NON-CONFIDENTIAL
FOR PUBLICATION

MONETARY PENALTY NOTICE

South Staffordshire Plc

South Staffordshire Water Plc

Penalty Notice to South Staffordshire Plc & South Staffordshire Water Plc under Section 155(1) Data Protection Act 2018

7 May 2026

NON-CONFIDENTIAL
FOR PUBLICATION

Contents

NON-CONFIDENTIAL
FOR PUBLICATION

DATA PROTECTION ACT 2018

(PART 6, SECTION 155)

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

PENALTY NOTICE

To: South Staffordshire Plc and South Staffordshire Water Plc

Of: Green Lane
Walsall
West Midlands
WS2 7PD

FAO: [redacted]

I. INTRODUCTION AND SUMMARY

1. Pursuant to section 155(1)(a) of the Data Protection Act 2018 ("**DPA 2018**"), by this written notice ("**Penalty Notice**"), the Information Commissioner (the "**Commissioner**") requires South Staffordshire Plc & South Staffordshire Water Plc (together, "**South Staffordshire**") to pay the Commissioner a penalty of **£963,900**.

2. This Penalty Notice is issued in respect of the Commissioner's findings of infringement of Article 5(1)(f) and Article 32(1) of the UK General Data Protection Regulation[1] ("**UK GDPR**") (the "**Infringements**)".

[1] 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 11 September 2020 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.

3. This Penalty Notice sets out the Commissioner's conclusions and the reasons why the Commissioner has decided to impose a penalty, including the circumstances of the Infringements and the nature of the personal data involved.

4. This Penalty Notice concerns failings identified by the Commissioner following an investigation into South Staffordshire arising out of a cyber-attack incident which began on 11 September 2020. Following correspondence between the Commissioner and South Staffordshire, the parties entered into settlement discussions to attempt to resolve this investigation. In line with the process set out in section 11.4.1 of the Commissioner's draft Data Protection Enforcement Procedural Guidance[2], the Commissioner provided South Staffordshire with a statement of facts including draft penalty calculation ("**Initial Statement of Facts**") on 18 December 2025. On 30 January 2026, South Staffordshire provided the Commissioner with written representations on the Initial Statement of Facts. The Commissioner provided an updated statement of facts including penalty calculation to South Staffordshire on 13 March 2026 ("**Updated Statement of Facts**"), which reflected South Staffordshire's written representations to the extent considered appropriate by the Commissioner.

5. South Staffordshire entered into a voluntary settlement agreement with the Commissioner on 23 April 2026. South Staffordshire has made full admissions in relation to the Commissioner's findings of infringement as set out in this Penalty Notice and has agreed to pay

[2] Draft Data protection enforcement procedural guidance – This draft guidance was published for public consultation on 31 October 2025. The consultation window closed on Friday 23 January 2026. The draft guidance has not yet been finalised.

a penalty of **£963,900**. As part of this settlement, South Staffordshire has agreed not to appeal this Penalty Notice.

6. The penalty referred to at paragraph 5 of this Penalty Notice includes a reduction to reflect the voluntary settlement with the Commissioner.

II. RELEVANT LEGAL FRAMEWORK

7. Section 115 of the DPA sets out the Commissioner's general functions under the UK GDPR. The DPA contains enforcement provisions in Part 6 which are exercisable by the Commissioner.

8. Section 155(1) of the DPA confers power on the Commissioner to issue a penalty notice where he is satisfied that a person has failed or is failing in the manner described in section 149(2). It provides that:

"*(1) If the Commissioner is satisfied that a person—*
(a) has failed or is failing as described in section 149(2) …,
the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice."

9. The failures identified in section 149(2) DPA are, insofar as relevant here:

"*The first type of failure is where a controller or processor has failed, or is failing to comply with any of the following –*

a provision of Chapter II of the UK GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);[3]

…

a provision of Articles 25 to 39 of the UK GDPR or section 64 or 65 of this Act (obligations of controllers and processors)…"[4]

10. The relevant substantive provisions of the UK GDPR are set out in **Section IV** of this Penalty Notice. The legal framework on setting penalties is set out in **Section V** of this Penalty Notice.

III. BACKGROUND TO THE INFRINGEMENTS

1) Background to South Staffordshire's processing of personal data

11. South Staffordshire Plc is an integrated services group that operates a regulated water company, South Staffordshire Water Plc. The group also operates a range of complementary non-regulated businesses that serve essential services markets in the UK.[5]

12. South Staffordshire Water Plc supplies clean water to approximately 1.6 million people in parts of Staffordshire, the West Midlands, surrounding counties and Cambridge.[6]

[3] As relevant to this case, the specific provision of Chapter II of the UK GDPR is Article 5(1)(f) UK GDPR.
[4] As relevant to this case, the specific provision of Chapter II of the UK GDPR is Article 32(1) UK GDPR.
[5] South Staffordshire follow-up breach report, 18 August 2022, page 2.
[6] South Staffordshire follow-up breach report, 18 August 2022, page 2.

13. South Staffordshire Plc is, through two intermediate companies, a parent company of South Staffordshire Water Plc.[7]

14. During the period 11 September 2020 to 4 August 2022 (the "**Relevant Period**"), South Staffordshire Water Plc and South Staffordshire Plc (together, "**South Staffordshire**") stored the personal data[8] of customers and employees in a corporate network and information system (the "**IT environment**"). Customers' personal data was stored in order to supply clean water to those individuals and their households. Employees' personal data was stored in order to manage and administer the employment of those individuals.[9] The personal data was stored on infrastructure physically located at South Staffordshire's data centre in Walsall.[10] This storage is the relevant processing with which this Penalty Notice is concerned (the "**Relevant Processing**").

15. South Staffordshire Water Plc and South Staffordshire Plc were controllers of personal data in respect of the Relevant Processing.[11]

16. The personal data subject to the Relevant Processing related to approximately 1.85 million customers (750,000 current, 1.1 million

[7] Annual Report and Financial Statements 2023/24 - South Staffordshire Plc (accessed 18 December 2025), page 155.
[8] In this Penalty Notice, terms such as "controller", "personal data", "processing" and "personal data breach" have the same meaning as in Article 4 UK GDPR.
[9] Letter from DLA Piper UK LLP, 10 November 2022, data subject notification template; Letter from DLA Piper UK LLP, 27 January 2023, Annex 1 Data Scoping Analysis Paper, page 6; Letter from DLA Piper UK LLP, 8 November 2022, response to questions 3(b); Letter from DLA Piper UK LLP, 16 September 2022, template DSAR letters; Letter from DLA Piper UK LLP, 27 January 2023, Annex 1 Data Scoping Analysis Paper, page 6.
[10] Letter from DLA Piper UK LLP, 16 September 2022, network topology.
[11] Letter from DLA Piper UK LLP, 23 May 2023.

former), 2,791 current employees, and at least 2,298 former employees.[12]

17. Categories of personal data not subject to the Relevant Processing (i.e. which were not stored in the IT environment) include:

    a) customer payment card data;

    b) employee health data (e.g. occupational health/ return to work/ absence from work).[13]

2) Cyber-attack incident

18. On 15 July 2022 South Staffordshire observed marked IT performance issues and commenced an investigation. This investigation identified anomalous server and database performance and unscheduled database exports. On 19 July 2022, South Staffordshire instructed its outsourced security service provider to support its investigation. This identified that South Staffordshire had been subject to a cyber-attack (the "**Incident**"[14]), with the threat actor using the Cobalt Strike tool on a number of devices to provide communication and control. On 21 July 2022 South Staffordshire became aware of malicious code in the IT environment.[15]

19. South Staffordshire's investigation found that initial access occurred on 11 September 2020 through a successful phishing campaign. The

[12] Letter from DLA Piper UK LLP, 5 August 2022, page 3; South Staffordshire follow-up breach report, 18 August 2022, pages 12 and 13; Letter from DLA Piper UK LLP, 27 January 2023, data analysis scoping paper, pages 3-4; Letter from DLA Piper UK LLP, 30 November 2023, page 3.
[13] Letter from DLA Piper UK LLP, 27 January 2023, Annex 1 data scoping analysis paper, pages 6 and 8.
[14] The "Incident" refers to the cyber-attack which began on 11 September 2020, when the threat actor initially compromised South Staffordshire's IT environment, and appears to have ended on 4 August 2022, following which no further activity from the threat actor was observed.
[15] River Forensic Investigation Findings Report, 4 November 2022, page 2.

opening of the malicious attachment to a phishing email led to the installation of the tool Get2 and the Remote Access Trojan, SDBBOT, which was used to establish persistence on the endpoint. The threat actor is understood to have remained dormant, albeit with potential access to the network, until 17 May 2022, following which they began to move laterally within the network. The threat actor was identified as having accessed twenty different endpoints between 17 May 2022 and 4 August 2022, the date of the last observed activity by the threat actor on the IT environment.[16]

20. South Staffordshire reported a personal data breach to the ICO on 24 July 2022.

21. On 26 July 2022, South Staffordshire discovered a ransom note that the threat actor had unsuccessfully attempted to distribute to certain staff.[17] In that ransom note, the threat actor claimed to have exfiltrated 5.5TB of data.[18]

22. No threat actor activity was observed on the IT environment after 4 August 2022.[19]

23. Between 25 August 2022 and 18 November 2022, South Staffordshire detected an approximate total of 4.121 TB of exfiltrated data published on the dark web.[20]

24. The 4.121 TB of published data included the personal data of approximately 633,887 UK data subjects. This comprised current customers, former customers, individuals on the Priority Services Register, current employees and former employees.[21]

[16] River Forensic Investigation Findings Report, 4 November 2022, page 4
[17] River Forensic Investigation Findings Report, 4 November 2022, pages 3 and 23.
[18] River Forensic Investigation Findings Report, 4 November 2022, page 23.
[19] Letter from DLA Piper UK LLP, 26 January 2024.
[20] Letter from DLA Piper UK LLP, 27 January 2023, page 1.
[21] Letter from DLA Piper UK LLP, 25 July 2024.

25. The following categories of personal data were published on the dark web:

    a) personal details (full name, physical address and email address, date of birth/age, gender, telephone number);

    b) for employees only, HR information (employee number, applicant number, National Insurance number, username and password);

    c) for customers only, account information (customer reference number, property information including occupant information, bank account number and sort code, financial status information, Priority Services data, username and password);[22]

    d) for a small percentage of customers on the Priority Services Register, information from which disabilities could be inferred.[23]

    Not all data subjects who had personal data exfiltrated and published would have had personal data falling into every category set out above.

26. The data published on the dark web also included race/ethnicity data relating to one former customer and religion/philosophical belief data relating to one former customer.[24]

[22] Letter from DLA Piper UK LLP, 26 January 2024, response to question 2. South Staffordshire Water Plc's Priority Services Register seeks to help those with a medical, learning or physical disability, or those who are struggling financially. This includes hands on help in an emergency, and a braille bill, large print bill and information service. (South Staffordshire Water Plc Priority Services Register leaflet, https://www.south-staffs-water.co.uk/media/wiyevlxb/vulnerability-leaflet_final_ssw_web_4.pdf, accessed 9 December 2025).
[23] Email from DLA Piper UK LLP, 24 September 2022; Letter from DLA Piper UK LLP, 7 October 2022, page 2; Letter from DLA Piper UK LLP, 16 December 2022, pages 2-3.
[24] Letter from DLA Piper UK LLP, 30 January 2026

27. The Incident constituted a personal data breach (as it involved unauthorised access to personal data and unauthorised disclosure of personal data).

28. Following an analysis of the published personal data, South Staffordshire notified 390,628 data subjects of the personal data breach. Data subjects were notified where South Staffordshire considered there were good grounds for supposing that Article 34 UK GDPR was engaged. The vast majority of those notifications consisted of the following:

    a) September 2022 - 2,791 notifications to all individuals who were employed at the time of the incident due to the inclusion of payroll information and other HR related information within the dataset;

    b) September 2022 - 2,298 notifications to a subset of former staff members who had left the business before the incident due to the inclusion of payroll data within the dataset, and to pensioners;

    c) November 2022 – 315,992 notifications to a subset of customers for which bank account, sort code and current address was published within the published personal data, due to the risk of direct debit fraud;

    d) January 2023 – 69,116 notifications to customers whose information was included in a version of the Priority Services Register database contained within the published personal data and who were not included in the cohort of customers notified in November 2022.[25]

[25] Letter from DLA Piper UK LLP, 26 January 2024, response to question 1.

29. South Staffordshire provided all current employees and those current customers it had notified with a free 12-month subscription to a credit monitoring service, to assist in identifying any potentially fraudulent activity. South Staffordshire set up a dedicated helpline to answer any questions which notified current customers might have about the publication of personal data. HR surgeries were set up for current employees to discuss any questions or concerns.[26]

IV. INFRINGEMENTS

30. The Commissioner has concluded that during the Relevant Period, South Staffordshire infringed Article 5(1)(f) and Article 32(1) UK GDPR for the reasons set out below.

1) Legal framework

31. Article 5(1)(f) UK GDPR provides:

"*Personal data shall be … processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*"

32. Article 32(1) UK GDPR provides:

"*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, including inter alia as appropriate:*

[26] Letter from DLA Piper UK LLP, 7 September 2022, response to question 11; South Staffordshire draft consumer notification, 10 November 2022.

(a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

2) Technical and organisational measures

33. During the Relevant Period, South Staffordshire failed to:

    a) properly implement the principle of least privilege[27];

    b) implement adequate security monitoring and logging[28];

    c) migrate away from certain devices running obsolete software[29]; and

    d) implement adequate vulnerability management[30]

    in the IT environment.

34. Paragraphs 35 to 43 below explain each of these measures and set out relevant industry standards.

Principle of least privilege

[27] Letter from DLA Piper UK LLP, 27 January 2023, annex 8, item 13; Letter from DLA Piper UK LLP, 8 March 2023, response to question 4(d).
[28] Letter from DLA Piper UK LLP, 8 March 2023, annex 6; Letter from DLA Piper UK LLP, 27 January 2023, response to questions 9 and 10; River Forensic Investigation Findings Report, 4 November 2022, page 2.
[29] Letter from DLA Piper UK LLP, 27 January 2023, annexes 14 and 15; Letter from DLA Piper UK LLP, 8 March 2023, response to question 1.
[30] Letter from DLA Piper UK LLP, 8 March 2023, response to question 8; Letter from DLA Piper UK LLP 27 January 2023, responses to questions 13(b) and (d).

35. The National Cyber Security Centre ("**NCSC**")'s "*Preventing Lateral Movement*" guidance recommends that the principle of 'least privilege' (where accounts and users have the minimum amount of access needed to perform their role) should be implemented wherever possible. This guidance further explains that a tiering model for administrative accounts ensures they only have access to the specific administrative capabilities needed, rather than all of them. Using various tiers of administrative accounts limits the number of very high privileged accounts in use, and reduces the access an attacker gains if a lower privilege administrator account is compromised.[31]

36. During the Relevant Period, South Staffordshire failed to properly implement the principle of least privilege and specifically Active Directory tiering in the IT environment.[32] The threat actor was able to move laterally across the environment with a Domain Administrator account, making extensive use of Remote Desktop Protocol (RDP) and logging onto multiple endpoints with this account. Therefore, by not properly implementing the principle of least privilege and a tiered approach to network infrastructure, the threat actor faced limited resistance in pursuit of their goals.

Security monitoring and logging

37. The NCSC's device security guidance explains that "*Security monitoring is central to the identification and detection of threats to your IT systems.*"[33]

[31] https://www.ncsc.gov.uk/guidance/preventing-lateral-movement (accessed 17 December 2025)
[32] Letter from DLA Piper UK LLP, 27 January 2023, annex 8, item 13.
[33] https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/logging-and-protective-monitoring (accessed 9 December 2025)

38. The United States National Institute of Standards and Technology's (NIST) Computer Security Incident Handling Guide includes a key recommendation that incident handlers: "*Require a baseline level of logging and auditing on all systems, and a higher baseline level on all critical systems.*"[34]

39. During the Relevant Period, South Staffordshire failed to implement adequate security monitoring and logging. For instance, in December 2021, a third-party security operations centre was monitoring only 5% of the IT environment.[35] The IT environment also had limited logging.[36] Endpoint telemetry and logging were not integrated into South Staffordshire's security incident and event monitoring platform.[37]

Obsolete software

40. The NCSC's device security guidance includes the following in relation to obsolete products: "*All software, including device operating systems, will eventually become out of date. Ideally, once out of date, technology should not be used. … The only fully effective way to mitigate this risk is to stop using the obsolete product.*"[38]

41. During the Relevant Period, South Staffordshire failed to migrate away from devices running obsolete software, such as Windows Server 2003 Release 2, an end-of-life operating system.[39] Extended support Windows Server 2003 ended in July 2015 and it was

[34] NIST Special Publication (SP) 800-61 Revision 2, published August 2012 and withdrawn April 2025. https://csrc.nist.gov/pubs/sp/800/61/r2/final (accessed 9 December 2025).
[35] Letter from DLA piper UK LLP, 8 March 2023, annex 6.
[36] River Forensic Investigation Findings Report, 4 November 2022, page 2.
[37] Letter from DLA Piper UK LLP, 27 January 2023, responses to questions 9 and 10.
[38] https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/logging-and-protective-monitoring (accessed 9 December 2025)
[39] Letter from DLA Piper UK LLP, 27 January 2023, annexes 14 and 15; Letter from DLA Piper UK LLP, 8 March 2023, response to question 1.

documented at this time that continuing to run this system could result in security risks.[40]

Vulnerability management

42. A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack. Vulnerabilities can occur through flaws, features, or user error, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal.[41]

43. During the Relevant Period, South Staffordshire failed to implement adequate vulnerability management. As at May 2022, two domain controllers in the IT environment were unpatched against the ZeroLogon vulnerability (CVE-2020-1472), which was first published in August 2020 and which allows for the rapid escalation of privileges. While it is noted that the Incident did not occur as a result of this vulnerability, the vulnerability was exploited by the threat actor during the Incident.[42] Further, when asked to provide reports of any external vulnerability scans of the IT estate conducted during and/ or after September 2020 and prior to May 2022, South Staffordshire responded "*There are no external vulnerability scans of the SSW IT estate conducted between September 2020 and May 2022 to provide.*" Similarly, when asked to provide reports of any internal vulnerability scans of the IT estate conducted during the same period, South Staffordshire responded: "*There are no internal vulnerability*

[40] https://www.microsoft.com/en-us/windows-server/blog/2015/07/14/migration-is-worth-it-support-for-windows-server-2003-ends-today
[41] https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities (accessed 9 December 2025).
[42] Letter from DLA Piper UK LLP, 27 January 2023, responses to questions 13(b) and (d).

scans conducted between September 2020 and May 2022 to provide."[43]

3) Summary of the Commissioner's findings on infringements

44. The failures at paragraph 33 constitute infringements of Articles 5(1)(f) and 32(1) UK GDPR in respect of the Relevant Processing, during the Relevant Period.

45. The Commissioner notes that, on 30 November 2023, South Staffordshire shared a letter with the Commissioner in which it admitted having infringed Articles 5(1)(f) and 32 UK GDPR.[44]

V. DECISION TO IMPOSE A PENALTY

46. When deciding whether to issue a penalty notice to a person, and when determining the appropriate amount of the penalty, in respect of matters to which the UK GDPR applies, section 155(2)(a) DPA 2018 requires the Commissioner to have regard to the matters listed in Article 83(1) and (2) UK GDPR, in so far as they are relevant in the circumstances of the case.

47. Article 83(1) UK GDPR requires any penalty imposed by the Commissioner to be effective, proportionate and dissuasive in each individual case.

48. Article 83(2) UK GDPR requires the Commissioner to have due regard to the following factors when determining whether to issue a penalty notice and the appropriate amount of any such penalty in each individual case:

[43] Letter from DLA Piper UK LLP, 8 March 2023, response to question 8.
[44] Letter from DLA Piper UK LLP, 30 November 2023.

a) the nature, gravity and duration of the infringement, taking into account the nature, scope, context and purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them;

b) the intentional or negligent character of the infringement;

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

e) any relevant previous infringements by the controller or processor;

f) the degree of cooperation with the Commissioner in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the manner in which the infringement became known to the Commissioner, in particular whether and, if so, to what extent the controller or processor notified the infringement;

i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

49. The Commissioner has had regard to each of these factors and has set out his analysis in relation to these issues in the 'Calculation of the Penalty' section of this Penalty Notice at **Section VI**. Following his consideration of those factors, the Commissioner has determined that the Infringements are sufficiently serious to warrant a monetary penalty. Specifically, the Commissioner has decided to impose a single penalty of **£963,900** on South Staffordshire in respect of the Infringements in accordance with section 155(1)(a) DPA 2018.

50. The Commissioner has also considered the requirement to ensure that the imposition of an administrative fine shall be effective, proportionate and persuasive.

51. The Commissioner finds that the imposition of a penalty would, in the circumstances of this case, be an effective means of ensuring compliance with the UK GDPR, sanctioning the Infringements and would also be dissuasive against future non-compliance.

52. The Commissioner also finds that a penalty would be a proportionate regulatory response and would not exceed what may be considered appropriate and necessary in all the circumstances of the case, including in particular the seriousness of the infringements, the number of data subjects affected and the duration of the infringements.

53. In reaching his conclusion, the Commissioner has also had regard to the desirability of promoting economic growth, as required under section 108 of the Deregulation Act 2015 and the desirability of promoting innovation and competition, as required by section

120B(a) and (b) DPA 2018 respectively. However, the Commissioner is mindful that the desirability of promoting economic growth, innovation and competition does not legitimise non-compliance with data protection law. Furthermore, non-compliant activity or behaviour harms the interests of legitimate businesses that are working to comply with data protection law, which disrupts competition and acts as a disincentive to invest in compliance.[45]

VI. CALCULATION OF THE PENALTY

54. In line with the ICO's Data Protection Fining Guidance[46], the proposed penalty of **£963,900** has been calculated as follows.

1) Relevant statutory maximum

55. South Staffordshire has admitted an infringement of Article 5(1)(f) UK GDPR. Pursuant to Article 83(5) UK GDPR, this is subject to a maximum penalty of the higher of £17.5 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover in the preceding financial year.

56. For the purposes of the calculation, the Commissioner has assessed the turnover of the undertaking comprising South Staffordshire Plc and its subsidiaries. This undertaking is referred to as the "Group" in South Staffordshire Plc's *Annual Report and financial statements*, for the year ended 31 March 2024.[47] Those financial statements report a Group consolidated turnover of approximately £385 million.

[45] Data Protection Fining Guidance | ICO, paragraph 105.
[46] Data Protection Fining Guidance | ICO
[47] Annual Report and Financial Statements 2023/24 - South Staffordshire Plc (accessed 18 December 2025), page 155.

57. As this figure is below the threshold at which a turnover-based maximum becomes applicable, the relevant statutory maximum of £17.5m applies.

58. Article 83(3) UK GDPR provides:

"*If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.*"

59. The Commissioner considers that the infringements in this case arise from the same or linked processing operations. Having considered the nature of the Relevant Processing and the infringements, the Commissioner proposes to impose a single penalty. This penalty will not exceed the maximum penalty available for the gravest infringement, i.e. £17.5m in respect of the infringement of Article 5(1)(f) UK GDPR.

2) Step 1: Assessment of the seriousness of the infringements

60. The Commissioner has determined a starting point of 15% to reflect the infringements being within the medium seriousness category. In proposing this starting point, the Commissioner has had regard to the following:

a) As regards the nature of the infringements, the infringement of Article 5(1)(f) is subject to the higher maximum fine[48], reflecting its seriousness. An infringement of Article 32(1) UK GDPR is subject to the standard maximum amount.[49]

[48] £17,500,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(5) UK GDPR).
[49] £8,700,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(4) UK GDPR)

b) In assessing the gravity of the infringements, the Commissioner has considered the nature, scope and purpose of the Relevant Processing, as well as the number of data subjects affected and the level of damage they have suffered:

- Nature of the processing: The Relevant Processing was carried out in the context of business activities. For a small percentage of customers on South Staffordshire's Priority Services Register, the Relevant Processing involved the personal data of vulnerable people who needed extra support to protect themselves;[50]
- Scope of the processing: The Relevant Processing relates to data subjects in parts of Staffordshire, the West Midlands, surrounding counties and Cambridge.[51] The Relevant Processing related to approximately 1.85 million customers (750,000 current, 1.1 million former), 2,791 current employees and at least 2,298 former employees. However, not all of these data subjects had personal data exfiltrated during the Incident. Specifically, 633,887 UK data subjects were affected by exfiltration of personal data during the Incident;
- Purpose of the processing: The purpose of the Relevant Processing was to provide clean water to customers and to manage and administer employment relationships. This was central to South Staffordshire's main business and commercial activities;

[50] Letter from DLA Piper UK LLP, 7 October 2022, page 2; Letter from DLA Piper UK LLP 16 December 2022, page 2.
[51] South Staffordshire follow-up breach report, 18 August 2022, page 2.

- Number of data subjects affected: The Relevant Processing related to (and the infringements therefore potentially affected) approximately 1.85 million customers (750,000 current customers, 1.1 million former customers), 2,791 current employees and at least 2,298 former employees. The Incident resulted in the unauthorised disclosure and publication on the dark web of personal data of approximately 633,887 data subjects. South Staffordshire notified 390,628 data subjects of the personal data breach;
- Level of damage suffered: For the purposes of the Commissioner's regulatory assessment, the publication of personal data on the dark web is assumed to be capable of giving rise to loss of control over personal data and a risk of harm to affected data subjects. The Commissioner has received complaints from data subjects detailing that they have suffered distress as a result of the publication of their personal data on the dark web. These complaints have not been interrogated by the Commissioner.

c) The duration of the infringements was from 11 September 2020 to 4 August 2022. It is noted that the threat actor is understood to have remained dormant on South Staffordshire's IT environment, without detection, from 11 September 2020 until 17 May 2022, following which they began to move laterally within the network.

d) The infringements are considered to be negligent in character.

e) The categories of personal data affected by the infringements are set out at paragraph 25 above. In particular, the Commissioner has considered the following:

- Only a very small subset of data subjects had special category data published on the dark web, comprising personal data revealing racial or ethnic origin relating to only one former customer, personal data revealing religious or philosophical belief relating to only one former customer, and for a small percentage of customers on the Priority Services Register, information from which disabilities could be inferred);[52]
- The categories also include sensitive personal data such as financial data (bank account number and sort code), noting however that customer card data was not included. For some customers on the Priority Services Register, financial hardship information was also affected.[53]

3) Step 2: Accounting for turnover

61. Taking into account South Staffordshire plc's turnover of £385 million for the year ended 31 March 2024, the Commissioner considers that an adjustment of 85% is appropriate to reflect the size of the undertaking.

4) Step 3: Calculating the starting point

62. The starting point is **£2,231,250** (£17.5 million x 0.15 x 0.85).

[52] Email from DLA Piper UK LLP, 24 September 2022; Letter from DLA Piper UK LLP, 7 October 2022, page 2; Letter from DLA Piper UK LLP, 16 December 2022, pages 2-3.
[53] Email from DLA Piper UK LLP, 24 September 2022.

5) Step 4: Aggravating and mitigating factors

63. A **20%** reduction (**£446,250**) is proposed to reflect South Staffordshire's:

    a) degree of cooperation with the ICO's investigation (which includes pro-actively communicating an admission of infringement of Articles 5(1)(f) and 32 UK GDPR during the course of the investigation[54]);

    b) actions to pro-actively report the personal data breach to the NCSC and other relevant bodies;

    c) actions to mitigate the damage suffered by data subjects (set out at paragraph 29 above).

64. Subtracting this figure from the starting point of **£2,231,250** provides a figure of **£1,785,000**.

6) Step 5: Adjustment to ensure the fine is effective, proportionate and dissuasive

65. The Commissioner has considered all of the relevant circumstances of this case including the seriousness of the infringements, the mitigating factors, South Staffordshire's size and financial position and the need for effective deterrence. [redacted]

[54] Letter from DLA Piper UK LLP, 30 November 2023.

[redacted]

[55] Email from DLA Piper UK LLP, 24 September 2022

[redacted]

69. [redacted] the Commissioner has chosen to exercise his discretion and apply a reduction of **10%** (**£178,500**) to the penalty. This results in a penalty of **£1,606,500** which the Commissioner considers represents an effective, proportionate and dissuasive response to the infringements.

7) Settlement discount

70. Taking into account all of the circumstances of this case including the early stage of settlement (prior to a notice of intent being issued) and the resource savings involved, the Commissioner considers it appropriate to apply a settlement discount of **40%**, i.e. **£642,600.** The discount reduces the penalty to **£963,900**.

VII. FINANCIAL HARDSHIP

71. The *Fining Guidance* outlines that, in exceptional circumstances, the Commissioner may reduce a penalty where an organisation is unable to pay due to its financial position.

72. South Staffordshire has not made any claim of financial hardship.

VIII. PAYMENT OF THE PENALTY

73. The penalty must be paid to the ICO by BACS transfer or cheque by 5 June 2026 or in accordance with the terms of any agreed payment plan.

74. Pursuant to paragraph 9(1) of Schedule 16 to the DPA 2018, the Commissioner cannot take action to recover a penalty unless:

    a) the period specified in this Penalty Notice (i.e. by 5 June 2026) has ended;

    b) any appeals against this Penalty Notice have been decided or otherwise ended;

    c) if this Penalty Notice has been varied, any appeals against the penalty variation notice have been decided or otherwise ended; and

    d) the period for appealing against this Penalty Notice, and any variation of it, has ended.

75. Under paragraph 9(2) of Schedule 16 to the DPA 2018, in England and Wales, the Commissioner is able to enforce the payment of the penalty. The penalty is recoverable:

    a) if the County Court so orders, as if it were payable under an order of that court; or
    b) if the High Court so orders, as if it were payable under an order of that court.

IX. RIGHTS OF APPEAL

76. There is a right of appeal to the First-tier Tribunal (Information Rights) pursuant to section 162 DPA 2018 against:

    a) The imposition of the penalty; and/or

b) The amount of the penalty specified in the penalty notice.

77. Information about the appeals process is set out in **Annex 1** to this Penalty notice. Any notice of appeal should be sent or delivered to the Tribunal so that it is received within 28 days of the date of this Penalty Notice.

78. South Staffordshire has admitted the Infringements, agreed to pay the penalty specified in this Penalty Notice and has agreed not to appeal this Penalty Notice.

Dated 7 May 2026

Jennifer Ackers

Director (Enforcement and Investigations)

Information Commissioner's Office

Wycliffe House, Water Lane

Wilmslow, Cheshire

SK9 5AF

NON-CONFIDENTIAL
FOR PUBLICATION

ANNEX 1

DATA PROTECTION ACT 2018 (PART 6, SECTION 162)

RIGHTS OF APPEAL

1. Section 162(1) of the Data Protection Act 2018 gives any person upon whom a penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:

   a) that the notice or decision against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently,

   the Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.

3. You may bring an appeal by sending notice of appeal to the Tribunal at:

   grc@justice.gov.uk

   or

   General Regulatory Chamber
   HM Courts and Tribunals Service
   PO Box 11230
   Leicester
   LE1 8FQ
   UK
   Telephone: 0300 123 4504

4. The notice of appeal should be received by the Tribunal within 28 days of the date of this Penalty Notice (which is the date that this Penalty Notice was sent).

5. If your notice of appeal is late, the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule.

6. The notice of appeal must include at least:

   a) Your name and address;

   b) the name and address of your representative (if any);

   c) an address where documents may be sent or delivered to you;

   d) the name and address of the respondent (the Information Commissioner);

   e) details of the decision to which the proceedings relate;

   f) the result that you are seeking;

   g) the grounds on which you rely;

   h) a full copy of this Penalty Notice; and

   i) (if the notice of appeal is late) a request for an extension of time, giving the reason(s) why the notice of appeal is late and why the Tribunal should accept it.

7. Before deciding whether or not to appeal, you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct their case themselves, or may be represented by any person whom they may appoint for that purpose.

8. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the DPA 2018 and The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules (Statutory Instrument 2009 No. 1976 (L.20)).