National Protocol

for the Handling, Transmission and Storage of Reservoir Information and Flood Maps

UK Reservoir Safety Liaison Group
Version 2.4.5

JUNE 2018

UK National Protocol for the Handling, Transmission and Storage of Reservoir Information and Flood Maps

Contents

Purpose and application of the protocol

1. This protocol has been produced by the UK Reservoir Safety Liaison Group (UKRSLG), comprising the Government Departments and Regulatory Bodies provided in **Annex 5.**

2. This protocol sets out the principles on how to identify, handle, transmit, share and store data and information relating to the safety of regulated reservoirs, including reservoir flood maps, some of which may be considered OFFICIAL-SENSITIVE or SECRET under Government Security Classifications. It does not advise on the status of the overarching national security risks associated with regulated reservoirs.

3. A "Regulated Reservoir" is a

   - "large raised reservoir" as defined by section 1 of the Reservoirs Act 1975;
   - "controlled reservoir" as defined by sections 1–5 of the Reservoirs Act (Northern Ireland) 2015; and
   - "controlled reservoir" as defined by section 1 of Reservoirs (Scotland) Act 2011.

4. Application of this protocol will help minimise the risk of misuse of information. It also offers guidance to those with responsibility for managing reservoir information; that which should, and that which should not, be made publicly available.

5. This protocol is for the use of Defra, the Devolved Administrations and the Regulatory Authorities appointed to regulate reservoir safety who should adhere to this protocol. Where consultants are appointed for work related to reservoir safety they should be contracted to adhere to this protocol.

6. Failure to apply this protocol may lead to the intended, or unintended, release of sensitive information which may then be used for malicious purposes. The handling, transmission, sharing or storage of information which does not follow this protocol is likely to be at an increased risk of contravening policy on Government Security Classifications; a breach of which could result in disciplinary action being taken against an individual by the appropriate body.

The context of data security

7. Changes in Government Security Classifications in 2014 and advances in digital media technology have prompted a review of the security arrangements for sensitive information.

8. The UK Government, Devolved Administrations, Regulatory Authorities, water companies, reservoir undertakers, owners, managers, qualified civil engineers and other organisations all hold information relating to reservoirs and their inherent flood risk. This information may be used by people with malicious intent.

9. This protocol replaces the guidance provided by the National Protocol for the Handling, Transmission and Storage of Reservoir Flood (Inundation) Maps for England and Wales, v6.3, December 2010.

10. When developing this protocol, consideration has also been given to other information (e.g. reservoir engineer inspection reports) where controls are necessary to protect against malicious threats to reservoir safety, and to guide the disclosure or withholding of information. Previous guidance on what information may be considered non-sensitive and sensitive has been reviewed and is provided within **Annex 1** of this protocol.

11. Guidance on measures for handling reservoir information which should be taken in addition to central government guidance is set out in **Annex 2**.

Disclosure of information

12. Reservoir legislation in the UK does not require the disclosure of information other than the information which is available on the public reservoirs registers – See Public Registers below.

13. It is expected that requests for information relating to reservoirs held by public bodies would be considered under Environmental Information Regulations (EIR). Public bodies must process requests for environmental information in line with the EIR Regulations. Where information is not held by the public body there is no requirement to create new records in response to the request. If the information being requested is already publicly available, the requester should be directed to where the information is available. If the public body receiving a request for information does not hold the information, but knows that the information is available elsewhere, the requester should be directed to the place or organisation that holds the information.

14. Any public body that receives a request under EIRs for information relating to regulated reservoirs, which is not already publicly available, should

consider release of the information in accordance with the provisions of the legislation and the guidance provided by this Protocol.

Exceptions

15. Several exceptions from the public rights of access to environmental information exist under the legislation whereby a public body may refuse or withhold information, including that where its disclosure would adversely affect national security. The Environmental Information Regulations require that a test of the public interest in disclosure be conducted before any exception is applied (there is a greater presumption in favour of disclosure than under FOI).

16. National security should only be used as a reason for not disclosing information when deemed genuinely necessary, and retention or redaction of information must be justified. Adherence to this protocol maximises the disclosure of information to the public, whilst maintaining control of sensitive information. Considerations in favour of and against disclosure cannot be prejudged; one size does not fit all. The public interest must be considered in relation to each specific case. There may be a need to know and a public interest in disclosure. It is for each public body to assess the risks and make judgements about what information can and cannot be released.

17. Care needs to be taken, as once information is disclosed, it is in the public domain and the recipient can share the information without restriction with any other person and can combine the disclosed information with other sources of information.

18. Any public body in receipt of a request for reservoir information should refuse the request if an exception under the EIR applies and the "public interest test" is not satisfied.

19. Information should not be released where the public interest in maintaining the exception outweighs the public interest in disclosing the information. If in doubt a decision maker should contact their internal information manager before deciding whether to release the information.

Public Registers

20. Reservoir legislation requires that regulatory authorities maintain a register of certain information about regulated reservoirs and make this available to the public. The information to be contained in the public registers is prescribed in legislation. If information is requested that is held on the

public register, then the requester should be informed of how to inspect or access the register. Aggregated public register information may also be released.

Open Data

21. Information which can be made publicly available may also be placed on an Open Data Portal for use by the public. Information available on an Open Data Portal may be used for any purpose without restrictions.

Service Reservoirs

22. Service Reservoirs, i.e. sealed reservoirs which supply treated drinking water, present both a flood risk and a contamination risk. However, the exclusion of Service Reservoir information, through its absence, could draw attention to its importance. Therefore, while these reservoirs will be included on a public register the listing will not specifically indicate the purpose of the reservoir. For example, a service reservoir named "Bigwater SR" may be listed as "Bigwater". Service reservoir basic flood maps may also be produced and made public in accordance with this protocol i.e. the purpose of the reservoir should not be included.

Information contained in reports, etc.

23. Legislation may provide that reservoir reports, certificates, annexed drawings, etc. made by qualified civil engineers, or summaries of those documents, are placed on the public register. The contents of these reports, etc. may refer to reservoir vulnerabilities and liable to be considered OFFICIAL-SENSITIVE and should be redacted. All other information should be released. Measures required in the interest of safety could also indicate vulnerabilities and a response to an information request should be provided with all reference to vulnerabilities redacted. **Annex 1** provides detailed guidance on this.

Disclosure of information not held in a public register

24. Any public body that receives a request under EIRs for information relating to regulated reservoirs, which is not included within a public register, should consider release of the information only in accordance with the provisions of the legislation and the guidance provided by this protocol.

25. Further information on EIRs can be found at:

    - https://ico.org.uk/, or
    - http://www.itspublicknowledge.info/home/ScottishInformationCommissioner.aspx, or
    - https://ico.org.uk/about-the-ico/who-we-are/northern-ireland-office/

26. If in doubt a decision maker should contact their departmental information manager for advice.

27. Any public authority in receipt of an information request for reservoir information that is classified as OFFICIAL-SENSITIVE or SECRET should never disclose information that is classified "Secret" and should only release information classified as "OFFICIAL-SENSITIVE" if it is decided that it is in the public interest to do so. Even then it should be released on a need to know basis.

28. In addition to the public register requirements for reports, etc., Regulatory bodies may be asked to release full reports or other extensive information. These requests are subject to the appropriate rules for EIRs as set out above. The checklist at **Annex 1** provides indicative details of what should be considered sensitive information or aspects of vulnerability; these should generally be withheld.

29. Requests for information about reservoirs may include documents which include a mix of OFFICIAL publicly available information and OFFICIAL-SENSITIVE information about dam vulnerabilities or personal data. Documents marked OFFICIAL-SENSITIVE or higher to protect sensitive information may only be disclosed, with appropriate redaction, if doing so is in the public interest, and caution is advised to ensure the public interest test is sufficiently robust before the information is released.

30. Information on incidents affecting the safety of reservoirs may be collected. The raw information and original reports may contain information considered sensitive and, therefore, not suitable for public release. Where summary reports for public consumption are produced, these should be anonymised and all sensitive information removed before disclosure.

Protective security – determining what information is sensitive

31. The policy for protective security, and the sharing & handling of information is set out in the **Government Security Classification** v1 (Oct-2013) policy document produced by the Cabinet Office which came into force on 2 April 2014. This protocol does not alter or replace that guidance but provides

specific additional measures which should be taken to control access to particularly sensitive information.

32. Government Security Classification policy aims to ensure that information receives a uniform level of protection and treatment across all public bodies according to its degree of sensitivity. The security classifications are provided in **Annex 3**.

33. Information that is protectively marked OFFICIAL-SENSITIVE or higher should only be seen by those with a specific "need to know", and with the appropriate level of security clearance. This protocol sets out a proportionate approach to sharing reservoir flood maps and information.

Aggregation of information

34. Information may be requested which does not appear on the public register but which also may not be considered OFFICIAL-SENSITIVE. If this information is aggregated with other information of a similar nature, it may provide an increased knowledge of the subject reservoirs. Through the application of this protocol it is expected that the release of OFFICIAL information should not be at risk of any increased sensitivity when aggregated with other OFFICIAL information.

Reservoir flood maps

35. The general types of reservoir flood map have been categorised to indicate the level of sensitivity and the recommended security classification in **Table 1** below:

Table 1. Types of reservoir flood map and their indicative sensitivity.

Type	Summary Description	Intended Use	Protective Marking
Basic	A map showing the extent of the wetted area.	For warning and informing purposes, including public awareness.	OFFICIAL
Detailed	A map showing inundation characteristics limited to: depth, or velocity, or hazard derived from depth & velocity and time of flood arrival, time of peak flow. and/ or any information which conveys the likely or expected number or rate of fatalities which would result in the event of a reservoir failure.	For informing reservoir risk/ consequence designation, development planning or for generic or specific off-site emergency planning	OFFICIAL-SENSITIVE

Type	Summary Description	Intended Use	Protective Marking
Enhanced	A map showing any of the Detailed Map inundation characteristics with the addition of other consequence information listed in the section on 'Creation & Handling of Enhanced Maps'.	For specific off-site emergency planning and response	OFFICIAL-SENSITIVE (or SECRET in limited circumstances)
A generic off-site flood plan is an emergency plan devised to prepare for the failure of reservoirs in a locality and is based on the general consequences of failure, as indicated by the inundation maps A specific off-site flood plan is an emergency plan devised to prepare for the failure of a specific reservoir (or group of reservoirs) and based on the likely consequences of failure.			

Creation and handling of detailed maps

36. Detailed maps are normally produced to provide specific flood information for subject reservoirs. These should be marked OFFICIAL-SENSITIVE and should be handled, stored and/or shared with adherence to the protocols set out in **Annex 2**: Guidance for handling information. Creation and handling of enhanced maps

Creation and handling of enhanced maps

37. In routine circumstances, for example, preparing detailed emergency response procedures, enhanced maps may be created by Category 1 Responders, Government Departments and Agencies by overlaying geographical and impact information on to a basic or detailed map to create a single map that shows detailed consequences of reservoir failure. Enhanced maps may only be created by organisations essential to detailed emergency response arrangements, plans and procedures, and then only by individuals within those organisations with a security clearance of Baseline Standard or above.

38. The information listed below, if added to a basic or detailed map, will raise the map to enhanced and should normally only be added in exceptional circumstances:

    i. Any information or marks which identify infrastructure (e.g. hospitals, power stations etc.) as Critical National Infrastructure (CNI) or identify a point or area as being the location of CNI whether, or not, the type of infrastructure is indicated;

    ii. Any information which conveys the potential impact (on life or property) of the loss of a CNI asset;

    iii. Any information which indicates the number of people likely to occupy a building or premises at a given time within an indicated inundation zone; where the number is significant in size. For example: schools, public venues, stadia etc.

39. Where information needs to be added that identifies assets as CNI, the advice of the relevant CNI sponsor department must be sought first since they may require protective markings above OFFICIAL-SENSITIVE.

40. Where a reservoir flood map does not clearly fit the descriptions in Table 1; and / or the map contains references to structural damage to infrastructure (CNI or other infrastructure); and/or potential fatalities; and / or Likely Loss of Life values; and / or Fatality Rates, it may require classification as SECRET and advice should be sought from the information owner's security advisors.

41. Addition of information includes all electronic methods for overlaying information on to electronically stored maps as well as writing or printing on hardcopy maps. This includes adding any marks or symbols which, without reference to a separately and securely held reference source, would clearly convey any of the information described by above.

42. If the circumstances that required the creation of an enhanced map no longer exist; or one is inadvertently created, then all electronic and hard copies of the map should be destroyed in accordance with current security guidance.

Transmission & sharing of grouped information and maps

43. Where a set of detailed or enhanced maps, covering multiple reservoirs, is to be moved, shared or otherwise transmitted, then a judgement should be made as to whether additional precautions should be applied to minimise the loss of sensitive data and conceivably increase the likelihood of the subject reservoirs becoming a terrorist target. As a guide, when making this

judgement the following questions should be asked:

i. Does the information describe severe consequences of failure?

ii. Would the release of the information add significantly to the likely consequence of failure information (relating to the reservoirs in the set) that can be easily inferred from information already in the public domain?

iii. Does the information, when taken in aggregate, allow an assessment to be made as to the relative impact of the reservoirs in that set failing?

44. If the judgement is that a compromise of the grouped information or maps could conceivably increase the risk of terrorist threat to any of the reservoirs (e.g. if the answers to any of the three questions above is "yes") then additional precautions are advised. Alternatively, the information and/or maps should be transmitted in isolation of each other.

Annex 1: Reservoir information & data checklist

Requests for information must consider public interest factors. In applying public interest factors to common areas of reservoir information, the following table indicates whether the test favours the information to be:

- Withheld;
- Disclosed with redaction;
- Disclosed in full.

If the information requested includes the details of any individual person, the provisions of the Data Protection Act should be considered to establish if the information can be disclosed.

The general principle in releasing information is that it should not expose any vulnerabilities of a reservoir, such as structural details, faults, safety measures, etc. Requests for any documents, data or information not specifically mentioned in the table below, may be released following redaction in accordance with the principles above.

Annex 1.1 Information to be withheld	
Name & address or reservoir owner (n.b. see guidance for reservoir undertaker/ manager in **Annex 1.2**)	Withhold
Modifications, remedial works, history	
Overflow	
Dam flood category	
Dam and associated structures	
Inlet, outlet pipework, valves	
Scour	
Access	
Overflow structure/ tunnels	
Valve shaft and tunnel	
Inlet and outlet pipework and valves	
Seepages/ drainage flows	
Settlement, displacement and movement	
Emergency Plans	
Access for maintenance/ emergency	
Control of inflow	
Movement of surrounding land which might affect stability	
Adequacy and condition of waste weir overflow/ and channels	
Flood assessment	
Efficiency of scour pipe / other means of lowering water/ controlling inflow	
Measure(s) to be taken in the interests of safety	
Recommendation(s) from previous reports / status	
Flood calculations	
Valve schematic	
Construction drawings and photographs	
Incident reports and information relating to use of emergency powers	Withhold, unless it is considered items do not expose vulnerabilities.
Matters of mandatory maintenance (e.g. to be monitored by a supervising engineer.	
Directions given by the supervising engineer	

Annex 1.2 Information which may be disclosed subject to vulnerability checks	
Description of Reservoir	Disclose, omitting vulnerabilities
Geology	
Catchment	
Instrumentation	
Valley downstream of the dam	
Description of inspection and general conditions	
Wave surcharge and freeboard	
Area downstream of the dam	
Measures recommended in the interests of improving monitoring or supervision	
Recommendations as to non-safety related maintenance of the reservoir to be monitored or watched by the supervising engineer	
Matter(s) to be watched by the supervising engineer	
Enforcement notices	
Name, signature & date of engineer making the report, etc.	Disclose name & date, withhold signature
Site location plan Geological map showing location	Disclose maps/ plans showing general location of reservoir. Withhold plans showing layout of site
Photograph(s)	Disclose, unless the photographs/ drawings/ documents relate to vulnerabilities.
Drawing(s)/ document(s) available to the engineer	
Creation, certification, testing of flood plans	Disclose, unless required to be withheld by Regulation

Annex 1.2 Information which may be disclosed subject to vulnerability checks	
Name and business address of engineer	Disclose, unless subject to national security direction
Name, location and grid reference	Disclose, unless subject to direction to withhold
Risk / consequence designation	Disclose if public register info
Name & address of the reservoir undertaker or reservoir manager	Disclose
Panel and date(s) of appointment	
Method of recording water levels	
Recommendation as to date of next inspection	
Alterations to overflow sill	
Alteration in water storage level	
Seismic risk	
Supervision provided by undertakers/operators/ managers	
Correctness of records	
Other measures not requiring supervision by a qualified engineer	
Directions in respect of record keeping	
Method of recording water levels	

Annex 2: Guidance for handling information

The document Government Security Classifications sets out the general principles for storing, sharing and handling information with security classifications. This section provides advice on additional measures to be taken with information relating to regulated reservoirs.

Additional measures for handling OFFICIAL-SENSITIVE information

(a) Must not be made publicly available.

(b) Requests to view flood maps by professional partners who act as Category 1 Responders should initially be directed to access them from Resilience Direct to avoid unnecessary copying and sharing. However, information may be viewed at the premises where it is held, by a person who can identify themselves as being an employee or representative of any Category 1 or 2 Responder organisation (as per the Civil Contingencies Act 2004) with a clear need to view the information, and may be copied, retained and/ or removed from such premises provided this protocol is adhered to.

(c) In limited circumstances, e.g. for assessing the likely impact of failure of a reservoir to assign a dam category, to establish risk/consequence designation, or in the event of a statutory appeal, etc. then, at the discretion of the appropriate manager, permission may be given to the following people to view, but not copy, the information:

- i the owner, manager, undertaker or operator of the subject reservoir, or
- ii a statutorily appointed qualified civil engineer for the reservoir, or
- iii a statutorily appointed referee (e.g. to determine a dispute or appeal)

(d) Information or data produced by a public body or their consultants should incorporate an appropriate disclaimer; date of production; any licence restrictions, and a note on intellectual property rights.

(e) Flood map data may be sent electronically only if the media is encrypted with a minimum 128-bit encryption and marked with the security classification of "OFFICIAL-SENSITIVE" or higher.

(f) Must not be uploaded onto the internet. May be uploaded and downloaded without encryption within the OFFICIAL-SENSITIVE level environment of the Resilience Direct extranet or any other network with security equivalent to OFFICIAL-SENSITIVE level or higher.

(g) May only be sent by non-secure email when the attached files are marked clearly as OFFICIAL-SENSITIVE and secured by 128-bit encryption.

(h) May be sent unencrypted by secure email between two systems only when both the sender's and the recipient's email address contains ".gsi." or ".pnn." in the domain name and has a form of either:

- username@organisation.gsi.gov.uk, or
- username@organisation.x.gsi.gov.uk, or
- username@organisation.pnn.police.uk, or
- username@organisation.x.pnn.police.uk

(i) All attached files must be individually password protected.

Additional measures for handling SECRET information

(a) The information contained within original documents produced under reservoir legislation, and the production of reservoir flood maps showing flood extent, depth, velocity & hazard, is not generally anticipated to contain information that would require protection beyond OFFICIAL-SENSITIVE.

(b) It is conceivable that staff within Category 1 organisations or within government may need to overlay geographical and impact information from a variety of sources to create a combined document or data set that entails higher levels of protection, for example a Detailed map with additional data showing likely loss of life or impact on Critical National Infrastructure (CNI). Any organisation without secure methods of producing or storing electronic information at SECRET level or higher must not combine information which could raise the protective marking to SECRET. The information in the annex must be understood before any staff add or amend information to SENSITIVE information.

(c) Must not be uploaded onto the internet or the intranet.

(d) May be uploaded and downloaded within ICT network with security equivalent to SECRET level or higher.

(e) May not be sent to or from a non-secure email system.

(f) May be sent unencrypted by secure email between two systems only when both the sender's and the recipient's email address contains "x" in the domain name and has a form of either:

- username@organisation.x.gsi.gov.uk, or
- username@organisation.x.pnn.police.uk.

Annex 3: The UK Government protective marking scheme

The marking scheme is reproduced here for quick reference. For detailed consideration, the full Cabinet Office guidance should be referred to, see **References**.

	The UK Government Protective Marking Scheme
OFFICIAL (OFFICIAL-SENSITIVE)	OFFICIAL – This classification applies to most information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. There is no requirement to explicitly mark OFFICIAL information. OFFICIAL-SENSITIVE – Access to **sensitive** information must **ONLY** be granted based on a genuine "need to know" and an appropriate personnel security control. Where there is a clear and justifiable requirement to reinforce the "need to know", information should be conspicuously marked.
SECRET	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime. Should not be made publicly available and it should only be seen by those with a specific need to know, and with the appropriate level of security clearance.
TOP SECRET	Government's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations. This protocol does not consider this classification applies to any regulated reservoir information.

Annex 4: References

Legislation

Title	Legislation Years and Numbers	Legislation type
Reservoirs Act 1975	1975 c. 23	UK Public General Acts
Reservoirs Act (Northern Ireland) 2015	2015 c. 8	Acts of the Northern Ireland Assembly
Reservoirs (Scotland) Act 2011	2011 asp 9	Acts of the Scottish Parliament
Freedom of Information Act 2000	2000 c. 36	UK Public General Acts
Freedom of Information (Amendment) (Scotland) Act 2013	2013 asp 2	Acts of the Scottish Parliament
Freedom of Information (Scotland) Act 2002	2002 asp 13	Acts of the Scottish Parliament
The Environmental Information Regulations 2004	2004 No. 3391	UK Statutory Instruments
The Environmental Information (Scotland) Regulations 2004	2004 No. 520	Scottish Statutory Instruments

Information Commissioners

Office of the Information Commissioner
Northern Ireland Information Commissioner
https://ico.org.uk/about-the-ico/who-we-are/northern-ireland-office/
Scottish Information Commissioner

Government security marking

Security Policy Framework	April 2013	Cabinet Office
Government Security Classifications website	March 2014	Cabinet Office
Government Security Classifications	May 2018	Cabinet Office
Working with Official Information, v1.2	April 2013	Cabinet Office

Flood mapping

Supplementary Note on Flood Hazard Ratings and Thresholds for Development Planning and Control Purposes.	May 2008	Defra. (n.d.).

Annex 5: UK Reservoir Safety Liaison Group

This document has been produced by the UK Reservoir Safety Liaison Group. The members of the group are listed below:

Department for Environment Food & Rural Affairs	Department for Environment, Food & Rural Affairs Seacole Building, 2 Marsham Street London, SW1P 4DF
Department for Infrastructure An Roinn Bonneagair www.infrastructure-ni.gov.uk	Department for Infrastructure Reservoir Safety Team Room 15 Benson House 40a Benson Street, Lisburn, BT28 2BS
Scottish Government Riaghaltas na h-Alba gov.scot	Scottish Government Flood Risk Management Team Victoria Quay, Edinburgh, EH6 6QQ
Llywodraeth Cymru Welsh Government	Welsh Government Flood & Coastal Erosion Risk Management Cathays Park Cardiff, CF10 3NQ
Cyfoeth Naturiol Cymru Natural Resources Wales	Natural Resources Wales Reservoir Safety Team 29 Newport Road Cardiff, CF24 0TP
Environment Agency	Environment Agency Reservoir Safety Team Manley House Exeter, EX2 7LQ
SEPA Scottish Environment Protection Agency Buidheann Dìon Àrainneachd na h-Alba	Scottish Environment Protection Agency Strathallan House Castle Business Park, Stirling, FK9 4TZ

UK National Protocol

for the Handling, Transmission and Storage
of Reservoir Information and Flood Maps

UK Reservoir Safety Liaison Group
Version 2.4.5

JUNE 2018