NON-CONFIDENTIAL – FOR PUBLICATION

REPRIMAND

POST OFFICE LIMITED

Reprimand concerning infringements of Articles 5(1)(f), 32(1) and 32(2) UK GDPR

2 December 2025

UK GENERAL DATA PROTECTION REGULATION

(Article 58(2)(b))

CORRECTIVE POWERS OF THE INFORMATION COMMISSIONER

REPRIMAND

DATED: 2 December 2025

To: Post Office Limited

Of: 100 Wood Street
London
EC2V 7ER

I. INTRODUCTION AND SUMMARY

1. Post Office Limited (the "**Post Office**") is a company registered with Companies House in England and Wales with company number 02154540.

2. The Post Office provides mail, financial and government services to the public through its nationwide network of over 11,500 Post Office branches. The vast majority of these branches are run by franchise partners or independent business people who used to be

known as sub-postmasters or sub-postmistresses (but are now known as postmasters).[1,2]

3. This Reprimand relates to the unauthorised disclosure of the personal data[3] of 502 postmasters (the "**Data Subjects**") who were part of the group litigation that exposed the Horizon IT scandal.[4]

4. On 25 July 2025, the Commissioner sent a Notice of Intent to issue a Reprimand (the "**NOI**") to the Post Office setting out provisional findings that the Post Office had infringed Articles 5(1)(f), 32(1) and 32(2) of the UK General Data Protection Regulation ("**UK GDPR**").[5] The Post Office submitted representations (the "**Representations**") to the Commissioner in response to the NOI in writing on 15 September, 31 October, 21 November 2025 and 2 December 2025. The Post Office also made oral representations during a virtual meeting on 10 November 2025. This Reprimand takes into account the Representations, and, where appropriate, makes specific reference to them.

5. Pursuant to Article 58(2)(b) UK GDPR, the Information Commissioner (the "**Commissioner**") issues the Post Office with this Reprimand.

[1] Post Office Corporate
[2] Post Office - GOV.UK
[3] As defined in Article 4(1) UK GDPR.
[4] Further details of the Horizon IT scandal are set out at paragraph 13 below.
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018. For the period 25 May 2018 to 31 December 2020, references in this Penalty Notice to the UK GDPR should be read as references to the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) as it applied in the UK during that period.

6. The Commissioner finds that between 31 March 2023[6] and 15 November 2024[7] the Post Office infringed Articles 5(1)(f), 32(1) and 32(2) UK GDPR (the "**Infringements**") for the reasons set out in this Reprimand. In summary:

   a. The Infringements relate to the processing of personal data by the Post Office's Corporate Communications Team that took place if that team prepared information to be published on the Post Office's public facing corporate website that related to the Horizon IT scandal (the "**Relevant Processing**"). This included the processing of personal data of the Data Subjects.

   b. The Infringements of Article 5(1)(f) and Article 32 UK GDPR occurred because the Relevant Processing was not carried out in a manner that ensured appropriate security[8] of the personal data of the Data Subjects using appropriate technical and organisational measures as required by Articles 5(1)(f) and 32 UK GDPR.

7. As a consequence of the Post Office not having appropriate technical and organisational measures in place, as required by Articles 5(1)(f) and 32, the personal data of the Data Subjects was disclosed publicly, on the Post Office's corporate website, on 25 April 2024 (the "**25 April Incident**").

8. In reaching the decision to impose a Reprimand in this case, the Commissioner has had regard to all of the circumstances of this case, the remedial measures put in place, the steps taken to

[6] The date when the Horizon webpage was established.
[7] The date on which the Commissioner finds the Post Office implemented appropriate security measures (see paragraph 56 below).
[8] Specifically, protection against unauthorised disclosure.

mitigate damage to Data Subjects and the compensation paid to the majority of Data Subjects by the Post Office in respect of the 25 April Incident. The Commissioner has had regard to the Regulatory Action Policy and to the Commissioner's public sector approach. Please see section IV below for further details on the application of the public sector approach.

RELEVANT LEGAL FRAMEWORK

9. Under Article 58(2)(b), the Commissioner has the power "*to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation*".

10. Chapter II of the UK GDPR sets out the principles relating to the processing of personal data that controllers must comply with. Article 5(1) UK GDPR lists these principles and at subsection (f) includes the requirement that "*personal data shall be … processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised … processing … using appropriate technical or organisational measures*". This is referred to in the UK GDPR as the "*integrity and confidentiality*" principle.

11. Article 32 UK GDPR (security of processing) materially provides:

> *"(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…*

(2) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from … unauthorised disclosure of … personal data transmitted, stored or otherwise processed."

II. BACKGROUND TO THE INFRINGEMENTS

12. This section summarises the relevant background to the Infringements. It does not seek to provide an exhaustive account of all the details of the events that have led to the decision to issue this Reprimand.

A. Wider context to the Infringements

13. The Post Office describes the 'Horizon IT Scandal' as "*a dispute, between Post Office and a group of postmasters, which took place over many years. It primarily concerned the reliability of the Horizon computer system used in post offices, issues related to postmasters' contracts, and the culture of Post Office at the time*".[9]

14. The Post Office rolled out the Horizon computer system to all of its branches in 1999. Between 1999 and 2015, many postmasters were wrongly held responsible for losses in their branch accounts that they could not explain, with many being prosecuted for theft, fraud and false accounting, based on unreliable Horizon data.[10]

15. In 2017, a group litigation action was brought against the Post Office by 555 postmasters. This legal action exposed the Horizon IT scandal. The impact of the Horizon IT scandal is well documented, with the then Prime Minister, Rishi Sunak, describing

[9] Post Office Corporate
[10] Post Office Corporate

it as "*one of the greatest miscarriages of justice in this country's history*".[11]

16. In 2019 the 555 postmasters reached a settlement with the Post Office which was formalised in a Group Litigation Order ("**GLO**") settlement deed (the "**Settlement Deed**").

B. The report by the Post Office

17. On 19 June 2024 at 18:12, the Post Office formally reported a personal data breach by completing the Commissioner's 'Report a data breach' online form.[12] The Post Office reported that an unredacted copy of the Settlement Deed had been uploaded to the Post Office's corporate website in error, and had been available since 19 April 2024. In subsequent correspondence, the Post Office clarified that the supplier who manages the Post Office's corporate website confirmed that the unredacted Settlement Deed was available on the website from 25 April 2024 (not 19 April 2024) to 19 June 2024.

18. The Post Office has informed the Commissioner that the timeline of events leading up to the Post Office reporting the incident was as follows:

    a. The Horizon webpage was set up by the Post Office on 31 March 2023 to share information about ongoing initiatives with the wider public.

    b. On 25 April 2024, the Corporate Communications Team[13] was conducting routine updates to the Horizon webpage

[11] Government to quash wrongful Post Office convictions - GOV.UK
[12] Post Office Limited breach report dated 19 June 2024
[13] The Post Office has confirmed that the Corporate Communications Team are responsible for routine website maintenance and are actively involved in publishing information on various Post Office webpages.

when it was identified that the link to the redacted version of the Settlement Deed was 'broken'. This required the document to be re-uploaded to the Horizon webpage to fix the link. A redacted version of the Settlement Deed had previously been uploaded to the Post Office's corporate website in 2020, following a Freedom of Information request.

c. 'Employee A' sent 'Employee B' a copy of the Settlement Deed. This was intended to be the redacted version of the Settlement Deed previously published on the corporate website in 2020, however it was the unredacted version.

d. The unredacted Settlement Deed contained personal data relating to 502 Data Subjects[14] involved in the court case against the Post Office which exposed the Horizon IT scandal. The categories of personal data involved were: the full names and home addresses of the Data Subjects, their postmaster status as of 2019, and the sum of money paid to the group in total (this included payments under the settlement deed covering legal costs, damages and litigation funding). The ICO understands that a significant majority of the payments went towards the claimants' legal costs and litigation funding.

e. At 14:00 on 19 June 2024, the Director of the Post Office's Remediation Unit received a text message from an external law firm alerting the Post Office to the presence of the unredacted Settlement Deed on the Post Office's corporate website. The unredacted Settlement Deed was removed from

[14] During the course of this investigation, the Post Office stated that although 555 postmasters reached a settlement with the Post Office, only 502 of these 555 claimants are Data Subjects (following the removal of businesses and claimants who have since died).

the website within the hour. The Post Office reported the 25 April Incident to the Commissioner on the same day.

19. Upon becoming aware of the 25 April Incident, the Post Office established an emergency working group to review the events and implement appropriate actions in response.

20. The Post Office has informed the Commissioner that it took the following steps to mitigate the impact of the 25 April Incident on the affected data subjects:[15]

    a. Corresponded with the three main law firms representing the majority of the Data Subjects, apologising for the 25 April Incident and setting out the steps taken by the Post Office. The letter also provided the Post Office's Data Protection Officer's direct contact details. The Post Office contacted the remaining claimants via their legal representatives or directly in writing;

    b. Offered compensation to all Data Subjects either directly or through their legal representatives;

    c. Provided the Experian Identity Plus product for UK residents covering 24 months of identity, fraud checking and dark web monitoring. Experian Identity Works Global was provided for those with overseas addresses which covered 24 months of dark web monitoring;

[15] Email from the Post Office DPO to the ICO Lead Case Officer dated 27 June 2024; Letter from the Post Office to the ICO dated 6 August 2024

d. Contacted Wayback Machine, Google and National Archives to remove the unredacted Settlement Deed from their respective caches;

e. Added the document name to [redacted] which monitors the dark web on behalf of the Post Office;

f. Checked all links on websites under the Post Office's control to ensure that there were no other incidents;

g. Conducted an urgent internal assurance review to assess the status of the control environment within the Post Office's Corporate Affairs function; and

h. Reviewed the process for uploading documents to the Post Office's corporate website and created a new documented policy for publishing information on the website.

21. [redacted]

22. The Post Office confirmed in its Representations, that it accepts that the 25 April Incident breached the UK GDPR. It emphasised that it had informed the Commissioner of its acceptance of a breach of Article 5(1)(f) UK GDPR on 6 August 2024. The Commissioner

acknowledges this admission of liability, which was considered as part of his investigation and consideration of this case.

23. Policies and guidance (relevant to the security of the Relevant Processing) which the Post Office introduced following the 25 April Incident are further described at paragraphs 35 to 37 below.

C. Damage and distress caused to the Data Subjects

24. No individual complaints have been received by the Commissioner, however, the Commissioner received a letter from Freeths LLP ("**Freeths**"), on behalf of 365 of the Data Subjects, setting out how the 25 April Incident has caused considerable stress and anxiety for its clients.[16] The letter specified that "*the shock and anxiety of this incident cannot help but compound all of the adverse harms suffered by our clients as a result of the wider Horizon scandal*". The letter stated that many of its clients were already emotionally fragile or suffering from physical or mental health problems which had themselves been caused or exacerbated by their previous treatment by the Post Office. Other clients expressed concerns about being identified as an individual in receipt of a settlement sum, including experiencing anxiety about being targeted for, or being vulnerable to, burglary (due to names and addresses being disclosed).

25. The Commissioner notes that the Post Office has received individual complaints from Data Subjects directly[17].

26. The Representations noted that the Commissioner had not received any individual complaints but had instead placed reliance on

[16] Letter from Freeths LLP to the ICO dated 24 July 2024
[17] Letter from the Post Office to the ICO dated 6 August 2024

correspondence from Freeths. The Post Office considered the letter from Freeths setting out how the 25 April Incident caused its clients shock and anxiety to be "*obviously problematic, given that the impact of the Incident on affected data subjects is likely to have varied substantially*". The Post Office explained that it had reached out to all affected Data Subjects and stated that "*a considerable number of those data subjects have either not responded or have given every impression that they were not meaningfully impacted by the Incident.*". The Post Office submitted that although passwords and telephone numbers were not disclosed in the 25 April Incident, some individuals reported that the 25 April Incident caused them to change their passwords and to receive unwanted telephone calls.

27. The Commissioner has carefully considered the representations from the Post Office on the impact of the 25 April Incident on data subjects. Whilst the Commissioner does not discount that the impact of the 25 April Incident will vary between Data Subjects, the Commissioner considers that it is clear from Freeths, as well as from media reporting at the time,[18] that the 25 April Incident had a considerable impact, causing stress and anxiety for many of the Data Subjects.

28. The Post Office, in its Representations, sought to understand the basis for the Commissioner's reliance on the Freeths 24 July letter, as the purpose of the letter was for civil litigation. This letter was addressed to the Post Office but copied to the Commissioner on the

[18] Post Office data leak: hundreds of Horizon victims offered up to £5,000 compensation | Post Office Horizon scandal | The Guardian: "*We cannot underestimate the level of pain, anxiety, stress and worry that so many people have had to suffer through this new episode…. The impact on myself and my family has been profound on top of an already traumatic past 10 years due to the Horizon scandal.*"; Post Office accidentally leaks names of sub-postmasters - BBC News: "*As you can imagine this has caused a great amount of upset, distress and anger amongst those whose data is now within the public domain*."

basis that "*the ICO will inevitably be interested in the impact on affected data subjects of the Disclosure*". The Commissioner is satisfied that it is reasonable for him to review and assess this letter for the purposes of his investigation. The Commissioner is aware that the letter was prepared for the purposes of civil litigation. This context was taken into account and appropriate weight was given to the contents of the letter in assessing its relevance and evidential value.

D. The Post Office's relevant procedures, policies and guidance

Organisational measures in place prior to the 25 April Incident

29. During his investigation, the Commissioner asked for information about the Post Office's policies, procedures or guidance in place in relation to the Corporate Communications Team's role in maintaining the corporate website, including the uploading of documents.

30. The Commissioner understands that there were no documented policies, procedures or guidance in place prior to the 25 April Incident relating to the Relevant Processing. Instead, there was a heavy reliance on individual experience and no established processes or controls.[19]

31. The uploading of documents to the corporate website, and routine website maintenance, was part of the role of employees in the Post Office's Corporate Communications Team. Indeed, the Corporate Communications team set up the Horizon webpage for the purpose

[19] Post Office internal assurance review dated 27 June 2024

of sharing information about ongoing initiatives with the wider public.

32. The Commissioner finds that, in practice, the procedure (as it related to the Relevant Processing) was as follows:[20]

    a. The ability to upload documents to the Horizon webpage was limited to one employee in the Corporate Communications team.

    b. As the Corporate Communications team did not have access to the Post Office's internal information rights case management system or the FOI team's SharePoint folder, they retained copies of relevant documents on their OneDrives.

    c. The employee with the ability to upload documents to the Horizon webpage would receive documents for upload from another colleague within the Corporate Communications team, who had such documents saved on their OneDrive.

    d. No checks were conducted on documentation prior to upload, as the employee responsible for uploading was under the impression that such checks had already been performed.

    e. The relevant document was uploaded to the relevant part of the Horizon webpage.

33. The Commissioner has also been made aware that, prior to the 25 April Incident:

[20] Letter from the Post Office to the ICO 6 August 2024; Post Office internal fact finding investigation report dated 22 June 2024; Letter from the Post Office to the ICO 29 August 2024

a. All Post Office staff received training in both data protection and information security on induction and were required to complete a 'refresher' version on an annual basis, with a focus on key topics of interest based on incident trends from the past 12 months and relevant legal / business requirements. The training content included guidance on recognising personal data, how personal data may be processed, and how to report data protection incidents. Both individuals involved in the 25 April Incident completed their training within the required window.[21] However, there was no training provided that specifically covered the uploading of information to the corporate website.[22]

b. The Post Office had an 'Information Classification Standard' policy in place which stipulated that 'Confidential Information' (the unauthorised disclosure of which "*could result in financial or reputational damage*") "*must only be shared with employees, agents and contractors who have a "need to know""* and "*must not be published to the Internet*".[23] This document was last updated on 14 February 2024.

34. The Post Office's 'Protecting Personal Data Policy' included a section on 'Protecting Post Office information', reminding employees that they must "*take personal responsibility for the proper use, circulation, retention, protection and disposal of Post Office's information*". This document was last updated on 18 December 2023. Prior to the 25 April Incident, there were no documented

[21] Letter from the Post Office to the ICO dated 6 August 2024.
[22] Letters from the Post Office to the ICO dated 8 and 29 August 2024.
[23] Cyber Security Standard – Information Classification Standard version V2.3

policies, procedures or guidance in place in relation to the Corporate Communications team in maintaining the corporate website, nor in respect of their approach to quality assurance or data management.

Organisational measures introduced following the 25 April Incident

35. On 27 June 2024, the Post Office completed an internal assurance review to establish the root cause of the 25 April Incident, and to identify actions and measures to prevent a similar incident from reoccurring. The Post Office informed the Commissioner that by 15 November 2024, all actions identified from their internal assurance review had been addressed.[24]

36. By the end of July 2024, the Post Office had created a 'Data control framework' for the Communications, Corporate Affairs and Brand team. This policy sets out the protocols and processes for storing and publishing data within this team. The policy states that:

    a. Documents should be appropriately classified as either 'Public', 'Internal', 'Confidential' or 'Strictly Confidential' (the definitions of such classifications are found in the Post Office's 'Information Classification Standard').

    b. 'Confidential' and 'Strictly Confidential' documents should be stored centrally on SharePoint, in the relevant folder, with access restricted accordingly.

    c. All documents which include 'Confidential' or 'Strictly Confidential' data need to go through a three-step process

[24] Post Office Internal Assurance review dated 27 June 2024; Letter from the Post Office to the ICO dated 29 November 2024

prior to publication. The Commissioner understands that this process involves the following steps:[25]

i. The document intended for publication is sent to the publisher, with an appropriate confidentiality marking;

ii. The publisher will then review the document to ensure it is valid (not corrupted) and has a sensitivity level assigned. This publisher will then return the document to the individual requesting publication, confirming the document is correct; and

iii. In doing so, the publisher will copy in a member of the Communications lead team (with their prior agreement) who has not been involved in that publication previously so they can review and approve publication.

37. By 14 November 2024, the Post Office had updated its risk and controls register. This now includes a specific risk for internal confidential or strictly confidential data being accidentally or maliciously shared, and stipulates the control as the three-step process noted above, for publishing confidential data.[26]

III. THE COMMISSIONER'S FINDINGS OF INFRINGEMENT

A. Controllership and jurisdiction

38. The UK GDPR applied to the Relevant Processing by virtue of Article 3(1) UK GDPR. The Relevant Processing took place in the context

[25] As set out in 'Comm team Process Risk and Controls mapping' dated 14 November 2024
[26] 'Comm Team Process Risk and Controls mapping' dated 14 November 2024

of the activities of a controller established in the UK, and none of the exceptions in Article 2 UK GDPR applied.

39. The Post Office was the controller in respect of the Relevant Processing. The Post Office determined its purpose and means within the meaning of Article 4(7) UK GDPR and s6 Data Protection Act 2018 ("**DPA**").

40. As the controller of the personal data of the Data Subjects and pursuant to Articles 5(1)(f) and 32 UK GDPR the Post Office was responsible for implementing appropriate technical and organisational measures to ensure and to be able to demonstrate that the processing operations were performed in accordance with the UK GDPR.

B. Nature of the personal data and context of the Relevant Processing

41. The unredacted Settlement Deed involved in the Relevant Processing included personal data (specifically full names, addresses, postmaster status as of 2019, and the overall settlement sum) relating to identified natural persons. The unredacted Settlement Deed did not contain details of the specific sums paid to individual Data Subjects.

42. The Commissioner acknowledges the particular sensitivities of the personal data disclosed, given the wider context of the Horizon IT Scandal (as addressed at paragraphs 13 to 16 above) in which postmasters were dismissed and / or prosecuted based on unreliable Horizon evidence.

C. The Infringements

43. The fact that an unauthorised disclosure took place on 25 April 2024 is not, in and of itself, sufficient to find that the Post Office has infringed Articles 5(1)(f) and 32 UK GDPR.[27]

44. In order to assess the Post Office's compliance with Articles 5(1)(f) and 32 UK GDPR, the Commissioner must necessarily exercise his judgement, as regulator, as to whether the Post Office ensured "*appropriate*" security, and whether "*appropriate*" technical and organisational measures were in place (taking into account "*the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*").

45. For the reasons set out below, the Commissioner's view is that the Post Office has infringed Articles 5(1)(f), 32(1) and (2) UK GDPR. The Infringements involved a failure by the Post Office to use appropriate technical and organisational measures to ensure the appropriate security of the personal data subject to the Relevant Processing.

Appropriate security of the personal data

46. In assessing whether the Post Office processed personal data in a manner that ensured "*appropriate security of the personal data*" under Article 5(1)(f) UK GDPR (and, equivalently, the "*level of security appropriate to the risk*" under Article 32 UK GDPR), the Commissioner has considered the risk to the rights and freedoms

[27] See the CJEU's judgment in VB v Natsionalna agentsia za prihodite (ECLI:EU:C:2023:986) (Case C-340/21) at paragraphs 22-39, which the Commissioner has had regard to.

of the Data Subjects which the Relevant Processing presented, in particular, from unauthorised disclosure. Recital 75 UK GDPR states that such risk "*may result from personal data processing which could lead to physical, material or non-material damage*".

47. In ensuring a level of security appropriate to the risk, Article 32(1) UK GDPR requires a controller to take into account the likelihood and severity of the risk to the rights and freedoms of data subjects.

48. The Commissioner considers that the evidence establishes that the Post Office knew, or ought to have known, that the data was highly sensitive because:

    a. The context of the Horizon IT scandal, and the fact the Data Subjects had been through group litigation in order to reach the settlement (as agreed in the Settlement Deed) with the Post Office (following dismissals and / or prosecutions based on unreliable Horizon evidence), meant that the personal data in the unredacted Settlement Deed was particularly sensitive.

    b. The Horizon IT scandal was a widely publicised miscarriage of justice[28], meaning that the Data Subjects were already subject to media and public scrutiny; and

    c. The unredacted Settlement Deed contained names, personal addresses and financial settlement details[29], making individuals potentially vulnerable to fraud, burglary and targeted scams. In its Representations dated 15 September

[28] The Criminal Cases Review Commission (CCRC) called the Horizon IT scandal "*the most widespread miscarriage of justice the CCRC has ever seen*": The CCRC and Post Office/ Horizon cases - Criminal Cases Review Commission

[29] As set out at paragraph 41, the unredacted Settlement Deed included the total financial settlement figure. It did not contain details of the specific sums paid to individual Data Subjects.

2025, the Post Office submitted that the consequences of the 25 April Incident had been overstated by the Commissioner which it considered to be unfair and contrary to the public interest. The Post Office has since clarified, in its representations of 21 November 2025, that it only considered the Commissioner had overstated the *potential for fraud, burglary and targeted scams* arising from the 25 April Incident.

d. The Commissioner has taken these representations into account but finds that the consequences have not been overstated. In light of the nature of the disclosure, the Commissioner considers it reasonable to draw the conclusion that the disclosure on 25 April made the Data Subjects *potentially* vulnerable to fraud, burglary and targeted scams.

49. The factors above indicate that a high level of security was appropriate to the risk presented by the Relevant Processing. The Post Office was required to implement appropriate technical and organisational measures to ensure this high level of security.

Assessment of compliance prior to the 25 April Incident

50. Under Article 5(2) UK GDPR, it is for the Post Office to demonstrate compliance with Article 5(1)(f). Article 24 UK GDPR also requires the Post Office to demonstrate compliance with Articles 32(1) and (2).

51. Paragraphs 29 to 34 above detail the Commissioner's findings of fact in relation to the Post Office's relevant procedures, policies and guidance in place prior to the 25 April Incident.

52. The Commissioner finds that the Post Office breached Articles 5(1)(f) and 32(1) UK GDPR as there is sufficient evidence to demonstrate that, despite the known risks to the rights and freedoms of the Data Subjects, the Post Office failed to implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk. Prior to the 25 April Incident, the Post Office did not have:

    a. any documented policies, procedures or guidance in place in relation to the Corporate Communications Team's role in maintaining the corporate website, including the uploading of documents;

    b. any documented quality assurance or sign off process in place for documents uploaded to the corporate website;

    c. any documented policy, procedure or guidance in place to clarify where and how the Corporate Communications Team should store, label and segregate documents;

    d. a central repository of data for the Corporate Communications Team to save documents to; or

    e. an adequate risk and control register, as the only register the Post Office had in place was neither complete nor accurate, and did not included risks of inadvertently publishing, distributing or sharing confidential / inaccurate information.

53. Indeed, the Post Office's own internal review concluded that their overall control environment was not fit for purpose, and considered there to be fundamental weaknesses in the framework of governance, risk management and control. The Post Office's review

determined that it was more than likely that an incident of a similar nature may occur.[31]

54. The Commissioner concludes that the Post Office did not adequately assess the information risk it faced or assess how valuable, sensitive or confidential the information it held was (as required by Article 32(2) UK GDPR). The Post Office identified that its risk and control register was inadequate (being neither complete nor accurate), and its risk profile was predicated around reputational risks and management.[32] The Post Office did not identify or address the risks of inadvertently publishing, distributing or sharing confidential / inaccurate information.[33]

Assessment of compliance following the introduction of organisational measures

55. Paragraphs 35 to 37 above set out the Commissioner's finding of fact in relation to the procedures, polices and guidance introduced by the Post Office following the 25 April Incident.

56. The Commissioner finds that upon becoming aware of the breach, the Post Office conducted an urgent internal assurance review to identify areas where controls could be strengthened or introduced to mitigate the risk of a similar incident occurring in the future. As a result of this review, the Post Office told the Commissioner that "key themes were identified where improvements could be introduced in the Corporate Affairs team and more widely across the Post Office".[34]

[31] Post Office Internal Assurance review dated 27 June 2024
[32] Post Office Internal Assurance review dated 27 June 2024
[33] Post Office Internal Assurance review dated 27 June 2024
[34] Correspondence from the Post Office to the Commissioner dated 29 November 2024

57. The recommended process and checks were documented in the Communications Corporate Affairs and Brand team data protocols dated July 2024. The risks and controls were documented on 14 November 2024. The Post Office confirmed that all actions were completed by 15 November 2024.

58. The Commissioner finds that by 15 November 2024, the Post Office had implemented appropriate measures to ensure an appropriate level of security of the personal data subject to the Relevant Processing. The Infringements of Articles 5(1)(f) and 32 UK GDPR were therefore remedied by that date.

Duration of the infringements

59. The risk of damage to data subjects (i.e. the potential for an incident such as the 25 April Incident to occur) existed from as early as 31 March 2023, the date when the Horizon webpage was established. The risk materialised on 25 April 2024.

60. The Commissioner finds that by 15 November 2024 the Post Office had implemented appropriate technical and organisation measures to ensure the security of the personal data and prevent the risk which materialised on 25 April 2024 occurring again.

61. The duration of the infringements is the period during which those measures were not in place.

62. The Post Office made representations that it considered the Commissioner's Reprimand to relate only to "*the single incident of the processing of the unredacted deed which led to the 25 April Incident*".

63. In its Representations, the Post Office submitted that if the scope of the investigation was widened to include the systems and controls in place between March 2023 and November 2024 it ought to have been given the opportunity to comment on that specifically. The Commissioner notes that the Post Office had the opportunity to make representations on the reprimand.

64. As explained above, the Commissioner finds that the 25 April Incident arose as a consequence of the Post Office not having appropriate technical and organisational measures in place to ensure the security of the personal data (as required by Articles 5(1)(f) and 32 UK GDPR).

65. The Commissioner has investigated the security failings which led to the 25 April Incident occurring and finds that if the procedures, polices and guidance introduced by the Post Office following the 25 April Incident had been in place when the Horizon Webpage was set up, it is more likely than not the incident could have been avoided.

66. In reaching this conclusion, the Commissioner has considered all the information provided by the Post Office during the course of the investigation and its Representations in response to the NOI.

IV. DECISION TO ISSUE THIS REPRIMAND AND THE PUBLIC SECTOR APPROACH

67. In response to these findings of infringement, the Commissioner has a range of regulatory tools at his disposal including the imposition of administrative penalties, enforcement notices and reprimands.

68. The Commissioner has decided to impose a reprimand on the Post Office in respect of the infringements of Articles 5(1)(f) and 32 UK GDPR.

69. In June 2022, the Commissioner set out a revised approach to public sector enforcement, initially to be trialled over two years. To support this approach, the Commissioner committed to working proactively with senior leaders in the public sector to encourage compliance, prevent harms before they occur, and learn lessons when things have gone wrong.[35] In practice, this means that for the public sector the Commissioner has committed to increasing the use of Reprimands and Enforcement Notices, only issuing monetary penalties in the most egregious cases, that is where the infringements are especially serious.

70. In December 2024, the Commissioner set out the outcome of his two-year trial of this approach. His review noted the positive impact the public sector approach has had in protecting personal data. The Commissioner decided to continue with the public sector approach and provide greater clarity on its parameters.[36]

71. The Commissioner finds the infringements in this case to be serious. The Post Office did not adequately assess the information risk it faced or assess how valuable, sensitive or confidential the information it held was. It is likely that the 25 April Incident would have been avoided if the security measures implemented after that date (none of which required significant resources or expenditure) had been introduced when the Relevant Processing began. Having

[35] https://webarchive.nationalarchives.gov.uk/ukgwa/20220702165657/https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/open-letter-from-uk-information-commissioner-john-edwards-to-public-authorities/

[36] ICO consultation on the revised approach to public sector regulation | ICO; Post-implementation review: Public sector approach trial – September 2024 | ICO

examined all the circumstances of this case and having had regard to the matters set out in Article 83 UK GDPR, the Commissioner initially took the view that it would be appropriate to impose a monetary penalty.

72. However, since June 2022, the Commissioner has adopted the revised approach to public sector enforcement (as outlined above). In following this approach, the Commissioner considered whether the infringements identified in this case were 'egregious' such that they would warrant a monetary penalty being imposed, despite the Post Office's standing as a public sector authority. The Commissioner did not consider the infringements identified reached the threshold of 'egregious'. It was therefore determined, in line with the Commissioner's public sector approach, that a Reprimand should be imposed instead.

73. Had the public sector approach not been in place, the Commissioner considers that a monetary penalty of an amount *up to* £1.094 million would have been deemed appropriate, having taken into account all of the circumstances of the case, the seriousness of the infringements, the aggravating and mitigating factors, along with indicators of the financial position of the Post Office.

74. In its Representations, the Post Office asserted that the inclusion of the monetary penalty figure was contrary to the Commissioner's Data Protection Fining Guidance[37] (the "**Fining Guidance**"). The Post Office submitted that the Commissioner had not followed the Fining Guidance as he had calculated the fine amount despite not deciding to issue a penalty notice. The Commissioner wishes to

[37] Data Protection Fining Guidance | ICO

clarify that his Fining Guidance exists alongside his public sector approach. The Commissioner clearly and publicly explained at the outset of the public sector approach that he would share the value of the fine that would have otherwise been imposed. The Commissioner's open letter to public authorities in 2022 stated: "*We will also do more to publicise these cases, sharing the value of the fine that would have been levied, so there is wider learning*". This approach necessarily involves calculating the amount of the fine that would have been levied, using the Fining Guidance. This approach is entirely consistent with the Commissioner's broader focus of raising data protection standards across the public sector and prioritising other enforcement tools, including reprimands.

75. The Post Office also made Representations disputing the Commissioner's inclusion of the monetary penalty amount that would have been deemed appropriate in the Reprimand. The Post Office submitted that it was not appropriate to include the proposed amount of any monetary penalty when the Post Office had not had the opportunity to make representations on it and the amount would necessarily change between NOI and final decision in any case. The Commissioner is satisfied that it is reasonable to include the value of the fine that could have been imposed, but for the public sector approach. As described above at paragraph 74, this approach is clearly set out in the Commissioner's open letter to public authorities in 2022.

76. The Commissioner notes that the Post Office has had the chance to make representations on the reprimand and given the penalty will not be imposed due to the public sector approach considers

that further detailed representations on the penalty calculation are not required.

77. The Post Office made additional representations on 31 October 2025. These representations were in relation to consistency of approach in the representations process where a monetary penalty is imposed. The Commissioner has considered these representations and acknowledges that the monetary penalty amount included in this reprimand does not reflect any additional discount that may have been applied including in response to representations that the Post Office could have made on the proposed penalty amount, had the public sector approach not been in place.

78. The Post Office submitted in its Representations, that issuing a reprimand in this case would be inconsistent with action taken in other public sector breach cases. The Commissioner has carefully reflected on these representations from the Post Office, has had regard to the regulatory action taken in other public sector breach cases, and does not consider that issuing a reprimand in this case would be inconsistent with the approach taken in other public sector breach cases.

79. Recital 129 UK GDPR, in relation to the enforcement powers of the Commissioner states that "*each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case…*". In reaching a decision as to whether it is appropriate, necessary and proportionate to take enforcement action and issue a reprimand in this case, the Commissioner has

given due consideration to the non-exhaustive criteria set out within the Regulatory Action Policy.[38]

80. The Commissioner considers the Post Office's acknowledgement of the infringements, the remedial measures implemented, the steps taken to mitigate damage to Data Subjects (including those additionally raised by the Post Office in its Representations), and the compensation paid to the majority of Data Subjects by the Post Office in respect of the 25 April Incident[39], do not outweigh the seriousness of the infringements. Accordingly, the Commissioner has decided that it would be appropriate to issue a Reprimand to the Post Office in relation to the Infringements of Articles 5(1)(f) and 32 UK GDPR. The Commissioner considers that this course of action is necessary, appropriate, proportionate, and in the public interest.

Dated:2 December 2025

Signed: 

Sally Anne Poole

Head of Investigations

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

[38] Regulatory Action Policy
[39] The Post Office confirmed to the ICO on 30 April 2025 that compensation payments had so far been made to 440 Data Subjects.