

LIFE SMART Waste project

Smarter regulation of waste in Europe

LIFE13-ENV/UK/000549



Cyfoeth Naturiol Cymru
Natural Resources Wales



Contents:

- [1. Terms of Use](#)
 - [2. Privacy Statement](#)
-

Terms of Use

Important information about the Intelligence Communications Hub web pages.

We, the Scottish Environment Protection Agency (SEPA), provide a service called the Intelligence Communications Hub (“the Service”). The Service supports SEPA and Associated Beneficiary partners working under the LIFE SMART Waste Project by providing a web based portal and cloud platform (“Platform”) for increased collaboration and co-operation between international environmental regulators engaged in identifying and tackling serious waste crime. The technology behind the Service and its operation is provided by International Business Machines UK (“IBM”). As a member of this community you are encouraged to contribute and post material onto this Service and to access information and resources stored within. However, be responsible in what you contribute. In particular, make sure that none of the prohibited items listed below are included in any contributions you make to the Service or get linked to from the Service (for example spam, viruses, or hate content). SEPA and Associated Beneficiaries will not share any personal data collected through this Service with other organisations. See [here](#) for a Privacy Statement with full list of participating data controller organisations and their associated responsibilities in respect of managing personal data collected through this Service.

If you find any content that you believe violates these Terms of Use, please contact us at lifsmartadministrator@sepa.org.uk.

Terms of Use – the Details

1. Responsibility for Contributions

If you place comments or ideas on the Service, post material to the Service, post links on the Service, or otherwise make (or allow any third party to make) material available by means of the Service (any such material), ("Content"), you are entirely responsible for the content of, and any harm resulting from, that Content. That is the case regardless of whether the Content in question constitutes text, graphics, an audio file, or computer software. You understand that you are solely responsible for all electronic communications and Content sent by or on behalf of you. You must use the Platform for lawful purposes only.

You warrant that you will not use this Service otherwise than in accordance with these Terms. You must not use the Service in any way that causes or is likely to cause the Service or access to it to be interrupted, damaged or impaired in any way. By making Content available, you represent and warrant that:

1. The downloading, copying and use of the Content will not infringe the proprietary rights, including but not limited to the copyright, patent, trademark or trade secret rights, of any third party;
2. If your employer has rights to intellectual property you create, you have either (i) received permission from your employer to post or make available the Content, including but not limited to any software, or (ii) secured from your employer a waiver as to all rights in or to the Content;
3. You have fully complied with any third-party licenses relating to the Content, and have done all things necessary to successfully pass through any required terms to anyone else who accesses the Content;
4. The Content does not contain or install any software viruses, worms, time bombs, keystroke loggers, spyware, adware, malware, Trojan horses or other harmful or destructive content or similar computer code designed to adversely affect the operation of any computer software or hardware;
5. The Content is not spam, political campaigning, commercial solicitation, chain letter or mass mailings, is not machine- or randomly-generated, and does not contain unethical or unwanted commercial content designed to drive traffic to third party sites or boost the search engine rankings of third party sites, or to further unlawful acts (such as phishing) or mislead recipients as to the source of the material (such as spoofing);
6. The Content is not illegal, offensive, abusive, indecent, harmful, obscene or menacing, racist, threatening, pornographic, libellous or defamatory, does not contain threats or incite violence towards individuals or entities, is not in breach of confidence and does not violate the privacy or publicity rights of any third party or is otherwise injurious to third parties;
7. The Content does not cause annoyance, inconvenience or needless anxiety;

8. The Content is not used for fraudulent purposes or in connection with a criminal offence or otherwise to carry out any unlawful activity;
9. You will not reproduce, duplicate, copy or resell any part of the Service web pages or Content in contravention of these Terms of use;
10. You will not cause the Service Platform to be interrupted, damaged, rendered less efficient or such that the effectiveness or functionality of this Platform is in any way impaired;
11. By submitting Content to the Service, you grant us and the operator of the Service IBM UK a world-wide, royalty-free, and non-exclusive license to reproduce, modify, adapt and publish the Content solely for the purpose of carrying out their responsibilities to collect, share, analyse, create, review, amend and publish LSW project outputs and documentation. If you delete Content, we will use reasonable efforts to remove it from the Service, but you acknowledge that through caching or other references to the Content, Content may not be made immediately unavailable.
12. We will be free to use any responses you submit and any similar ideas or suggestions, without any [credit or] recompense to you.
13. Without limiting any of those representations or warranties, we have the right (though not the obligation) to, in our sole discretion (i) refuse or remove any Content that, in our reasonable opinion, violates any of our or IBM's policies or is in any way harmful or objectionable, or (ii) terminate or deny access to and use of the Services to any individual or entity for any reason, in our sole discretion.
14. You will not transmit any information containing sensitive material relating to ongoing criminal investigations, personal data, intellectual-property rights (IPR), commercial arrangements or subjects of interest to any regulatory body.

2. Responsibility of Service Visitors

We have not reviewed, and cannot review, all of the material, including computer software, posted to the Service, and cannot therefore be responsible for that material's content, use or effects. By operating the Service, we do not represent or imply that we endorse the material there posted, or that we believe such material to be accurate, useful or non-harmful. You are responsible for taking precautions as necessary to protect yourself and your computer systems from viruses, worms, Trojan horses, and other harmful or destructive content. Despite our efforts, the Service may contain content that is offensive, indecent, or otherwise objectionable, as well as content containing technical inaccuracies, typographical mistakes, and other errors. The Service may also contain material that violates the privacy or publicity rights, or infringes the intellectual property and other proprietary rights, of third parties, or the downloading, copying or use of which is subject to additional terms and conditions, stated or

unstated. We and IBM disclaim any responsibility for any harm resulting from the use by visitors of the Service, or from any downloading by those visitors of content there posted.

3. Third party website Content

We have not reviewed, and cannot review, all of the material, including computer software, made available through the websites and webpages to which the Service links, and that link to the Service. We do not have any control over those third party websites and webpages, and we are not responsible and/or do not accept liability for their contents or their use. By linking to a third party website or webpage, we do not represent or imply that we endorse such website or webpage. You are responsible for taking precautions as necessary to protect yourself and your computer systems from viruses, worms, Trojan horses, and other harmful or destructive content. We disclaim any responsibility for any harm resulting from your use of third party websites and webpages.

4. Copyright and Intellectual Property Rights

These Terms of Use do not transfer to you any intellectual property rights in the Service, and all right, title and interest in and to such property will remain solely with us and the Associated Beneficiaries, IBM or the specified third party owner where applicable. SEPA trademarks/logos, Associated Beneficiary trademarks and logos, IBM trademarks/logos and all other trademarks, service marks, graphics and logos used in connection with the Service, are trademarks or registered trademarks of SEPA, Associated Beneficiaries or IBM. Other trademarks, service marks, graphics and logos used in connection with the Service may be the trademarks of other third parties. Your use of the Service grants you no right or license to reproduce or otherwise use any SEPA, Associated Beneficiary, IBM or third-party trademarks.

5. Changes

We reserve the right, at our sole discretion, to modify or replace any part of these Terms of Use. It is your sole responsibility to check them periodically for changes. Your continued use of or access to the Service following the posting of any changes to these Terms of Use constitutes acceptance of those changes. We may also, in the future, offer new services and/or features through the Service (including, the release of new tools and resources). Such new features and/or services shall be subject to these Terms of Use

6. Termination

We may terminate your access to all or any part of the Service at any time, with or without cause, with or without notice, effective immediately. All provisions of these Terms of Use which by their nature should survive termination shall survive termination,

including, without limitation, ownership provisions, warranty disclaimers, indemnity and limitations of liability.

7. Disclaimer of Warranties

The Service is provided "as is". SEPA, IBM and its suppliers and licensors and parent or associated companies hereby disclaim all warranties of any kind, express or implied, including, without limitation, the warranties of merchantability, satisfactory quality, fitness for a particular purpose and non-infringement. Neither SEPA, IBM nor its suppliers and licensors, makes any warranty that the Service will be error free or that access thereto will be continuous or uninterrupted. You understand that you download from, or otherwise obtain content or services through, the Service at your own discretion and risk.

8. Limitation of Liability

In no event will SEPA, IBM, or its suppliers or licensors, be liable with respect to any subject matter of these Terms of Use under any contract, negligence, statutory or other legal or equitable theory for:

1. Any special, incidental or consequential damages, including but not limited to loss of profits, loss of revenue, loss of business, howsoever caused and whether direct or indirect;
2. The cost of procurement or substitute products or services;
3. For interruption of use or loss or corruption of data; or

Neither SEPA nor IBM shall have liability for any failure or delay due to matters beyond their reasonable control. The foregoing shall not apply to the extent prohibited by applicable law.

9. General Representation and Warranty

You represent and warrant that (i) your use of the Service will be in strict accordance with the Privacy Policy, [here](#) these Terms of Use and with all applicable laws and regulations (including without limitation any local laws or regulations in your country, state, city, or other governmental area, regarding online conduct and acceptable content, and including all applicable laws regarding the transmission of technical data exported from the United Kingdom or the country in which you reside) and (ii) your use of the Service will not infringe or misappropriate the intellectual property rights of any third party.

10. Indemnification

You agree to indemnify and hold harmless SEPA, IBM, their contractors, and licensors, and their respective directors, officers, employees and agents from and against any and

all liabilities, losses, damages, costs, claims and expenses, including lawyers' fees, arising out of your use of the Service, including but not limited to your violation of these Terms of Service.

11. Miscellaneous

These Terms of Service constitute the entire agreement between SEPA and you concerning the subject matter hereof, and may only be modified through the posting by SEPA of a revised version. These Terms of Use, any access to or use of the Service will be governed by and construed in accordance with Scots Law, and any dispute shall be subject to the exclusive jurisdiction of the Scottish Courts. If any part of these Terms of Use is held invalid or unenforceable, that part will be construed to reflect the parties' original intent, and the remaining portions will remain in full force and effect. A waiver by either party of any term or condition of these Terms of Use or any breach thereof, in any one instance, will not waive such term or condition or any subsequent breach thereof. You may assign your rights under these Terms of Use to any party that consents to, and agrees to be bound by its terms and conditions; SEPA may assign its rights under these Terms of Use without condition. This Agreement will be binding upon and will inure to the benefit of the parties, their successors and permitted assignees.

12. System Operating Procedures

Users of the Service must comply with the following System Operating Procedures ("SyOps") security guidance.

12.1 Security Classification

The Platform can only be used to store, manage and review data up to a classification of, or equivalent to, **OFFICIAL** under the UK government security classification scheme (GSC).

If you find that data has been inadvertently imported that exceeds this level you should seek advice from SEPA's Information Technology Security Officer (ITSO) or Information Security Officer (ISO) and inform the Service Administrator. Do not try to rectify the problem yourself.

12.2 Access to the Service Platform

The Service is hosted on an IBM, 3rd party supplied, commercial off-the-shelf, cloud based, data sharing and collaboration Platform.

Access to the Platform must only be made from each individual organisation's approved desktop and laptop workstations.

SEPA and external partner organisation members are not permitted to utilise any of IBM Application Programming Interface (API) functionality.

The copying or storage of any data originating from the Platform to any external mobile devices such as (but not limited to) USB memory sticks, portable hard drives, CD and DVD drives is expressly prohibited.

12.3 Roles and Responsibilities

Administrator and Assistant Administrator – The Service Administrator is responsible for managing the IBM Platform account and is the main liaison with IBM. They are responsible for the creation and management of member accounts and in inviting or accepting users onto the Service. SEPA will be responsible for providing resource to undertake this role and to ensure resilience will further appoint an Assistant Administrator.

Community Manager – Responsible for managing the contents of folders within their allocated communities, inviting users to their workspace, monitoring activity on the workspaces and changing setting of their workspaces.

Community Member (collaborator) – Member of topic based workspace or workspaces with ability to access associated documents and resources, create, amend and post their own contributions and documents and to access associated collaborative and real time communications tools.

General Member – Able to view and access general Platform functionality toolkits, knowledgebase, help and support, meeting and communications facilities.

All terms within the SyOps must be followed therefore all users must comply with any variance between these SyOps and IBM's own system Terms of Use.

All roles must refer to and comply with the detailed work instructions and associated data process flows provided through online help and support facilities.

All users are reminded that the data being accessed from the Platform must only be used for the specific purpose of carrying out their responsibilities for collaborative working under the LIFE SMART Waste project.

12.4 Account and Password Management

Applicants to join the Service and gain access onto the Platform will be required to register their details through an online form including account and password details.

All users will be identified to the Service and gain access to the Platform through their unique combination of username and password.

File and folder permissions are used on this system. The Community Manager is responsible for the authorisation of individuals to gain access to their communities and associated workspace folders, files and is responsible for monitoring content and ensuring that folder permissions are reviewed monthly.

All users must protect their passwords at all times. Passwords are security “keys” which protect the content of the computer system to which they control access. Passwords **must** be treated with the same care that would be given to the information they protect. Passwords, which control access to the collaborative Platform, **must be protected**.

- a) Passwords must not be written down.
- b) Passwords must not be disclosed to other people – even another authorised user of the system, line manager or IT staff

- c) Passwords must have a minimum of nine (9) characters in length and a maximum of sixteen (16) characters
- d) Passwords must contain a minimum of at least one upper case alphabetic character and one lower case alphabetic character
- e) Passwords must contain a minimum of at least one numeric character.
- f) Passwords must contain at least one special character from the list - £ \$ % ^ & * () _ + : ~ # ! *
- g) Passwords must not contain a sequence of repeated alphabetic, numeric or special characters.
- h) Passwords must not be based on easily guessable or individually attributed words or phrases such as names, places, birthdates, etc.
- i) Passwords previously used for access to the system cannot be re-used and passwords must not be an incremental variant of a previously used password giving access to the Platform.
- j) Passwords should not be the same as passwords used for access to other work or personal IT systems.
- k) If a user forgets their password or locks themselves out of their account on the Platform the user must send an email message from their personal organisational email address to the SEPA Service Administrator requesting that their password is reset. On receipt the SEPA Service Administrator will invoke a password reset via the Platform procedures.
- l) If a user suspects that their password has become known it must be changed immediately
- m) Users must not give access to the Platform to anyone else using their log-on credentials

12.5 Prohibited Use

- a) The system and data must not be used for personal work.
- b) When connected to the Platform the computer **must not** be left unattended at any time. If you are away from your desk for a short time you must engage the screen lock by pressing Ctrl-Alt-Delete, then selecting "Lock". If you think you will be absent for longer than 30 minutes then the desktop / laptop must be shutdown
- c) All users **must not** store or copy any data from the Platform on to their local workstation (desktop or laptop). If a user requires saving information locally this must be saved to a local shared network drive folder which has sufficient security applied thereto to protect the information at **OFFICIAL** level.
- d) All users are advised that all transactions carried out on the system are logged and a full audit trail of all system access is automatically created.
- e) System audit trails may be checked periodically within each organisation with access to the Platform to ensure that this SyOps is being complied with.

12.6 Desktop Sharing

Users of web conferencing facilities on the Platform must ensure that screen sharing of applications and documents on their Desktop is restricted only to those of relevance to the meeting.

Detailed guidance is available on-line through the Platform.

12.7 Data Submissions

Community Members must submit data under any Platform feature for analysis and development of LSW project deliverables in compliance with provided work instructions or if subject of formal request via an interim staging workspace within the Platform so that it can be subject to a quality assurance vetting procedure.

Detailed data submission process and work instructions are available on-line through the Platform.

12.8 Recording of Web-conferences

The Platform supports the optional recording of tele-conferences to allow for more effective minuting of meetings. Meeting members should be made explicitly aware of and consent to any proposal to record meetings through meeting invitations or at the start of the meeting.

12.9 Access via Police National Network (PNN)

Users must ensure that under the PNN's agreed terms of use that the Platform is not accessed from the PNN.

12.10 Security Incident Reporting and Management

A security incident is any event which either results in an actual security breach or creates potential for a security breach to occur. Prompt action might prevent a simple incident from becoming a major incident.

- a) Any person discovering a Security Incident which affects the Platform must report it immediately via their organisation's standard Security Incident Reporting Policy and Internal Procedures. The person discovering the Incident must also report the circumstances to their line manager.
- b) Failure to report a Security Incident is a serious matter, which could result in consideration being given to disciplinary action (dependent upon each Organisation's policy).
- c) Each organisation undertakes to review all Security Incidents involving the Platform without delay and to advise the other partners of the circumstances via the Service Administrator (appointed by SEPA) who will act as coordinator for all security incidents. The SEPA Departmental Security Officer and / or the SEPA Information Security Officer must be advised of all Security Incidents in respect of the Platform occurring both within and out with SEPA's control.
- d) A review of the incident must take place and an assessment made as to whether or not this has / could affect the other partner organisation's security or if any data held by another partner organisation has been disclosed.
- e) If at any times it is suspected that any of the data held on the Platform could be infected by a virus or other malware or the integrity of Platform data is in doubt urgent consideration must be made to disabling all system access to all partner organisations, the public and the Platform provider whilst further investigation occurs.
- f) If any malicious activity is suspected to have occurred every effort should be made to preserve the evidence (e.g. audit log files) for potential forensic examination should the matter become criminal.
- g) A list of security contacts within each partner organisation will be collated by the SEPA System Administrator. This list will contain details of each partner organisation's security professionals such as the Departmental Security Officer (DSO), the Information Security Officer (ISO) and the Information Technical Security Officer (ITSO) or their equivalents.

If you **suspect a system fault**, this must be reported immediately to the SEPA Information Technology Security Officer (ITSO) and Intelligence Hub Administrator. You **must not** attempt to rectify it yourself.

12.11 Review

This Terms of Use must be reviewed annually and it must be updated if any changes to the procedures contained herein are amended during the course of a year. The LSW Project Workspace Administrator will coordinate the annual review of this SyOps.

Privacy Statement

By providing the information below you are accepting the processing of your personal data as set out in the privacy statement.

Scottish Environment Protection Agency (SEPA) and Associated Beneficiaries under the LIFE SMART Waste project have joint data controller responsibilities in accordance with EU Directive 95/46/EC as transposed into the National Data Protection Laws of the Parties for the processing of personal data submitted by users of the Intelligence Communications Hub service including data processing by International Business Machines Corporation (IBM) who host the supporting collaborative software platform IBM Connections Cloud S2.

IBM's own Online Privacy Statement including their policy on the use of Cookies can be accessed [here](#).

The Associated Beneficiaries are:

- NRW (Natural Resources Wales), United Kingdom
- ACR+ (Association of Cities and Regions for Recycling and Sustainable resource Management), Belgium
- IBGE-BIM [Institut Bruxellois pour la Gestion de l'Environnement – Brussels Instituut voor Mileubeheer ("Bruxelles Environnement – Leefmilieu Brussel")], Belgium

During the process of applying to join the service or accepting an invitation to join the service we will ask you to provide the following information:

- Title
- Surname
- Forename
- Company / Organisation Name
- Business Contact Phone Number
- Business e-mail Address
- Job Description
- Sponsor or Line Manager details (Name, Position and Contact details)
- Areas of Interest

By providing this information you will be deemed to have given your consent to the following processing of your personal data.

SEPA and the Associated Beneficiaries will process details or instruct IBM to process details of the above items for the express and sole purpose of carrying out their responsibilities under the LIFE SMART Waste project to:

- Establish the credentials of applicants registering to join the general service;
- Establish and maintain secure personal accounts and logins for users of the online collaborative software platform;
- Establish controlled access within the service to specific communities and associated software features and data;
- Distribute LIFE SMART Waste project newsletters.

Please note that SEPA and the Associated Beneficiaries and IBM as data processor will only retain your details for the period that the Intelligence Communications Hub and supporting collaborative software platform is being piloted under the LIFE SMART Waste project currently May 31st 2019. Upon customer's written request SEPA, the Associated Beneficiaries and IBM as data processor will destroy or return all personal data made available to the service.

Please address any questions, comments and requests regarding the processing of your data to: lifsmartadministrator@sepa.org.uk

ANNEX A - Form of Undertaking

This form must be completed and returned to the Account Administrator or Workspace Manager by every Authorised User of the IBM S2 Connections/Intelligence Communication Hub prior to using this system.

A User will not be invited to the IBM S2 Connections/Intelligence Communication Hub until a signed form, together with all other necessary signed documentation, has been received and accepted by the Account Administrator or Workspace Manager.

- I have read and understand the Intelligence Communication Hub Terms & Conditions and System Operating Procedures including the Hub service Privacy Statement (This document).
- I understand my responsibilities as a User of the IBM S2 Connections/Intelligence Communication Hub.
- When I have received my IBM S2 Connections/Intelligence Communication Hub invitation I will create a suitable username and password.
- I will protect my password and not reveal it to any other person for any reason.
- If I suspect that my password has been compromised I will inform SEPA's ISO, Account Administrator & Workspace manager immediately and will complete a security incident report supplied by SEPA.
- I will inform SEPA's Account Administrator if and when I no longer need my account on the IBM S2 Connections/Intelligence Communication Hub.
- I acknowledge that my use of the IBM S2 Connections/Intelligence Communication Hub will be monitored.
- I agree to adhere to IBM S2 Connections/Intelligence Communication Hub Terms of Use and the Data Sharing Agreement between SEPA and the external partner organisation.
- I undertake to observe the IBM S2 Connections/Intelligence Communication Hub Security Operating Procedures and to take all reasonable precautions to ensure that I do not breach the security of IBM S2 Connections/Intelligence Communication Hub.

I understand that if I fail to observe IBM S2 Connections/Intelligence Communication Hub Security Operating Procedures my account on the IBM S2 Connections/Intelligence Communication Hub will be suspended and the matter will be subject to SEPA's Disciplinary Procedures for SEPA personnel or the equivalent pursued in external partner organisation.