Part 4
The DP policy authoring process

CC BY 2.5 Denmark, Digital Bevaring

Policy authoring process – stage 1

- Read policies
- Policy template
- Gather requirements
- Set out main principles
- Define the stakeholder group membership (plus ways of engaging)
- Connect with policy working groups/policy staff in your organisation
- Frame the task
- Agree on scope – ours changed from “Cambridge University Library” to “Cambridge University Libraries”

Policy authoring process – stage 2

Iterative process

1. Drafting policy statements and principles
2. Meeting with the stakeholder group
3. Gathering feedback on the policy draft (internally and externally)
4. Incorporating feedback
5. Circulating a new version of the draft

- Developing associated documentation (to support the policy)

What do you need?

Needs

- Time to read & think – to devise your approach
- Uninterrupted blocks of time to draft & edit *(more than you will have planned for)*
- Organisational style guide

Actions

- Select & borrow statements from others
- Contact specific staff – ask specific questions
- Policy writer (if you have access) – ask for feedback early on
- Listen to staff needs (ideally prior to getting together as a group)
- Keep staff in the loop (briefing senior staff, discussing with practitioners)

Think about…

- Language
- Terminology
- Types/style of policies already in your organisation
- What policy/governance change/influence you wish to make

- Aspirational vs ‘active’
- Comprehensive vs high-level

What else do you need?

Other documents

- Checklist of principles/aspects to cover *(this is where the Maturity Modelling/TDR certification comes in handy)*
- List of existing organisational policies – including URLs
- Templates/notes files for other documents you're developing e.g. Strategy, Plans, Guidelines etc.
- Recommendations document – e.g. governance groups that your organisation needs
- Comms Plan
- Briefing Paper
- Glossary – borrow where possible

Actual drafting

- Set out the policy principle headings/sub-headings (from your checklist)
- Dot-points borrowed from other policies
- Dot-points you're drafting
- Term names for glossary (document as you use them) – *definitions can come later*
- Structural edits – sections will move around
- Comments & tracked changes

Early draft version

Maintain Fixity, Integrity, Authenticity and Provenance

Fixity is the measure used by the digital preservation community to ensure that no change to digital content occurs. CUL recognises that maintaining the integrity, authenticity and provenance of digital content is essential in order to be a trustworthy custodian. While digital processes cannot alone prove the integrity, authenticity or provenance of digital content, they can aid in ensuring that integrity, authenticity or provenance is not lost along the way. CUL undertakes to:

- *Ensure an adequate technical measure is placed on all digital content in CUL's custody to be able to measure fixity;*
- *Carry out adequate digital processes to ensure that any move of digital can show evidence that no change (accidental, unauthorised or malicious) or corruption to either content or metadata has occurred;*
- *Where digital content is created by CUL, persistent identifiers are assigned;*
- *If any unintended changes (accidental, unauthorised or malicious) or corruption occurs, undertake immediate reporting and recovery efforts;*
- *Undertake regular fixity checks on an ongoing basis to mitigate risks, including but not limited to, corruption of, or changes (accidental, unauthorised or malicious) to, digital content or metadata;*
- *Regularly monitor and report on the fixity of digital content to ensure no changes (accidental, unauthorised or malicious) or corruption have taken place.*

Published version

Maintaining fixity, integrity, authenticity and provenance

In order to be a trustworthy custodian, CUL recognises that maintaining the integrity, authenticity and provenance of digital content is essential. While digital processes alone cannot prove the integrity, authenticity and/or provenance of digital content, they can aid in ensuring knowledge about the digital content is retained over time. 'Fixity' is the measure used by the digital preservation community to ensure that no unauthorised change to digital content occurs. CUL ensures that adequate technical processes are in place for all digital content and/or metadata in its custody, in order to measure the fixity of CUL's digital content. Fixity is regularly monitored – annually for all digital content and more frequently for some classes of digital content, as required. Where unauthorised changes or corruption has occurred, this is immediately reported on and recovery efforts are enacted.

For all digital content, fixity is established immediately after preservation masters and/or co-masters are created by CUL, or transferred into CUL's custody. For digital content on offer, appraisal only takes place after fixity is established. Digital content and/or metadata moved within CUL, has in place appropriate digital processes to evidence that no unauthorised changes or corruption has occurred. Digital content acquired by CUL has persistent identifiers applied, with 'original' filenames retained in metadata.

Digital Preservation Policy - published versions

Oxford (April 2018)

- https://www.bodleian.ox.ac.uk/bodley/about-us/policies

Cambridge (November 2018)

- https://doi.org/10.17863/CAM.32927
- http://www.lib.cam.ac.uk/about-library/library-management/policies