Data protection complaints procedure

Northfield Services Ltd

How to raise a complaint and what to expect from Northfield Services Ltd

0. Document control

Document reference	DP-COM-001	**Version**	1.1
Document owner	Privacy Lead	**Approved by**	Operations Director
Approval date	6 August 2026	**Effective date**	6 August 2026
Next review	6 August 2027	**Review frequency**	At least annually
Status	Controlled procedure	**Classification**	Public
Rule pack	2026.07.31	**Sources reviewed**	6 August 2026
Review triggers	Material legal, regulatory, organisational, channel, incident or assurance change		
Related documents	Privacy notice; data rights request procedure; personal data breach response plan; retention schedule; records of processing; safeguarding procedure		
Internal review owner	Privacy Lead		
Internal review target	Organisation-defined		

Tailoring required. Sample document. This procedure uses fictional details and must be tailored, approved and implemented before use. It does not determine whether data protection law has been infringed or whether compensation is due. Replace the fictional details, confirm every organisation control and complete formal approval before use.

Version history

Version	Date	Author	Approved by	Change and rationale
1.0	2 August 2026	Privacy Lead	Operations Director	First approved sample issue following commencement of section 164A of the Data Protection Act 2018.
1.1	6 August 2026	Privacy Lead	Operations Director	Expanded controlled-procedure structure, legally separated complaint and rights-request timeframes, and added deterministic annex data.

Contents

Procedure overview

Step	Action	What happens
1	**Receive and preserve**	Record the date, time, channel and the complainant's own words.
2	**Acknowledge**	Acknowledge receipt no later than the adjusted 30-day deadline.
3	**Triage**	Identify urgent harm, a possible breach, a rights request and other linked processes.
4	**Plan and investigate**	Confirm the complaint points, gather relevant evidence and record the enquiries made.
5	**Keep informed**	Give meaningful progress information and explain any material delay.
6	**Decide and respond**	Explain the finding on each complaint point, the reasons and any action.
7	**Close and improve**	Record delivery, complete actions, set retention and review lessons learned.

How to complain

A person may complain to Northfield Services Ltd through any reasonable channel. They do not have to use a particular form.

Channel	Contact details
Email	privacy@northfield.example
Online	northfield.example/privacy-complaints
Telephone	0117 000 0000
Post	Data Protection Complaints, Northfield Services Ltd, 1 Northfield Square, Bristol BS1 1AA
Other channels	Email, online form, post, telephone, social media, in person and any other reasonable channel.

Tell us if you need information in another format, an interpreter or another reasonable adjustment.

1. Purpose

This procedure explains how Northfield Services Ltd receives, investigates and responds to complaints from people who consider that our handling of their personal information may have infringed UK data protection law.

It provides a consistent, fair and documented process and supports evidence of the enquiries, decisions and actions taken.

It must be read with the organisation's rights-request, personal data breach, retention, safeguarding and relevant sector procedures.

2. Scope

This procedure applies where a data subject considers that, in connection with personal data relating to them, there is an infringement of the UK GDPR or Part 3 of the Data Protection Act 2018.

It covers complaints from customers, workers, former workers, job applicants, website visitors, suppliers, service users and other people whose personal information Northfield Services Ltd handles as controller, including complaints made by an authorised representative.

A complaint may be oral or written and may arrive through any reasonable channel. It does not need to use the word complaint or quote legislation.

General service complaints, worker grievances, whistleblowing disclosures, freedom of information requests and sector complaints follow their own routes. Any data protection element remains linked and is handled under this procedure without unjustified delay.

A communication may also contain a data rights request, personal data breach, safeguarding issue, fraud concern or legal claim. Each applicable process keeps its own record, owner and timetable.

Scope and routing

Matter	Route
Data protection complaint	Open and manage this procedure.
Data subject rights request	Open a separate linked rights-request record and calculate its deadline independently.
Suspected personal data breach	Open the breach response process immediately and keep the complaint open.
General service, grievance or sector complaint	Route the non-data-protection issues separately without delaying the data protection outcome.
Law-enforcement processing	Confirm the Part 3 DPA 2018 route and tailor competent-authority controls.

3. Legal and regulatory framework

Section 164A of the Data Protection Act 2018 is the core complaint-handling provision. The related provisions below apply only where the facts engage them.

The controller must facilitate complaints, acknowledge receipt within 30 days, take appropriate steps to respond without undue delay, make enquiries to the extent appropriate, keep the complainant informed and communicate the outcome.

The organisation must not treat the time limit for a data rights request as the final-response deadline for a complaint.

Framework and operational relevance

Source	Operational relevance
DPA 2018 section 164A	Direct complaint route, acknowledgement, enquiries, progress and outcome.
DPA 2018 sections 165, 167 and 168	ICO complaint, court remedy and compensation routes.
UK GDPR Articles 5 and 24	Accountability and appropriate organisational measures.
UK GDPR Articles 12 to 22D	Separate data subject rights where a complaint also contains a request.
UK GDPR Articles 26 and 28	Joint-controller and processor arrangements where engaged.
UK GDPR Articles 33 and 34	Personal data breach assessment and notification where engaged.
DPA 2018 Part 3	Competent-authority law-enforcement processing where engaged.
PECR	Electronic marketing, cookies or communications complaints where engaged.
Equality legislation and sector rules	Communication, accessibility and sector-specific complaint duties where engaged.

4. Definitions

Operational definitions

Term	Definition
Data protection complaint	An expression that a person considers the handling of personal data relating to them may infringe the UK GDPR or Part 3 of the DPA 2018.
Complainant	The data subject or authorised representative who makes the complaint.
Complaint point	A distinct issue that must be investigated and answered separately.
Controller	The person that determines the purposes and means of processing, subject to the applicable statutory definition.
Processor	A person that processes personal data on behalf of a controller, subject to the applicable statutory definition.
Personal data breach	A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Term	Definition
Outcome	The communicated conclusion on each complaint point and any resulting action.
Working day	A day other than Saturday, Sunday or a relevant public holiday for the selected UK region.

5. Roles and responsibilities

Roles must be tailored to the organisation. A role described as a Data Protection Officer must retain the independence and reporting arrangements required for a formally appointed DPO.

All staff must be able to recognise a possible data protection complaint and know where to send it.

The complaint owner identifies and records any actual or perceived conflict. Where practicable, a person materially involved in the subject matter does not approve the outcome.

RACI matrix

Activity	Responsible	Accountable	Consulted	Informed
Recognise and route	All staff	Line manager	Complaints Manager	Privacy Lead where material
Acknowledge and record	Complaints Manager	Complaints Manager	Customer-facing team	Complainant
Triage linked risks	Complaints Manager	Privacy Lead	Security, safeguarding and authorised legal reviewers	Operations Director where material
Investigate	Assigned investigator	Decision-maker	Relevant specialists	Complaints Manager and complainant
Approve outcome	Decision-maker	Privacy Lead	Authorised legal reviewer where engaged	Complainant and action owners
Close and improve	Complaints Manager	Privacy Lead	Action owners	Operations Director where material

6. How complaints can be made

Northfield Services Ltd provides clear ways for people to make data protection complaints directly to us.

A person may use our complaint form, but does not have to. We accept complaints through any reasonable channel, including when first raised with a member of staff.

A verbal complaint is recorded in the person's own words and, where practicable, the summary is confirmed with them.

Anonymous complaints are considered where there is enough information to make appropriate enquiries, but anonymity may limit the investigation or the outcome information we can provide.

If a complaint reaches us through social media, we ask for an alternative contact method before discussing personal information.

Tell us if you need another format, interpretation, language assistance, help using a complaint route or another reasonable adjustment.

A family member, solicitor, advocate or another representative may complain for someone else. We ask for proportionate evidence that they are authorised to act.

Contact routes

Channel	Contact details
Email	privacy@northfield.example
Online	northfield.example/privacy-complaints
Telephone	0117 000 0000
Post	Data Protection Complaints, Northfield Services Ltd, 1 Northfield Square, Bristol BS1 1AA
Other channels	Email, online form, post, telephone, social media, in person and any other reasonable channel.

7. Triage and risk assessment

Triage starts on receipt and does not wait for the acknowledgement. Urgent containment and linked legal clocks are opened immediately where needed.

A severity rating supports prioritisation and oversight. It does not determine whether the law was infringed or replace a fact-specific investigation.

Mandatory triage checks

Check	Required action	Record
Possible personal data breach	Open the breach process immediately and assess containment and notification.	Incident reference and awareness time
Ongoing or serious harm	Prioritise containment and senior oversight.	Harm, action and decision time
Child, vulnerable person or safeguarding	Use appropriate communication and refer urgent safeguarding information.	Safeguarding reference and communication needs

Check	Required action	Record
Special-category or criminal-offence data	Apply enhanced access and evidence controls.	Data category and access restriction
Rights request	Open a separate linked record and calculate the applicable deadline.	Rights-request reference
Regulator, litigation, insurer or compensation	Refer to the authorised route without delaying appropriate complaint enquiries.	Referral, owner and boundary
Systemic issue or repeated complaint	Consider wider containment, risk register and DPIA review.	Affected process and control owner
Processor or joint controller	Preserve the original receipt date and activate the agreed information-sharing route.	Third-party contact and request

Severity matrix

Illustrative organisation-control criteria. Tailor thresholds and escalation roles before use.

Level	Indicative criteria	Examples	Minimum actions
1 Routine	Limited scope, no current harm and straightforward evidence.	Isolated accuracy or communication concern.	Standard owner, proportionate plan and normal oversight.
2 Significant	Sensitive data, repeated failure, vulnerable person, material delay or wider process concern.	Repeated disclosure error or unresolved rights handling failure.	Privacy oversight, documented risk controls and scheduled progress reviews.
3 Critical	Serious or ongoing harm, likely reportable breach, systemic failure, active regulator contact or senior conflict.	Large-scale exposure or continuing unsafe processing.	Immediate containment, senior escalation, linked incident or legal route and frequent review.

8. Timeframes

We acknowledge receipt of a data protection complaint within 30 days.

Day 1 is the calendar day after receipt. If the 30th calendar day falls on a weekend or relevant public holiday, the acknowledgement deadline moves to the next working day.

We make appropriate enquiries, keep the complainant informed and communicate the outcome without undue delay. There is no standard one-month final-response deadline or two-month complaint extension.

Any shorter acknowledgement target or progress cadence is an internal control and must not delay action that can reasonably be completed sooner.

Where representative authority is required and has not been established, we acknowledge receipt but do not begin substantive investigation until suitable evidence is received.

Timeframe controls

Event	Requirement or control	Classification
First receipt	Record immediately and preserve the original date and channel.	Evidence control
Acknowledgement	No later than the adjusted 30-day deadline.	Legal duty
Investigation start	Begin appropriate enquiries on receipt.	Legal duty
Progress update	Without undue delay and when a material timescale or delay changes.	Legal duty and organisation control
Outcome	Communicate without undue delay after appropriate enquiries.	Legal duty
Internal review	Use only the organisation's configured target and do not make it a prerequisite to contacting the ICO.	Optional organisation control

How the acknowledgement deadline is calculated

Rule	Application
Receipt Date	The date the complaint first reaches any part of the organisation.
Counting Rule	Count 30 calendar days from the day after receipt.
Adjustment Rule	If day 30 is a weekend or relevant public holiday, move to the next working day.
Boundary	This calculation is for acknowledgement, not the final outcome.

9. Investigation

We make enquiries into the complaint to the extent appropriate and without undue delay. The investigation begins when the complaint is received.

The nature and extent of the investigation depend on the circumstances, including complexity, scale, available evidence and any continuing harm.

The investigator distinguishes established facts, conflicting evidence and unresolved uncertainty, and records reasons for each finding.

Legal privilege is assessed only by an authorised legal reviewer. Routine complaint documents are not labelled privileged merely because a legal issue may arise.

- Review each complaint point thoroughly, fairly and accurately.
- Compare the complaint with the records held by the organisation.
- Speak to relevant staff and check applicable policies, notices, decisions and system records.
- Preserve relevant evidence and maintain a chronology of enquiries and decisions.
- Escalate a conflict where the complaint concerns the investigator, decision-maker or senior staff.

Investigation plan requirements

Element	Required record
Complaint points	Each issue in the complainant's own meaning and the outcome sought.
Conflict check	Actual or perceived conflict and mitigation.
Evidence map	Systems, logs, messages, notices, consent records, decisions, supplier records and witnesses.
Enquiries	Question, person consulted, date, answer and supporting evidence.
Assessment	Facts established, conflicting evidence, uncertainty and reasons.
Risks and referrals	Breach, safeguarding, Legal, insurer, regulator and senior escalation references.
Expected completion	Target date, review date and reason for any change.

Independent regulator

You may complain to the Information Commissioner's Office at any time. You do not have to complete an internal review first. Telephone 0303 123 1113.

ico.org.uk/make-a-complaint

10. Outcome and response

When the investigation is complete, we inform the complainant of the outcome without undue delay.

The outcome addresses each complaint point, explains the enquiries made and gives enough information for the person to understand the conclusion.

Where appropriate, each point is recorded as upheld, partly upheld, not upheld, withdrawn or out of scope.

If the complainant seeks compensation, the matter is referred to the authorised legal or claims process. This procedure does not determine legal entitlement or the amount of compensation.

Illustrative remedies and controls

Type	Examples	Approval boundary
Individual remedy	Explanation, apology, correction, restriction, erasure or communication preference change where legally appropriate.	Complaint decision-maker and relevant process owner
Control improvement	Procedure, notice, system, supplier, training or monitoring change.	Control owner and privacy oversight
Financial or legal claim	Compensation, ex gratia payment or settlement request.	Authorised legal, claims or insurer route only

The outcome should include

- Case reference and outcome date
- Each complaint point and the finding reached
- A concise account of the enquiries and evidence considered
- Facts established, material uncertainty and reasons for the conclusion
- Action completed or planned, including owners and target dates where relevant
- Any separate rights-request, breach or sector-process status
- Any internal review route
- Information about complaining to the ICO
- The contact point for questions about the outcome

11. Escalation and external rights

A person may complain to the Information Commissioner's Office at any time. They do not have to complete an internal review first.

The ICO suggests raising the matter within three months of the organisation's final response because delay may affect how it handles the complaint. This is not described as a statutory deadline.

Where an internal review is offered, it is conducted by a person who was not the original decision-maker where practicable, within the organisation's stated target.

The complainant may also have rights to seek a court remedy or compensation. The outcome signposts independent legal advice and does not state that an entitlement or amount has been established.

Contact routes

Channel	Contact details
Email	privacy@northfield.example
Online	northfield.example/privacy-complaints
Telephone	0117 000 0000

Channel	Contact details
Post	Data Protection Complaints, Northfield Services Ltd, 1 Northfield Square, Bristol BS1 1AA
Other channels	Email, online form, post, telephone, social media, in person and any other reasonable channel.

Independent regulator

You may complain to the Information Commissioner's Office at any time. You do not have to complete an internal review first. Telephone 0303 123 1113.

ico.org.uk/make-a-complaint

12. Recording and the complaints register

We keep a clear record from first receipt to closure so that we can show what we did and why.

The complaint file is itself personal data. The organisation records its lawful basis, any additional condition for sensitive data, access restrictions, privacy information and justified retention rule before operating this procedure.

We do not keep personal information for longer than necessary. Each case has a retention review date and disposal outcome under the approved retention schedule.

Complaints register field schema

Field	Purpose	Required
Case reference	Stable identifier and linkage	Yes
Receipt date, time and channel	Deadline and provenance	Yes
Complainant category	Trend and accessibility analysis	Yes
Complaint points and outcome sought	Investigation scope	Yes
Data, processing and systems involved	Evidence and risk scoping	Yes
Severity and linked process flags	Prioritisation and escalation	Yes
Owner, investigator and decision-maker	Accountability and conflict control	Yes
Acknowledgement and update dates	Timeliness evidence	Yes

Field	Purpose	Required
Outcome, remedy and root cause	Decision and improvement evidence	Yes
Corrective actions and completion	Control tracking	Where applicable
ICO or sector escalation	Regulatory history	Where applicable
Closure and retention review	Lifecycle control	Yes

Minimum case record

- First receipt date, time and channel
- The complaint in the person's own words
- Separate complaint points and the outcome sought
- Contact preference and accessibility requirements
- Identity and representative authority checks where required
- Triage rating and linked breach, rights, safeguarding, legal or sector records
- Acknowledgement date, method and delivery evidence
- Investigation plan, enquiries and evidence references
- Progress updates and material communications
- Findings, reasons, decision approval and conflicts
- Outcome communication and delivery evidence
- Root cause, corrective actions, owners and completion evidence
- Closure date, retention review date and disposal outcome

13. Root cause analysis and continuous improvement

After the outcome, we consider what can be learned or improved to prevent future complaints.

A documented root-cause review is required for upheld, repeated, significant or critical complaints. Corrective and preventive actions have named owners, due dates and completion evidence.

Where relevant, learning is fed into the risk register, DPIA reviews, policies, privacy information, system design, supplier oversight and training.

Corrective and preventive action record

Field	Requirement
Root cause	Record the underlying control, process, system, supplier or capability cause.
Immediate correction	Record action taken to address the present issue.

Field	Requirement
Preventive action	Record action intended to reduce recurrence.
Owner and due date	Assign accountable delivery and a realistic date.
Completion evidence	Link evidence that the action was implemented.
Effectiveness review	Record how and when the organisation checked that the action worked.

14. Reporting and metrics

We review complaint volumes, recurring themes and lessons learned to identify potential compliance issues and areas for improvement.

Reporting uses aggregated information where possible and does not include unnecessary case details. Reporting cadence and audiences are approved by the organisation.

Minimum management information

Metric	Definition	Control note
Acknowledgement timeliness	Percentage acknowledged by the adjusted 30-day deadline.	Report missed deadlines separately.
Outcome time	Average and median calendar days from receipt to outcome.	Do not turn the average into a standard deadline.
Outcome profile	Upheld, partly upheld, not upheld, withdrawn and out-of-scope points or cases.	Use consistent definitions.
Breach conversion	Complaints that opened a personal data breach record.	Do not infer reportability from the metric alone.
External escalation	ICO and relevant sector referrals.	Record status and learning, not assumptions about regulator findings.
Corrective-action completion	Open, overdue and completed actions.	Require completion evidence.

Monitoring measures

- Complaints received by channel, data subject category and theme
- Acknowledgements sent by the adjusted deadline
- Open complaints, age profile and average or median time to outcome
- Outcomes and upheld or partly upheld rate
- Complaints linked to personal data breaches
- Internal reviews, ICO escalations and sector referrals

- Repeated root causes and control failures
- Overdue corrective actions and unresolved material risks
- Training and complaint-route test completion

15. Confidentiality and no detriment

No person suffers retaliation or avoidable disadvantage because they raised a data protection concern in good faith.

Complaint information is shared only where needed to investigate, decide, oversee or comply with legal obligations. The organisation explains any material limit on confidentiality.

Anonymous complaints are considered where sufficient information is available, but anonymity may limit enquiries or feedback.

16. Rights-request exceptions and difficult communications

The manifestly unfounded or excessive provisions in Article 12(5) apply to requests made under the relevant data subject rights provisions. They do not remove the section 164A complaint duties.

A communication that also contains a data rights request is separated into linked records. Any Article 12(5) decision applies to the rights request only and requires its own evidence, approval and response.

A complaint that is repetitive, burdensome, hostile or considered unfounded is still acknowledged. We make enquiries to the extent appropriate and are not required to take unreasonable or disproportionate steps.

Communication restrictions address safety or conduct proportionately and preserve an effective route for the data protection complaint.

17. Processors, joint controllers and third parties

Where a joint controller receives a complaint, the original receipt date is preserved and the transparent arrangement is used to coordinate the investigation and communication.

Processors must follow the agreed route to forward complaints, preserve relevant evidence and provide information needed by the controller. The controller remains responsible for the complaint obligations.

Information shared for an investigation is limited to what is necessary and uses an approved secure route. International-transfer or sector concerns are referred to the relevant specialist process.

Third-party routing controls

Relationship	Minimum control
Joint controller	Transparent allocation, shared receipt rule, investigation coordinator and complainant contact.
Processor	Prompt forwarding, evidence preservation, investigation assistance and secure information provision.
Independent controller	Document the lawful and necessary information-sharing basis and each controller's separate responsibilities.

Relationship	Minimum control
Overseas recipient	Apply the relevant transfer arrangement and specialist escalation without merging jurisdictional duties.

18. Training and awareness

Staff receive enough training to recognise a data protection complaint and know where to send it.

People with complaint responsibilities receive role-specific training on acknowledgement, triage, identity, representatives, investigation, progress, outcomes and record keeping.

Completion, missed training, competence checks and remedial action are recorded. Published routes and absence cover are tested at planned intervals.

Training matrix

Audience	Minimum content	Evidence
All staff	Recognition, first receipt, secure handling and routing.	Induction and refresher completion
Customer-facing teams	Verbal, social-media and accessibility handling.	Scenario or route test
Complaint handlers	Triage, deadlines, investigation, progress, outcome and records.	Role-specific assessment
Decision-makers and oversight	Conflicts, evidence, remedy, external rights and assurance.	Briefing and approval record

19. Monitoring, review and assurance

The document owner reviews this procedure at least annually and sooner after a material legal, regulatory, organisational, channel, incident or assurance change.

Assurance includes sample case-file review, route testing, deadline-calculator testing, corrective-action tracking and confirmation that official sources remain current.

Findings, owners, due dates and completion evidence are reported through the organisation's approved governance route.

Monitoring measures

- Current approved version is available and obsolete versions are controlled
- Every public channel is reachable and has absence and business-continuity cover
- A sample of case files contains receipt, acknowledgement, enquiries, progress, outcome and closure evidence
- The calculator uses the selected UK bank-holiday region and active rule-pack version
- Official sources have a review date, change history and next scheduled review

- Overdue corrective actions and unresolved material risks are escalated
- Training, route tests and assurance actions are complete

Source register and document scope

The sources below were reviewed 6 August 2026.

UK Parliament

Data Protection Act 2018, section 164A

Complaints by data subjects to controllers | Reviewed 6 August 2026

UK Parliament

Data (Use and Access) Act 2025, section 103

Insertion of sections 164A and 164B into the Data Protection Act 2018 | Reviewed 6 August 2026

Information Commissioner's Office

What are data protection complaints?

Reviewed 6 August 2026

Information Commissioner's Office

How do we prepare to handle data protection complaints?

Reviewed 6 August 2026

Information Commissioner's Office

What do we do when we receive a complaint?

Reviewed 6 August 2026

Information Commissioner's Office

What do we do after we have finished our investigation?

Reviewed 6 August 2026

GOV.UK

UK bank holidays

Reviewed 6 August 2026

Scope and limitations

Applies to	Data protection complaints made to a UK controller and received on or after 19 June 2026.
Does not decide	Whether data protection law was infringed, compensation is due, identity or representative authority is sufficient, or sector-specific duties apply.
Before use	The organisation must tailor, approve, publish and operate the procedure and its linked internal controls.

Annex A. Complaint form template

Collect enough information to understand and route a complaint without making the form mandatory.

- State that a person may complain through another reasonable channel.
- Do not collect identity evidence by default.
- Keep the original receipt date if a staff member later enters the form.

Field	Required	Completion guidance
Name	Where applicable	Optional where an anonymous complaint can be assessed.
How should we contact you?	Where applicable	Collect only the contact details needed for the chosen method.
Are you acting for someone else?	Yes	If yes, request proportionate authority separately.
What happened?	Yes	Preserve the person's own meaning and words.
What personal information or processing is involved?	Where applicable	Help scope evidence without requiring legal terminology.
When did it happen?	Where applicable	Allow approximate dates where exact dates are unknown.
What would you like us to do?	Where applicable	This does not limit the investigation or available outcome.
Do you need another format or adjustment?	Where applicable	Record only what is needed to provide the adjustment.
Is anyone at immediate risk of harm?	Where applicable	Display the urgent safeguarding or emergency route.
Supporting information	Where applicable	Explain secure upload or alternative evidence routes.

Annex B. Acknowledgement template

Confirm receipt and explain the next steps within the adjusted 30-day deadline.

Subject

We have received your data protection complaint [CASE REFERENCE]

Receipt

We received your complaint on [FIRST RECEIPT DATE] through [CHANNEL].

Complaint points

Our current understanding is: [NUMBERED COMPLAINT POINTS]. Tell us promptly if this does not reflect your concern.

Next steps

[OWNER OR ROLE] will make enquiries appropriate to the complaint and keep you informed. Our next update is planned for [DATE OR TRIGGER].

Linked processes

We have opened the following separate linked records where applicable: [RIGHTS REQUEST, BREACH OR OTHER REFERENCE].

Contact and accessibility

Contact [CONTACT POINT] and tell us if you need another format or adjustment.

Annex C. Progress update template

Give meaningful progress information and explain any material delay without disclosing inappropriate investigation detail.

Status

We are continuing to investigate [CASE REFERENCE].

Progress

Since our last update, we have [HIGH-LEVEL PROGRESS].

Delay or dependency

The following matter affects the expected timescale: [REASON]. This does not change the duty to avoid unjustified delay.

Next update

We expect to provide [OUTCOME OR NEXT UPDATE] by [DATE].

Contact

Contact [CONTACT POINT] if your circumstances change or you have relevant information.

Annex D. Outcome templates

Provide reasoned, point-by-point outcomes without implying legal certification or determining compensation.

Upheld or partly upheld

Outcome

We have [UPHELD OR PARTLY UPHELD] the following complaint point(s): [POINTS].

Enquiries and evidence

We considered [MATERIAL ENQUIRIES AND EVIDENCE].

Reasons

Our reasons are [REASONS, INCLUDING MATERIAL UNCERTAINTY].

Action

We have completed or planned [ACTION, OWNER AND TARGET DATE].

Further steps

You may use [INTERNAL REVIEW ROUTE] and may complain to the ICO at any time.

Not upheld

Outcome

We have not upheld the following complaint point(s): [POINTS].

Enquiries and evidence

We considered [MATERIAL ENQUIRIES AND EVIDENCE].

Reasons

Our reasons are [REASONS, INCLUDING MATERIAL UNCERTAINTY].

Further steps

You may use [INTERNAL REVIEW ROUTE] and may complain to the ICO at any time.

Withdrawn or out of scope

Status

We have recorded this matter as [WITHDRAWN OR OUT OF SCOPE] because [REASON].

Routing

The following separate process remains available or open: [ROUTE AND REFERENCE].

Data protection element

We have completed the following enquiries into any remaining data protection complaint: [ENQUIRIES AND OUTCOME].

Annex E. Complaints register field schema

Define the minimum structured record for each complaint and its lifecycle.

- Add the current case to the register and supply a separate blank template.
- Restrict access and apply the approved retention rule.
- Do not put unnecessary identity documents or free-form evidence into the summary register.

Complaints register field schema

Field	Purpose	Required
Case reference	Stable identifier and linkage	Yes
Receipt date, time and channel	Deadline and provenance	Yes
Complainant category	Trend and accessibility analysis	Yes
Complaint points and outcome sought	Investigation scope	Yes
Data, processing and systems involved	Evidence and risk scoping	Yes
Severity and linked process flags	Prioritisation and escalation	Yes
Owner, investigator and decision-maker	Accountability and conflict control	Yes
Acknowledgement and update dates	Timeliness evidence	Yes
Outcome, remedy and root cause	Decision and improvement evidence	Yes
Corrective actions and completion	Control tracking	Where applicable
ICO or sector escalation	Regulatory history	Where applicable
Closure and retention review	Lifecycle control	Yes

Annex F. Receipt-to-closure process flow

Provide a deterministic operating sequence with separate breach and rights-request forks.

Start. F1

Step	Action	Decision or next route
F1. Receive	Record first receipt and preserve the person's wording.	Next: F2
F2. Acknowledge	Calculate and meet the adjusted 30-day deadline.	Next: F3
F3. Triage	Check urgent harm, breach, rights request, safeguarding, regulator and third-party involvement.	Are linked processes required? Next: F4, F3A, F3B
F3A. Open breach process	Start the breach clock, containment and reportability assessment while the complaint stays open.	Next: F4
F3B. Open rights-request process	Create a separate record and calculate its applicable deadline independently.	Next: F4
F4. Confirm scope	Separate complaint points, authority, communication needs and outcome sought.	Next: F5
F5. Investigate	Gather proportionate evidence, record enquiries and keep the complainant informed.	Next: F6
F6. Decide	Reach a reasoned finding on each complaint point and approve action.	Next: F7
F7. Communicate outcome	Explain the findings, reasons, action and external rights without undue delay.	Next: F8
F8. Close and improve	Record delivery, complete corrective actions, review learning and set retention.	

Annex G. RACI matrix

Allocate operational responsibility, accountability, consultation and information duties.

RACI matrix

Activity	Responsible	Accountable	Consulted	Informed
Recognise and route	All staff	Line manager	Complaints Manager	Privacy Lead where material
Acknowledge and record	Complaints Manager	Complaints Manager	Customer-facing team	Complainant
Triage linked risks	Complaints Manager	Privacy Lead	Security, safeguarding and authorised legal reviewers	Operations Director where material
Investigate	Assigned investigator	Decision-maker	Relevant specialists	Complaints Manager and complainant
Approve outcome	Decision-maker	Privacy Lead	Authorised legal reviewer where engaged	Complainant and action owners
Close and improve	Complaints Manager	Privacy Lead	Action owners	Operations Director where material

Annex H. Severity matrix

Prioritise oversight and containment without predetermining the legal outcome.

Severity matrix

Illustrative organisation-control criteria. Tailor thresholds and escalation roles before use.

Level	Indicative criteria	Examples	Minimum actions
1 Routine	Limited scope, no current harm and straightforward evidence.	Isolated accuracy or communication concern.	Standard owner, proportionate plan and normal oversight.
2 Significant	Sensitive data, repeated failure, vulnerable person, material delay or wider process concern.	Repeated disclosure error or unresolved rights handling failure.	Privacy oversight, documented risk controls and scheduled progress reviews.
3 Critical	Serious or ongoing harm, likely reportable breach, systemic failure, active regulator contact or senior conflict.	Large-scale exposure or continuing unsafe processing.	Immediate containment, senior escalation, linked incident or legal route and frequent review.

Annex I. ICO contact and escalation wording

Provide accurate, non-discouraging external-rights wording.

ICO route

You may complain to the Information Commissioner's Office at any time. You do not have to complete our internal review first.

Suggested timing

The ICO suggests raising the matter within three months of our final response because delay may affect how it handles the complaint. This is not presented as a statutory deadline.

Online

https://ico.org.uk/make-a-complaint/

Telephone

0303 123 1113

Post

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

Court and compensation

You may also have rights to seek a court remedy or compensation and may wish to obtain independent legal advice.

Annex J. Version history

Maintain an auditable record of approved changes and reasons.

Version history

Version	Date	Author	Approved by	Change and rationale
1.0	2 August 2026	Privacy Lead	Operations Director	First approved sample issue following commencement of section 164A of the Data Protection Act 2018.
1.1	6 August 2026	Privacy Lead	Operations Director	Expanded controlled-procedure structure, legally separated complaint and rights-request timeframes, and added deterministic annex data.

Prepared using Business Compliance Tools. The organisation remains responsible for approval, publication and operation.