistication, with some threat actors even including nation states. Despite the large data security budgets of global multinational companies or technical measures deployed by large public section organisations, no organisation is immune of being a victim of a cyber-attack. The repercussions can include the loss of access and theft/ransomware of personal data, the inability for some organisations to operate and extensive recovery times. Cyber-security material has been regularly distributed by the IT provider to raise awareness of these risks; however, despite these measures, a significant risk remains due to the nature of the threat. This practice should continue to reduce risk.

4.3.9 The Authority's IT provider is the Lake District National Park Authority, which has provided assurance regarding the implementation of appropriate technical measures to mitigate risk. The DPO was informed that devices have suitable encryption applied, firewalls are in place for the network, and appropriate password strengths are enforced. At present, Microsoft 365 is the primary suite of productivity tools in use and provides the facility to share data securely. This point should be incorporated into training to help prevent high-risk personal data from being shared via email, as this creates a risk of the data being sent to the wrong recipient. Another mechanism to prevent unauthorised access to personal data is to ensure that appropriate access controls are in place. Assurance was provided to the DPO that personal data is properly partitioned within internal drives and that suitable access controls have been applied.

4.4 Data Retention and Sharing

4.4.1 Article 5(1)(e) of the GDPR states data shall be '*kept in a form which permits identification of data subjects for no longer than is necessary'*. Principle (e) aka the storage limitation principle has close links with the data minimisation and accuracy principles.

4.4.2 A discussion was held regarding the retention and destruction of personal data. Due to changes in senior management over recent years, it was communicated to the DPO that the Authority does not hold a significant quantity of historic personal data. It was considered that any risk would be associated with individuals' own OneDrives.

4.4.3 To comply with this principle the Authority should adopt a 'Records Management Policy' that contains core expectations in relation to records management and a 'retention schedule' that stipulates specifically how long data is retained. This can be distributed to all employees with a reminder about their responsibilities in terms of data they hold. **(Recommendation 16).**

4.4.4 NW IFCA uses CCTV in various forms, such as at fixed locations at its offices, bodycams and drones. The retention of the footage is set out 30 days, unless its required to be retained longer for enforcement purposes.

4.4.5 The Privacy and Electronic Communications Regulations (PECR) applies specific rules to marketing. Direct marketing is defined as 'the communication (by whatever means) of advertising or marketing material that is directed to particular individuals'. Individuals may register as stakeholders and receive information about the Authority's activities; this operates on a consent basis. The GDPR introduced a higher standard of consent, requiring it to be specific and granular, and allowing individuals to freely withdraw their consent at any time. The DPO is of the view communications with stakeholders is compliant with both PECR and the GDPR.

4.4.6 As a public authority NW IFCA is required to exchange personal data with other organisations. In these instances, it is good practice to have a data sharing agreement in place. Data sharing agreements set out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all the parties involved in sharing to be clear about their roles and responsibilities. Having a data sharing agreement in place helps you to demonstrate you are meeting your accountability obligations under the GDPR. It is recommended that, owing to the frequency and nature of data sharing, the DPO should explore establishing a formal agreement with Lancashire Constabulary **(Recommendation 17).**

5 Recommendations

No.	Recommendations	Priority	Management Response	Owner	Target Completion Date
1	ICO registration be updated to include Blackpool Council's details as the DPO (4.1.2)	2	Accept, Alison has actioned.	Alison	Complete
2	To meet the requirement of the DPO reporting to the highest management level, it is recommended that this report be issued to the Chief Executive and tabled at a relevant Board meeting (4.1.4)	3	Accept, CEO has received report. To be tabled at next full Authority meeting.	Mark	19th March 2026
3	Data Security Policy be replaced with a more comprehensive version, titled Data Protection Policy (4.1.5)	2	Accept, Jonathan to provide.	Jonathan	28th Feb 2026
4	Revised Data Protection Policy to be distributed to all employees and incorporated into the induction process (4.1.6)	2	Accept, Mark or Alison to distribute	Alison	31st March 2026
5	Complete the Information Commissioner's Office (ICO) template RoPA to comply with the requirements of Article 30 of the GDPR (4.1.8)	1	Accept, Alison to co-ordinate with teams.	Alison	30th April 2026
6	Complete retrospective data protection impact assessments for core systems, such as the C-Front system and body-worn cameras, using a template provided by the DPO (4.1.9)	1	Accept, Jonathan to provide Joe with templates	Joe	31st March 2026
7	The Authority should review its existing data processors to ensure it is complying with Article 28 of the GDPR (4.1.10)	2	Accept, Alison to provide Jonathan with copies to review	Alison/ Jonathan	31st March 2026
8	Once the RoPA is completed, a determination is required from the DPO whether the requirements of Part 3 of the DPA 2018 apply (4.1.11)	3	Accept, Jonathan to review when RoPA is complete	Jonathan	30th June 2026
9	Review privacy notices to assess whether it is still reflective of practice and meet standard required by the ICO (4.2.4)	2	Accept, documentation to be provided to Jonathan and then meeting to review with relevant teams.	Jonathan/ Alison	30th June 2026

10	Implement a workforce privacy notice (4.2.5)	1	Accept, Jonathan to provide template.	Jonathan/ Mark	31st March 2026
11	Implement a right of access procedure to assist with subject access requests (4.2.8)	3	Accept, Jonathan to provide template	Jonathan	28th Feb 2026
12	Implement a personal data breach procedure (4.3.4)	2	Accept, Jonathan to provide template	Jonathan	28th Feb 2026
13	Circulate personal data breach procedure to all employees (4.3.4)	3	Accept, Alison to distribute	Alison	31st March 2026
14	Bespoke training delivered by the DPO, to take place at least every two years (4.3.6)	2	Accept, Jonathan to deliver via Teams. Mark to provide dates.	Jonathan	30th June 2026
15	Implement a 'Due Diligence Form' for processors (4.3.7)	2	Accept, Jonathan to provide template	Jonathan	28th Feb 2026
16	Create and implement a Records Management Policy & Retention Schedule (4.4.3)	1	Accept, Jonathan to provide template and completion joint effort.	Jonathan	30th June 2026
17	Explore establishing a formal data sharing agreement with Lancashire Constabulary (4.4.6)	3	Accept, Jonathan to provide template Joe	Jonathan	30th June 2026

1 = essential to address a high risk, 2 = necessary to address a moderate risk, 3 = represents best practice or addresses a low level of risk

6. Document Control

Document owner:	Data Protection Officer
Document number:	IFCA-A-01
Document category:	Audit Report

Record of Amendments:

Date	Version	Amended by	Description of changes
Dec 2024	0.1	Data Protection Officer	First Draft
Jan 2026	1.0	Data Protection Officer	Final