



## Content: Plain-Language Glossary (Starter)

*Definitions of common terms (trust, data, security).*


<b>Doc ID</b>	LS-CON-0001	<b>Doc Type</b>	Content
<b>Version</b>	v1.0	<b>Status</b>	Approved
<b>Confidentiality</b>	Public	<b>Last Updated</b>	2025-09-27
<b>Principal</b>	Transparency	<b>Next Review</b>	2026-06-30

### Change Log

Date	Author	Change	Version
2025-09-27	LucidSeal	Initial Version	v1.0

## Content: Plain-Language Glossary (Starter)

*To help organisations, boards, and communities cut through jargon when talking about digital trust, data, and security.*

 **Tip for community use** – Start with 5-10 terms that matter most to your organisation right now. Use this glossary in board packs, project proposals, or training sessions to cut through jargon. Encourage staff and volunteers to suggest new terms – making it a living glossary that grows with your community.

Term	Plain Explanation	Why it Matters
<b>Data minimisation</b>	Collecting only what you really need, nothing extra.	Reduces risk if data is lost or stolen.
<b>Encryption</b>	Scrambling data so only authorised people can read it.	Protects sensitive info in case of leaks.
<b>MFA (Multi-Factor Authentication)</b>	Using more than one way to prove it's really you (e.g., password + code on your phone).	Makes accounts much harder to break into.
<b>Access review</b>	Regularly checking who has access and removing those who no longer need it.	Stops old accounts from becoming easy targets.
<b>Incident</b>	An event where data, systems, or trust might be at risk (e.g., a hack attempt, lost laptop).	Quick response can reduce damage.
<b>Consent</b>	When someone agrees to how their data is collected or used, after being told in	Builds trust and keeps data use legal.

	clear terms.	
<b>Breach</b>	When information is accessed, stolen, or exposed without permission.	Can harm people and damage reputation.
<b>Phishing</b>	A fake email, message, or website that tries to trick you into giving away information.	A common way attackers steal passwords or money.
<b>Cookies</b>	Small files stored on your device that remember your activity (e.g., keeping you logged in).	Useful, but can also track you across sites.
<b>Audit</b>	An independent check to see if policies and practices are being followed.	Helps catch gaps and reassure stakeholders.
<b>Patch/Update</b>	Fixes applied to software to close security holes or improve performance.	Prevents attackers from exploiting known flaws.
<b>Zero trust</b>	A security approach where no one is trusted by default, even inside the network.	Reduces risk of internal or accidental breaches.
<b>Anonymisation</b>	Removing personal details so information can't be linked back to someone.	Protects privacy while keeping data useful.
<b>Resilience</b>	The ability to recover quickly from problems like outages, attacks, or mistakes.	Keeps services reliable and trustworthy.

### **How to Use This Glossary**

- Share it with your board or leadership team to make discussions clearer.
- Adapt it for your own policies or training – swap in examples from your organisation.
- Expand it over time – add terms that your community or sector uses often