

Security Prevention & Incident Policy

Policy Document – Version 1.3

Thurcroft Parish Council

Adopted on 30/10/25
Minute Reference: FC260

Review Date: 30/10/27
(Bi-Yearly)



Thurcroft Parish Council

SECURITY PREVENTION & INCIDENT POLICY

What is a breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

In line with NALC guidance, a “security incident” also includes unauthorised access to council IT systems, cyber-attacks (including phishing, malware, or ransomware), loss or theft of devices, and any breach of physical or digital security controls that may compromise council information or services.

Policy

This policy specifies the actions with respect to breaches of personal data. It also applies to all information security incidents, whether they involve personal data, council records, financial systems, or other assets

Example - Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and loss of availability of personal data

Examples of wider security incidents include:

- Unauthorised access attempts to council networks or email systems.
- Loss of paper records or files containing council information.
- Compromise of councillor or staff login credentials.
- Physical break-ins at council offices or facilities where data or IT systems are held.

Incident Prevention

- We have a clear desk policy
- We have a breach’s log to update when an incident occurs
- We keep all paperwork in lockable draws or cabinets which are in a locked room inaccessible to the public
- Our bank account and Scribe have a 2-factor authentication log on



Thurcroft Parish Council

SECURITY PREVENTION & INCIDENT POLICY

- We are digitising all paper records
- The bank password changes every 3 months
- Our computers are password protected
- We have a separate internet log on for staff and for the public
- We change all passwords when we change personnel
- We change the signatories on the bank account when someone leaves
- Only authorised users can use the bank account card

Dealing with an incident

Reporting Point.

On discovery of an incident either as a result of automatic notification, accidental discovery, manual record checking or any other means, all personnel shall;

1. Report the incident to the reporting points:
 - The clerk of the council and the council chairman:
 - email: clerk@thurcroftparishcouncil.gov.uk or call 07462 671978
 - email: b.clark@thurcroftparishcouncil.gov.uk
2. The email report should be followed by a telephone call to the clerk or council chairman.
3. Should neither the clerk nor the chair be available the vice-chair of the council should be informed.
4. All councillors, staff, and contractors must receive regular training and awareness on how to identify and report potential incidents.
5. The Council will maintain an Incident Log where all reported incidents (including non-notifiable ones) are recorded, retained, and reviewed as part of the Council's internal controls and audit process.

Reporting Point Responsibilities

All incidents must be recorded. The reporting point shall perform the following actions;

- Note the time, date and nature of incident together with a description and as much detail as appropriate on an Incident Response Form.
- Ensure the protection of any evidence and that a documented chain of evidence is maintained.
- Liaise with relevant authorities, individuals and the media where appropriate.



Thurcroft Parish Council

SECURITY PREVENTION & INCIDENT POLICY

- Keep a note of all communications together with their date, time, who has been communicated with, and what the content and nature of communication was on the Incident Response Form.
- The Reporting Point shall also ensure that all incidents are reviewed by the Responsible Financial Officer (RFO) and, where appropriate, the Data Protection Officer (if appointed), to confirm compliance with GDPR and NALC model guidance

Incident Response Plan

1. Assess the risk to individuals as a result of a breach: The following must be considered:
 - a. the categories and approximate number of individuals concerned, and;
 - b. the categories and approximate number of personal data records concerned, and;
 - c. the likely consequences of the personal data breach, in particular consider if the impact results in a risk to the rights and freedoms of individuals.
 - d. In all cases, the Clerk shall ensure that Full Council is notified of any notifiable breach and that the breach is reported in the Annual Governance and Accountability Return (AGAR) if required.
 - e. To help assess the risks refer to the Information Commissioner Office (ICO) website:
 - i. <https://ico.org.uk/for-organisations/report-a-breach/>
 - ii. <https://ico.org.uk/for-organisations/guide-to-the-general-data-protectionregulation-gdpr/personal-data-breaches/>
2. If the incident is deemed to be a notifiable incident the following actions must be taken:
 - a. Within 72 hours of becoming aware of the incident (even if not aware of all the details yet):
 - b. Call ICO: 0303 123 1113 – and provide the following information:
 - what has happened;
 - when and how the council found out about the breach;
 - the people (how many) that have been or may be affected by the breach;
 - what the council are doing as a result of the breach; and
 - who else has been told.



Thurcroft Parish Council

SECURITY PREVENTION & INCIDENT POLICY

- c. For reporting a breach outside normal working hours use the ICO Reporting Form: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>
 3. If the incident is deemed to result in a high risk to the right and freedoms of individuals:
 - a. Within 48 hours the affected individuals must be informed by telephone, letter or email about the incident as there may be a need for them to take actions to mitigate immediate risk of damage to them.
 - b. The individuals must be told in clear and plain language:
 - i. the nature of the personal data breach and;
 - ii. A description of the likely consequences of the personal data breach; and
 - iii. A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects, and;
 - iv. The name and contact details of the clerk and chairman from where more information can be obtained;Notifications to affected individuals must also include advice on steps they can take to protect themselves (e.g., password changes, fraud monitoring).
 4. If the incident is **not deemed to be notifiable**:
 - a. Update the Incident Response Form along with the outcome of the risk assessment.
 - b. Include the steps and evidence used to identify and classify the risk. Include reasons why the incident is not deemed to result in a risk to the rights and freedoms of individuals.
 5. **Incident Review:** The council clerk and chairman will ensure that the incident is reviewed at the next appropriate Council meeting under the Policy and Security section of the agenda.
 - a. The Council will consider whether discussion of the incident warrants exclusion of the press and public from the meeting during that discussion.
 - b. At that meeting the council should determine if there are any further actions that need to be assigned or completed as a result of the incident.
 - c. The council may decide to refer further actions and to a committee, working group or external parties.
-



Thurcroft Parish Council

SECURITY PREVENTION & INCIDENT POLICY

- d. It should be noted that this final stage of the incident may require a review of this policy document.
- e. Following an incident, lessons learned must be documented and integrated into the Council's Business Continuity Plan and staff training programmes.
- f. The Council will review and test its security controls annually (e.g., IT security, password policies, backup systems, physical security) to reduce the risk of recurrence.



Thurcroft Parish Council

SECURITY PREVENTION & INCIDENT POLICY

FLOW CHART

Thurcroft Parish Council

Security Incident – Quick Reference Flowchart

Step 1: Identify Incident

- Anyone (staff, councillor, contractor) discovers a possible security or data breach.
- Examples: unauthorised access, lost/stolen device, phishing email, data sent to wrong recipient.

Step 2: Report Immediately

- Report to **Clerk** and **Chairman** (or Vice-Chair if unavailable).
- Send **email** and follow up with a **phone call**.

Step 3: Initial Logging

- Clerk/Chair records on **Incident Response Form**:
 - Time, date, nature of incident.
 - People and data affected.
 - Evidence secured.
- Incident added to **Council Incident Log**.

Step 4: Assess Risk

- Clerk, RFO, and (if appointed) DPO assess:
 - How many individuals affected?
 - Type of data compromised?
 - Likely consequences?
- Use **NALC/ICO risk matrix** to score likelihood and impact.

Step 5: Decide Action

- **If Notifiable Breach**:
 - Report to **ICO within 72 hours**.
 - Notify affected individuals within 48 hours if high risk.
- **If Non-Notifiable**:
 - Record assessment, outcome, and justification.

Step 6: Contain & Mitigate

- Secure systems, recover lost data if possible.
- Apply technical/physical controls (password resets, backups, building security).
- Inform IT support or third parties if needed.

Step 7: Council Notification

- Report to Full Council at next meeting.
- Exclude press/public if sensitive.
- Agree follow-up actions or referrals.

Step 8: Review & Learn

- Clerk/Chair lead post-incident review.
- Update **Business Continuity Plan**.
- Deliver **staff/councillor training** if lessons identified.
- Review **insurance cover** if financial/reputational risks involved