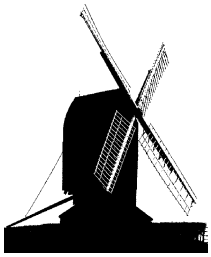

Rolvenden Parish Council

Data Breach Policy & Procedure

Adopted 17 September 2026

What is a personal data breach

Article 4(12) defines it as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

There are three kinds, and a single incident can be more than one:

Type	Meaning	Example
Confidentiality breach	Unauthorised or accidental disclosure or access	An email sent to the wrong person; a circular with addresses in the To field
Availability breach	Accidental or unlawful loss of access or destruction	Files lost to ransomware; the only copy of a record destroyed
Integrity breach	Unauthorised or accidental alteration	A record altered so that it is no longer accurate

A breach does not require malice or an attacker. Most breaches at councils of this size are ordinary mistakes. The following are all breaches:

- sending an email to the wrong recipient, or attaching the wrong document;
- sending a circular with recipients' addresses visible in the To or Cc field rather than Bcc;
- losing a laptop, phone, USB stick or paper file;
- leaving papers where an unauthorised person can read them, including in the shared office;
- publishing a document on the website that contains personal data that should have been removed;
- a councillor forwarding Council correspondence to a personal email account;
- posting personal data in a WhatsApp group or on social media;
- a supplier suffering a breach affecting Council data;
- ransomware, or any unauthorised access to Council systems;
- destroying a record that should have been retained.

Loss of access counts even where nobody else has seen the data. If a ransomware attack encrypts the Council's records and there is no backup, that is a reportable breach even though nothing was disclosed.

Reporting a breach internally

Anyone who knows or suspects that a breach has occurred must tell the Clerk immediately. That means straight away, not at the next convenient moment and not at the next meeting.

Report to	The Clerk: clerk@rolvendenparishcouncil.gov.uk / 07900 693572
If the Clerk is unavailable	The Chair of the Council
If the breach concerns the Clerk	The Chair of the Council,
If uncertain whether it is a breach	Report it anyway. The Clerk will decide

Do not attempt to fix it first. The instinct on sending an email to the wrong person is to recall it and say nothing. Recall is worth attempting, but the incident is still reportable internally, and the attempt may fail without the sender realising.

Nobody will be disciplined for reporting a breach promptly and honestly. Concealing one is a different matter, and for an employee would be a disciplinary issue. Most breaches are mistakes, and the Council needs to hear about them.

The first hour

On being told of a breach, the Clerk should work through the following in order.

Step 1: Record the time of awareness

Write down the date and time the Council became aware. This single fact determines the deadline. Awareness means a reasonable degree of certainty that a security incident has occurred and that personal data is affected, not the moment the breach itself happened.

Step 2: Contain

Stop the breach getting worse:

- attempt to recall a misdirected email, and ask the recipient to delete it and confirm they have;
- remove the document from the website;
- change passwords and revoke access where credentials may be compromised;
- disconnect an affected device from the network;
- use the remote wipe function on a lost device, if available;
- retrieve papers left where they should not have been.

Do not destroy evidence while containing. Keep the original email, the log entry, or the file, because it may be needed for the investigation and for the ICO.

Step 3 Establish the facts

Find out, as far as possible:

- what happened, and when;
- what personal data is involved, and whether any of it is special category or financial data;
- how many people are affected, at least approximately;
- who they are, and whether any is a child or a person in a vulnerable situation;
- who now has or may have had access to the data;
- whether the data was encrypted or otherwise protected;
- whether it can be recovered.

An approximate figure recorded now is more useful than an exact one three days later. Article 33(4) expressly permits reporting in phases.

Step 4: Assess the risk

The question is whether the breach is likely to result in a risk to the rights and freedoms of individuals. This is about consequences for people, not embarrassment for the Council.

Factor	What raises the risk
Type of data	Special category data, financial details, identity documents, safeguarding information
Volume	Larger numbers, though a single sensitive record can be high risk on its own
Ease of identification	Data that directly identifies people, or can be combined with other data to do so
Severity of consequences	Identity theft, financial loss, discrimination, reputational damage, physical harm, distress
Vulnerability of the individuals	Children; people at risk of domestic abuse; people whose address is confidential

Factor	What raises the risk
Who received the data	A trusted known recipient who confirms deletion, as against an unknown or hostile party
Protection	Encrypted and inaccessible data may present little or no risk
Recoverability	Whether the Council can restore the data or reverse the disclosure

One case deserves particular caution. Disclosing the address of a person who has fled domestic abuse is a high-risk breach even though only one record is involved, and would require notification of the individual as a matter of urgency.

The ICO provides a self-assessment tool for organisations unsure whether to report. Where the position is genuinely finely balanced, report: the ICO's stated aim is to help organisations rather than to penalise them, and an unnecessary report carries far less risk than an omitted one.

Step 5: Decide on notification

Risk level	ICO	Individuals
No risk to rights and freedoms	No report. Record in the register	No
Risk to rights and freedoms	Report within 72 hours	Not necessarily
High risk to rights and freedoms	Report within 72 hours	Yes, without undue delay

Every breach is recorded in the register regardless of whether it is reported. Article 33(5) requires this, and the ICO may ask to see it.

Reporting to the ICO

Where the breach is reportable, the Council reports without undue delay and, where feasible, within 72 hours of becoming aware.

How	Through the ICO's online reporting form at ico.org.uk, or by telephone on 0303 123 1113
Deadline	72 hours from awareness, including weekends and bank holidays
If later than 72 hours	Still report, and give reasons for the delay
If facts are incomplete	Report what is known within 72 hours and follow up in phases under Article 33(4)

The report must describe the nature of the breach, the categories and approximate number of individuals and records affected, the name and contact details of the Data Protection Officer, the likely consequences, and the measures taken or proposed. The companion notification form collects these in advance.

Where the breach involves a cyber incident, the Council should also consider reporting to the National Cyber Security Centre, and to Action Fraud where criminal intent is suspected. Neither substitutes for the ICO report.

Cover and out-of-hours arrangements

The 72 hours does not stop for annual leave. With a single employee, this is the point at which the procedure is most likely to fail, and the Council should resolve arrangements now rather than improvising during an incident.

Situation	Arrangement
Clerk available	Clerk leads the response
Clerk on leave or unavailable	The Chair of the Council takes the decision
Breach discovered at a weekend	The clock is running. Contact the Chair.
Breach concerns the Clerk	The Chair of the Council leads.
Breach at a supplier	The supplier notifies the Council; the Council decides whether to report to the ICO

6. Notifying individuals

Where a breach is likely to result in a high risk, the Council tells the affected individuals without undue delay. The purpose is to let them take protective steps, so the communication must be practical rather than defensive.

The notification must describe the nature of the breach in clear and plain language describe the likely consequences, and describe the measures taken or proposed. It should also say what the person can do to protect themselves.

Notification is not required where the Council has applied protection such as encryption that makes the data unintelligible, where it has taken subsequent measures ensuring the high risk is no longer likely to materialise, or where it would involve disproportionate effort, in which case a public communication is required instead.

Notify individuals directly and individually. A notice on the website is a public communication and is only appropriate where individual contact is genuinely impractical.

7. Investigation and lessons

Once the immediate response is complete, the Clerk investigates and records:

- what happened and why;
- whether a control failed, was absent, or was present but not followed;
- what will change as a result;
- who is responsible for the change and by when.

Recurring breaches of the same type indicate a systemic problem rather than individual carelessness. Three misdirected emails in a year is a sign that the way the Council sends circulars needs changing, not that the Clerk needs to be more careful.

The Clerk reports annually to the Council on breaches recorded and action taken. The report should not name individuals.

8. Related documents

- Data Protection Policy
- IT and AI Policy
- Record of Processing Activities