POLICY 07

Complaints, Whistleblowing and Non-Retaliation

Published November 17, 2026

Purpose and scope

Participants, personnel, donors and partners can raise concerns about service, conduct, financial practices, safeguarding and digital tools.

Report and escalate

Use the TBGN contact form to request the appropriate complaints channel. Keep sensitive details out of the initial message. Issues involving the usual contact must go to a designated Potter's House safeguarding or governance representative who is independent of the matter.

The service targets are five business days for acknowledgement of routine complaints and 20 business days for a status update. Triage urgent safeguarding concerns immediately and follow external reporting duties.

Review and protect people

Assign an impartial reviewer, preserve relevant information and allow a fair response when consistent with safety and law. Limit disclosure to people who need it. Anonymous reports may be reviewed where available information allows.

Retaliation against good-faith reporters or people assisting an investigation is prohibited. Address deliberate fabrication through fair process. People retain access to police, child protection, regulators and legal remedies.

Digital complaints

Provide human review for AI bias, errors, exclusion, misuse or harmful content. Preserve necessary evidence without circulating sensitive prompts, and document escalation and corrective action.

Records and review

The responsible lead keeps the records needed to demonstrate implementation, including relevant approvals, training, checks, incidents and corrective actions. Review this policy at least annually and after a material incident, change in law or funding, or significant program expansion. Refer material changes to the authority designated by Potter's House.

Standards for AI-assisted work

Use approved tools for a defined learning or operational purpose. A person reviews AI-assisted work, checks substantive claims against reliable sources and decides what to use. Protect private information, disclose material AI use and provide an accessible alternative where needed. Record the purpose, tool and permissions, privacy checks, verification, incidents and follow-up.