

DUAA Checklist

- ☐ Do we have a written data protection complaints procedure?
Covers how someone raises a complaint, who handles it, and your commitment to acknowledge within 30 days.
- ☐ Does our privacy notice mention how people can complain directly to us?
As well as their right to complain to the regulator.
- ☐ Do we know who in our organisation is responsible for logging and responding to complaints?
Name a person or role, not just "the office."
- ☐ Are we clear on the "reasonable and proportionate" standard for subject access requests?
You don't need to search everywhere — just where it's sensible to look.
- ☐ If we ever pause a SAR clock to ask for clarification, do we record when and why?
Keep a simple log so you can evidence this if asked.
- ☐ If we use any automated or AI-assisted tools that affect decisions about residents, is there always a human check?
Especially where health or care data is involved.
- ☐ Does our privacy notice clearly tell service users, residents, and families if we use AI or automated decision-making?
Be transparent about what it's used for, and explain their right to human review and to challenge a decision.
- ☐ Has our ROPA (Record of Processing Activities) been updated to reflect any new lawful basis being relied on?
Particularly where "recognised legitimate interests" is now used for a processing activity — record which one and why.
- ☐ Have we briefed staff on the DUAA changes affecting the regulator and complaints process?
No action required, just awareness so nobody is caught off guard.
- ☐ Have we linked these checks to our current DSPT evidence?
Particularly evidence under the Data Protection and Confidentiality, and Staff Responsibilities, themes.