



# Policy and Recommendations

Andrew Cormack

Chief Regulatory Adviser, JANET(UK)

[Andrew.Cormack@ja.net](mailto:Andrew.Cormack@ja.net)



# Federation Document Set

- Mandatory (legal agreement)
  - Rules of Membership
- Advisory (ways to get most out of it)
  - Use of Personal Data
  - Technical Recommendations for Participants
  - Federation Technical Specifications
  - Federation Operator Procedures
  - Etc.



# Rules (in Spirit)

- Tell the truth
- Look after users
- Look after the federation
- Fix problems within federation

Optional, but if you say you do, you must:

- [Hold users to account]



# Rules (in a bit more detail)

Omitting some administrative stuff



# Tell the Truth

(service contracts already require this)

- Statements must be accurate (§3.1)
  - Including optional declaration(s) you make
  - Statements to operator and other members



# Look After Users

(law already requires this)

- Comply with UK Data Protection Act (§5)
  - And any other applicable legislation
- Don't misuse information received (§4)
  - Use it only for what you agreed
  - Don't disclose it without authority
  - Don't data mine individual information
  - Ensure systems handling it are secure



# Look After the Federation

- Don't damage its reputation (§3.2)
- Don't misuse its name/logo(s) (§3.3)
- Help other members (§3.5)
  - E.g. when they need you to deal with misuse



# Fix Problems Inside Fed.

- No legal liability, unless agreed otherwise (§7)
- Help investigate problems (§3.5)
- Operator may audit problem processes (§8)
- Operator may make/require changes (§2.4)
- Escalation within organisations (§12)
  - Final appeal to independent expert, not court



# [User Accountability (§6)]

(service/JANET contracts already require this)

- Be able to match use to individual responsible
  - For at least 3 months after the event
  - And have policies/processes to deal effectively with misuse
- Document process for issuing credentials to users
  - Service Providers are entitled to ask to see it
- Remove out-of-date attributes promptly
- Don't reuse identifiers within 2 years of removal

Service providers may require this declaration

- May get reduced/no service without it



# Privacy Protection

- Users login at home organisation
  - Service provider sees neither username nor password
- Home organisation tells service
  - What user is (member, staff, student, ...)
  - Same user as last time (for personalisation)
  - NOT who user is: useless to most services anyway
- Home organisation deals with misuse
- Using these options improves privacy
  - And compliance with the law
- See Federation Personal Data Guide