POLICY 02

Conflicts of Interest and Related-Party Transactions

Published November 17, 2026

Purpose and scope

Governance, spending and referral decisions must serve the initiative and its participants. This policy applies to decision-makers, staff, volunteers and advisers.

Disclose and step aside

Disclose actual, potential or reasonably perceived conflicts on appointment, annually and when circumstances change. Disclose relevant financial, family, work and organizational relationships before a decision is made.

A person with a conflict must leave the deliberation, refrain from influencing or approving the decision, and provide factual information only when the independent reviewer requests it. Record the disclosure, recusal and decision in the minutes and restricted conflicts register.

Transactions and gifts

Refer purchases, referrals, grants, contracts and honoraria involving a related party for independent review under Potter's House procurement and conflict rules. The interested party must never approve their own transaction. Record the need, fairness, evidence and independent approval.

Decline cash and benefits that could influence decisions. Record gifts of nominal value under the church's applicable gift rules.

Technology and sponsorship

Disclose interests in AI suppliers, training sponsors, referral incentives and data processing arrangements. Apply the same independent assessment and recusal requirements when selecting or renewing tools.

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.