# Data Protection Complaints Procedure

## 1. Purpose

This procedure explains how Hall for Cornwall receives, records, investigates and responds to complaints about the way it handles personal data.

It is intended to ensure that data protection complaints are handled fairly, promptly, consistently and transparently, and in a way that demonstrates accountability under UK data protection law.

This procedure is designed to reflect the requirements introduced by section 103 of the Data (Use and Access) Act 2025, which inserts a new section 164A into the Data Protection Act 2018.

## 2. Scope

This procedure applies to all complaints about the processing of personal data by Hall for Cornwall It applies to complaints made by customers, clients, employees, workers, former employees, contractors, service users, suppliers, website users, patients or beneficiaries and any other individual whose personal data is processed by Hall for Cornwall

It applies whether a complaint is received by email, post, webform, telephone, live chat, social media, in person, through a service team or through any other channel.

## 3. What counts as a data protection complaint?

A data protection complaint is any complaint from an individual, or someone acting on their behalf, about how Hall for Cornwall has handled that individual's personal data. The individual does not need to refer to the UK GDPR, the Data Protection Act, the Data Use and Access Act or the phrase 'data protection complaint'. Staff must look at the substance of the concern.

how personal data was collected or obtained;
how personal data has been used, shared or disclosed;
inaccurate, incomplete or out-of-date personal data;
personal data being kept for too long;
a data breach or suspected security incident;
a delayed, incomplete or disputed subject access response;
a refusal or failure to deal with a request for erasure, rectification, restriction, portability or objection;

direct marketing, cookies or tracking technologies;
automated decision-making or profiling;
failure to provide clear privacy information.

## 4. Responsibility

| Role | Responsibility |
|---|---|
| **Procedure owner** | Marketing & Communications Director |
| **Operational owner** | Marketing & Communications Director |
| **Senior escalation** | Chief Executive |
| **All staff** | Must recognise potential data protection complaints and escalate them promptly. |

The Marketing & Communications Director is responsible for maintaining this procedure, overseeing data protection complaints, ensuring complaints are logged, advising on investigations, ensuring appropriate responses are provided, identifying themes and escalating significant issues.

## 5. How individuals can make a complaint

Hall for Cornwall will facilitate the making of data protection complaints through accessible routes. Individuals can complain using any of the following methods:

| Route | Details |
|---|---|
| **Email** | Dpo@hallforcornwall.org.uk |
| **Post** | Data Protection Lead, Hall for Cornwall Trust, Back Quay, Truro, TR1 2LL |
| **Other channels** | Complaints received through service teams, customer portals, HR, social media or general inboxes must still be accepted and escalated. |

Individuals should be asked to provide their name, contact details, details of the complaint, the personal data concerned, relevant dates, copies of relevant correspondence, and the outcome they are seeking. However, Hall for Cornwall will not refuse to consider a complaint simply because the individual has not used a particular form or has not provided all information at the outset.

## 6. Complaints made on behalf of another person

A complaint may be made by someone acting on behalf of an individual, such as a family member, solicitor, advocate, representative, person with power of attorney, parent or guardian.

Before disclosing personal data to a representative, Hall for Cornwall must be satisfied that the representative has authority to act. Suitable evidence may include written authority from the individual, a signed consent form, power of attorney documentation, evidence of parental responsibility or evidence that the representative is otherwise legally entitled to act.

Authority checks must not be used to delay or obstruct a complaint. The complaint must be logged on receipt while any authority checks are completed.

## 7. Receiving and identifying complaints

Any member of staff who receives a complaint that may involve personal data must forward it to the Marketing & Communications Director as soon as possible and, in any event, within two working days.

Staff must not decide whether the complaint is legally valid before escalating it. If the substance of the concern relates to personal data, it must be escalated.

Where a complaint includes both a service complaint and a data protection complaint, the data protection element must be handled under this procedure. The wider service complaint may be handled under Hall for Cornwall's general complaints process.

## 8. Logging the complaint

All data protection complaints must be recorded in the Data Protection Complaints Log. The log should be maintained by the Marketing & Communications Director or nominated complaints team.

| Log field | What to record |
|---|---|
| **Complaint reference** | Unique complaint number. |
| **Date received** | Date the complaint was first received by the organisation. |
| **Method received** | Email, post, webform, telephone, in person, social media or other. |
| **Complainant details** | Name and contact details. |
| **Representative** | Whether the complaint is made by a representative and whether authority has been checked. |
| **Summary** | Brief description of the complaint and the personal data issue. |
| **Category** | Subject access, erasure, accuracy, breach, sharing, marketing, retention or other. |
| **Business area** | Team, service or function involved. |
| **Investigator** | Responsible person or team. |
| **Acknowledgement deadline** | 30-day deadline calculated from receipt. |
| **Updates and outcome** | Progress updates, outcome date and decision. |
| **Remedial action** | Action required, owner and completion date. |
| **ICO escalation** | Whether the complainant has complained to the ICO. |
| **Lessons learned** | Any wider action required. |

## 9. Acknowledging the complaint

Hall for Cornwall will acknowledge receipt of a data protection complaint within 30 days of receiving it. The 30-day period starts on the day after the complaint is received. If the final day falls on a weekend or public holiday, acknowledgement can be sent on the next working day.

The acknowledgement should confirm that the complaint has been received, explain that it is being handled as a data protection complaint, provide the complaint reference number, identify the person or team handling the complaint, explain whether any further information is needed, explain the next steps, and provide an indicative timescale for a response where possible.

## 10. Investigation

The investigation must begin without undue delay. Hall for Cornwall should not wait until the end of the 30-day acknowledgement period before starting to investigate.

The investigator should consider:

what personal data is involved;
what processing activity is being complained about;
whether the complaint relates to a rights request;
whether a personal data breach may have occurred;
whether a processor, supplier or joint controller is involved;
whether Hall for Cornwall complied with the UK GDPR, Data Protection Act 2018 and internal policies;
whether remedial action is required;
whether the complaint raises wider organisational risks.
Investigation steps may include reviewing correspondence, checking systems and records, speaking to relevant staff, reviewing access logs or audit trails, checking privacy notices and policies, reviewing contracts or processor arrangements, checking whether a DPIA or legitimate interests assessment is relevant and obtaining legal or specialist advice where appropriate.

## 11. Keeping the complainant informed

Where a complaint cannot be resolved quickly, Hall for Cornwall will keep the complainant informed about progress.

Updates should be provided where the complaint is complex, further information is needed, the investigation is taking longer than expected, third-party input is required, or Hall for Cornwall needs more time to reach a fair outcome.

Updates must be clear, brief and meaningful. They must not disclose information about other individuals unless it is lawful and appropriate to do so.

## 12. Outcome response

Once the investigation is complete, Hall for Cornwall will provide the complainant with an outcome without undue delay.

The outcome response should include:

a summary of the complaint;

the issues investigated;
Hall for Cornwall's findings;
whether the complaint is upheld, partially upheld or not upheld;
reasons for the decision;
any action already taken;
any further action Hall for Cornwall will take;
any apology, where appropriate;
details of the complainant's right to complain to the ICO.

## 13. Possible outcomes

| Outcome | Meaning |
|---|---|
| **Upheld** | The organisation accepts that the complaint is justified in full. |
| **Partially upheld** | The organisation accepts some elements of the complaint but not all. |
| **Not upheld** | The organisation does not accept that there has been a failure, and explains why. |
| **Corrective action** | This may include correction, erasure, restriction, process change, training, supplier review, security improvement or further response to an individual rights request. |
| **No further action** | Where no further action is required, the organisation should still explain the reasons clearly. |

## 14. Escalation

The Marketing & Communications Director must escalate a complaint to senior management/DPO where:

the complaint involves a serious or repeated data protection issue;
there is a risk of significant harm to an individual;
the complaint relates to special category data or criminal offence data;
the complaint relates to a vulnerable individual;
the complaint concerns a senior employee or high-risk processing activity;
the complaint may result in litigation;
the complaint may be reported to the ICO;
the complaint may create reputational risk;
a personal data breach may have occurred.
Where the complaint suggests that a personal data breach may have occurred, Hall for Cornwall's personal data breach procedure must also be followed.

## 15. Complaints involving processors, suppliers or joint controllers

Where a complaint involves a processor, supplier or joint controller, the Marketing & Communications Director must identify the relevant contract, data processing agreement or data sharing arrangement.

Hall for Cornwall should consider whether the third party needs to assist with the investigation, whether it has complied with contractual obligations, whether personal data

has been processed outside agreed instructions, whether breach notification obligations have been triggered and whether remedial action is required.

Processors must be required to escalate data protection complaints to Hall for Cornwall promptly where the complaint relates to personal data processed on behalf of Hall for Cornwall

## 16. Complaints involving individual rights requests

Where a complaint concerns a subject access request or other individual rights request, the Marketing & Communications Director must review the original request, the response provided, the timeframe for response, any exemptions relied upon, searches carried out, redactions applied, information withheld, and correspondence with the individual.

If the complaint identifies an error or omission, Hall for Cornwall should correct it promptly.

## 17. Interaction with the ICO

Individuals have the right to complain to the Information Commissioner's Office if they are dissatisfied with how their personal data has been handled.

Outcome responses should include the ICO's contact details:

| ICO contact | Detail |
|---|---|
| **Website** | www.ico.org.uk |
| **Telephone** | 0303 123 1113 |

## 18. Record keeping

Hall for Cornwall must retain appropriate records of data protection complaints and how they were handled. Records should include the complaint received, acknowledgement sent, internal investigation notes, evidence reviewed, internal decisions, correspondence with the complainant, outcome response, remedial actions and closure date.

Complaint records should be retained for six years from closure unless a longer period is required due to litigation, regulatory investigation, safeguarding, insurance or other legal reasons. If a longer period is required, this must be noted on the register along with the reasons why.

## 19. Confidentiality

Data protection complaints must be handled confidentially. Information about a complaint should only be shared with staff or third parties who need access in order to investigate, respond, take advice or implement remedial action.

Hall for Cornwall must avoid disclosing personal data about other individuals unless it is lawful and necessary to do so.

## 20. Monitoring and reporting

The Marketing & Communications Director will review the Data Protection Complaints Log at least quarterly. The review should consider the number of complaints received, categories, response times, overdue complaints, repeat issues, business areas involved, upheld or partially upheld complaints, ICO escalations, remedial actions, training needs and process improvements.

A summary report should be provided to Audit Risk & Finance Committee at least annually.

## 21. Staff training

All staff must receive appropriate training so that they can recognise and escalate data protection complaints. Training should cover what a data protection complaint is, how complaints may be received, why legal terminology is not required, who complaints should be escalated to, the importance of prompt escalation, confidentiality, the 30-day acknowledgement requirement and the need to avoid deleting or altering relevant records.

## 22. Review of this procedure

This procedure will be reviewed annually, following changes to data protection law or ICO guidance, following a serious complaint, following an ICO complaint or investigation or where monitoring identifies recurring issues.

# Appendix 1: Data protection complaint acknowledgement template

**Subject: Your data protection complaint**

Dear [Name],

Thank you for contacting us.

We acknowledge receipt of your complaint dated [date] about [brief description]. We are treating this as a data protection complaint.

Your complaint reference is: [reference number].

We will review the matters you have raised and may contact you if we need any further information. We will keep you informed about the progress of our investigation and will provide an outcome without undue delay.

If you have any questions in the meantime, please contact [name/team] at [email address].

Yours sincerely,

[Name]

[Role]

# Appendix 2: Data protection complaint outcome template

**Subject: Outcome of your data protection complaint**

Dear [Name],

We are writing further to your data protection complaint dated [date].

**Summary of your complaint:** You complained that [summary of complaint].

**What we considered:** As part of our investigation, we reviewed [records reviewed], [systems checked], [staff or teams consulted] and [policies or procedures reviewed].

**Our findings:** We have found that [set out findings clearly]. Your complaint is [upheld / partially upheld / not upheld]. The reasons for our decision are [insert reasons].

**Action taken:** We have taken, or will take, the following action: [insert action].

**Right to complain to the ICO**: If you are unhappy with our response, you have the right to complain to the Information Commissioner's Office. You can contact the ICO through its website at www.ico.org.uk or by telephone on 0303 123 1113.