

AI acceptable use note

A one-page starting point for a communications team. Adapt it, then agree it with your legal, compliance or trustee colleagues.

ORGANISATION

VERSION

OWNER

AGREED BY, ON

NEXT REVIEW

name, role

board, leadership or trustees

three months on

● Why we have this

AI tools save time. They also carry risks we are accountable for: what goes into them, what comes out, and whether a reader can trust it. This note sits under our [data protection policy] and [information security policy]; where they say more, they win.

● Approved tools and uses

Tool and account type	Approved for (task and kind of information)	Approved by, on	Owner
[tool, account type]	[e.g. first drafts from public information]	[name, date]	[name]

If a tool or a use is not on this list, ask [the communications lead] first. Before adding one, check how the account handles what you put in; if you cannot tell, treat it as public.

The red lines

One test covers most cases: **if you would not email it to a journalist, do not paste it into a public AI tool.**

The following never go into a public or personal-account AI tool. They go into an approved tool only where that use has been agreed by [the communications lead] with [our data protection lead, legal adviser or, if we have neither, a named trustee or our sector body]:

- **Personal data** about anyone: staff, supporters, customers, journalists, service users.
- **Confidential, donor and client information**, and anything covered by an NDA or a funding agreement.
- **Beneficiary, service-user and safeguarding content**: case studies, testimonies and images involving beneficiaries, patients or children, and anything touching a safeguarding concern. Permission to publish a story is not permission to put it through an AI tool; that is a separate decision.
- **Embargoed or price-sensitive information**: unannounced appointments, results, partnerships, funding and campaigns.
- **Legal and regulatory material**: contracts, complaints, correspondence with regulators, legal advice.
- **Crisis and incident content** before the facts are confirmed, and **security incident details** at any time.

Before you paste, four questions. Is any of this not yet public? Does it name or identify a person? Is it covered by a confidentiality obligation? Would it cause harm if it appeared in a news article tomorrow? **Yes to any of them means an approved tool for an approved use, or no AI for this task.** Unsure means yes.

● Outputs: what leaves us is ours

AI drafts; a named person publishes. Every figure, name, quote, date and claim in anything AI helped produce is checked against its source before it goes out, and we check that people are portrayed fairly and accurately. We do not publish a claim we cannot stand behind because a tool wrote it confidently. Where AI has materially shaped a piece, we say so in a line at the foot. Our usual sign-off applies.

● Keeping this current

[The communications lead] owns this note, keeps the tool list current as terms and tools change, briefs new staff on it, and brings it back to [board / leadership team / trustees] every [three] months with a short note of what changed and anything that went wrong.

● What we use AI for, and what we do not

Approved tools, for first drafts, summaries, research on public topics, editing, rewriting for different audiences, and planning with non-sensitive material. Not for the message itself in a crisis, not for decisions about people, and not for anything we would be uncomfortable saying AI helped with.

● If you are unsure, or something goes wrong

Ask [the communications lead] before, not after. Nobody will be criticised for asking, or for choosing not to use AI on something that felt wrong. If you think personal data or confidential material has gone where it should not, stop using that tool for the task and tell [the communications lead] straight away, the same hour if you can: some incidents have to be reported to the ICO within 72 hours, and the clock starts when we find out.