



Grant Agreement No. 687676

Innovation Action

ICT-20-2015

D1.9 Data Management and Ethics Process Plan

Due date	Month 24
Actual date	Month 23
Deliverable author(s)	Anna Barenbrock, Jakob Baalsrud Hauge, Heiko Duin, Christian Gorldt
Partner(s)	BIBA, ATS, COVUNI, GEOMOTION, HFC, HWU, Ifinity IMA, INESC TEC, ORT, UCM, SEBIT, SIVECO
Contributors	Cristina Alonso, Jannicke Baalsrud Hauge, Jayne Beaufoy, Massimiliano Cazzaniga, António Coelho, Olivier Heidmann, Neil Judd, Tom Kawka, Theo Lim, Leonel Morgado, Luca Morini, Marius Preda, Antoniu Ştefan, Ioana Andreea Ştefan, Malte Sudmann, Ali Turker, Pau Yanez
Version	1
Status	Final
Dissemination level	Public

Project Coordinator

Coventry University

Sylvester Arnab

Priory Street, Coventry CV1 5FB, UK

E-mail: s.arnab@coventry.ac.uk

Project website: <http://www.beaconing.eu>

This project has received funding under the Horizon 2020 Framework Programme of the European Union – Grant Agreement No. 687676



Version control				
Version	Date	Author	Institution	Change and where applicable reason for change
0.1	08.09.2017	Anna Barenbrock	BIBA	Table of content and structure and first input of Ethical Guidelines
0.2	12.09.2017	Anna Barenbrock	BIBA	Input for new ethical guidelines and our FAIR Data Management Plan.
0.3	12.09.2017	Neil Judd	HFC	Input of component information
0.4	14.09.2017	Massimiliano Cazzaniga	IMA	Input of mini games component information
0.5	15.09.2017	Theo Lim, Tom Kawka, Luca Morini, Olivier Heidmann, Pau Yanez, Cristina Alonso	HWU, Ifinity, COVUNI, ORT, GEOMOTION, UCM	Input of Fair Data Management Access Plan tables.
0.6	16.09.2017	Anna Barenbrock	BIBA	Revision of partner input
0.7	17.09.2017	Jannicke Baalsrud Hauge	BIBA	Revision and comments
0.8	20.09.2017	Anna Barenbrock	BIBA	Incorporate comments
0.10	12.10.2017	Anna Barenbrock	BIBA	Incorporated language check, edited the introduction
0.12	13.10.2017	Anna Barenbrock	BIBA	Incorporated comments from internal review, added annex, edited introduction, swapped chapters, deleted the components tables in chapter 3.2.
0.13	13.10.2017	Jakob Baalsrud Hauge	BIBA	Added the conclusion
0.14	14.10.2017	Antoniu Ştefan, Ioana Andreea Ştefan	ATS	Revision and comments
0.15	29.10.2017	Jannicke Baalsrud Hauge	BIBA	Revision and comments
0.16	02.11.2017	Heiko Duin	BIBA	Language check, revision and comments.

0.17	02.11.2017	Anna Barenbrock	BIBA	Incorporated comments, edited the data security chapter, introduction, executive summary and FAIR Data.
0.18	03.11.2017	Leonel Morgado	INESC TEC	Small language corrections, data backup plan for Portugal pilot, clarification on its users and ethical guidelines.
0.19	06.11.2017	Anna Barenbrock	BIBA	Incorporated SEBIT's info on ethical guidelines, revision of the entire document.
0.20	06.11.2017	Christian Gorldt	BIBA	Language check, revision and comments.
0.21	06.11.2017	Anna Barenbrock, Malte Sudmann	BIBA	Incorporated revision and comments. Revision of the entire document. Layout. Finalising the document.
0.22	14.11.2017	Anna Barenbrock	BIBA	Incorporated internal reviews from UCM and INES TEC, final revision, layout.
0.23	30.11.2017	Anna Barenbrock	BIBA	Incorporated feedback from QM.

Quality control				
QA Version	Date	QA Responsible	Institution	Change and where applicable reason for change
0.9	03.10.2017	Jayne Beaufoy	COVUNI	Language Check
0.11	13.10.2017	Cristina Alonso	UCM	Revision and comments.
0.21	10.11.2017	António Coelho	INESC TEC	Internal review.
0.21	14.11.2017	Cristina Alonso	UCM	Internal review
1	30.11.2017	Jayne Beaufoy	COVUNI	Language Check

Release approval				
Version	Date	Name	Institution	Role
0.22	28.11.2017	Ioana Andreea Ștefan	ATS	QM

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Contributors

Contributors				
Version of document contributed to	Chapter	Contribution description	Institution	Name of contributor
0.3	3.1 & 4.2	Filled in information about log-in data and personal settings in chapter 3.1. Filled in information about the access plan for the Accessabar in chapter 4.2.	HFC	Neil Judd
0.4	4.1 & 4.2	Input for 4.1 about metadata of minigames. Input about the access plan for minigames in chapter 4.2	IMA	Massimiliano Cazzaniga
0.5	4.2	Input for 4.2 about the open accessible research data.	HWU, Ifinity, COVUNI, ORT, GEOMOTION, UCM	Theo Lim, Tom Kawka, Luca Morini, Olivier Heidmann, Pau Yanez, Cristina Alonso
0.7	Entire document	Revision and comments	BIBA	Jannicke Baalsrud Hauge
0.9	Entire document	Language check	COVUNI	Jayne Beaufoy
0.11	Entire document	Revision and comments	UCM	Cristina Alonso
0.15	Entire document	Revision and comments	BIBA	Jannicke Baalsrud Hauge
0.15	2.1	Info about what data minigames can collect in pilots.	SIVICO	Marius Preda
0.16	Entire document	Language check, revision and comments.	BIBA	Heiko Duin
0.16	2.2	VET GLP Data management	HWU	Theo Lim
0.18	2.2 & 4	Small language corrections, data backup plan for Portugal pilot, clarification on its users and ethical guidelines.	INESC	Leonel Morgado
0.19	2.2	Data Backup Plan for Turkey pilot	SEBIT	Ali Turker
0.19	3.1.1	Clarification of Minigames Metadata	IMA	Massimiliano Cazzaniga
0.20	Entire document	Language check, revision and comments	BIBA	Christian Gorltd
0.21	Entire document	Layout	BIBA	Malte Sudmann

0.21	Entire document	Internal Review	INES TEC	António Coelho
0.21	Entire document	Internal Review	UCM	Cristina Alonso

TABLE OF CONTENTS

EXECUTIVE SUMMARY..... 8

1 INTRODUCTION..... 9

1.1 BACKGROUND9

1.2 ROLE OF THIS DELIVERABLE IN THE PROJECT9

1.3 APPROACH.....9

1.4 STRUCTURE OF THE DOCUMENT9

2 DATA MANAGEMENT 10

3 FAIR DATA 12

3.1 MAKING DATA FINDABLE 12

3.1.1 *Minigames* 12

3.1.2 *Asset Library* 13

3.2 MAKING DATA OPENLY ACCESSIBLE..... 13

4 ETHICAL GUIDELINES 15

5 CONCLUSION 17

6 REFERENCES..... 18

ANNEX I: ETHICAL GUIDELINES..... 19

DEFINITION OF TERMS

Abbreviation	Description
CNPD	Comissão Nacional de Protecção de Dados
DBS	Disclosure and Barring Service
FAIR	Findable, accessible, interoperable and reusable (regarding research data)
GLP	Gamified Lesson Plan
ORDP	Open Research Data Pilot
POI	Point of Interest
VET	Vocational Education Training

EXECUTIVE SUMMARY

The BEACONING project carries out the development of a platform that will be used by full-aged persons, as well as minors and vulnerable groups. Therefore, it is vital that data, which concerns and is produced by the users, are handled with care. This is the third of fourth deliverable regarding data management and ethics and defines how the consortium needs to handle data of different kinds.

This document describes which kind of sensitive data are handled within the project internally and explains how those data are secured, where they are saved and who has access to them. Afterwards, the data backup plan is described, which ensures that the BEACONING platform can still be used after a server crash.

BEACONING's participation in the Open Research Data Pilot (ORDP) implies that the project will make its data FAIR (Findable, Accessible, Interoperable and Reusable). As the software is in its Beta version now, the document describes how metadata is used to make data findable. The consortium also presents their plan on how to make data accessible.

The document also contains the ethical guidelines, which are used by the pilots that have started in month 18.

1 INTRODUCTION

This document further develops the guidelines made in D1.8, which were not possible to address earlier, due to too many uncertainties in the piloting and the early stage in software development.

The first part of this deliverable is about the Data Management Plan. In two separate sections, it is discussed how BEACONING handles data within the project and how the consortium plans to contribute to the Open Research Data Pilot (ORDP). Therefore, FAIR Data aspects will be described in more detail, which were not specified in the earlier deliverables.

Moreover, ethical guidelines have been developed in close collaboration with the pilots' ethical committees, in order to ensure that all pilot sites will comply with regional and national regulations, procedures and deadlines.

1.1 BACKGROUND

The BEACONING Platform is in its Beta version now. The individual components were integrated in the core system and the overall architecture and data structure appears clearer. Also, the structure and preparation of the small-scale pilots were further developed and detailed. Therefore, this deliverable focuses on handling sensitive data and provides ethical guidelines for each of the pilots.

1.2 ROLE OF THIS DELIVERABLE IN THE PROJECT

While the software is still under final developments, it appears in more detail which data BEACONING handles and collects, and this document is updated regularly throughout the project. This deliverable contributes to the work of all work packages. This document sets the guidelines for ethics, as well as for handling data of all kinds. This includes how data is treated within the software architecture, but also how to proceed and secure data outside the BEACONING Platform, e.g. questionnaire results. Therefore, this deliverable is necessary to ensure that all partners comply with the agreements. The ethical part of this document is mostly relevant for WP5 and WP6, which focus on the small and large-scale pilots. This deliverable will be updated once more at the end of the project, in month 36.

1.3 APPROACH

As the BEACONING project handles many different kinds of data, the data security is vital for the consortium. Therefore, we worked closely with the technical partners ATS, UCM, INESC TEC, IMA and HFC to define their internal process on data security. The other technical partners were also involved, but due to the software architecture, data security is handled in the core system. Furthermore, this deliverable ensures the adherence of regulations and national laws for each pilot. The ethical guidelines were created in close collaboration with the pilot's ethics committees.

1.4 STRUCTURE OF THE DOCUMENT

The document is composed of 5 chapters. Chapter 1 gives an overview about the document. Chapter 2 focuses on the data management part, including data security and a data backup plan. The third chapter is about the projects' FAIR data management plan and elaborates on the metadata system. This chapter is followed by the ethical guidelines and the conclusion. As this document further develops the realization on Data Management and Ethics, no familiar information written in D1.7 and D1.8 will be repeated here.

2 DATA MANAGEMENT

This Data Management Plan describes where the data handled in BEACONING is saved internally and who has access to it, in order to ensure data security of sensitive information.

2.1 Data security

Personal settings, e.g. for the Accessabar, as well as log-in data are stored in the core services of the BEACONING platform in a MySQL database. It is de-personalized, while the passwords are encrypted using bcrypt. Besides the associated users who can access their data through normal tool operations, only server administrators have access to the overall infrastructure. For offline access to the platform, the personal settings are also saved to the local browser storage which is called upon login and when settings are changed by the user.

Location-based data is not saved in the platform. The information is only relevant for in-game actions to detect whether a point-of-interest (POI) has been reached.

All in-game data, such as scores from minigames, will be sent to the analytics server and saved in Elasticsearch documents and JSON files, following the xAPI-SG model. All data is de-personalized prior to sending, according to the open data architecture plan, described in D1.8. The access to the analytics server is managed via the authorization and authentication component in the core system. Students will only have access to their own data, while teachers will have access to specific individual student's data and data aggregated by a class. The only data that can be seen by teachers involves the analytics of the student's progress in the Gamified Lesson Plans (GLP) (e.g. how many correct and incorrect answers were given in a quiz, time spent on a certain task, etc.) and the student's profile page. Students will decide what information they want to make visible. Developers will only have access to condensed analytics data, compounded by the data generated by students.

Minigames do not save any in-game data in their backend but rather send data instantly to the analytics server. Only configurations made by teachers will be stored in the minigames, in order to ensure a personalized experience. Depending on the type of minigame, it is possible to track the number of correct and incorrect answers, number of skipped questions, duration of time spent for each question, duration of time spent in-game, if a game has started or ended, the text of each answer, number of times help used and number of attempts.

Questionnaires used to assess user requirements in small-scale pilots are de-personalized (no personal information about gender or age are requested) and cannot be traced back to the participants. Nevertheless, the answers contain sensitive data such as impairments the participants have, a workshop ID, and in case of the teachers also a timestamp of the date and time the questionnaire was filled out. That is why the consortium also handles the raw data with care. They are saved in a MySQL database on a BIBA server which is protected by a complex password composed of at least 12 characters including numbers, special characters and capital and small letters. Only authorized BIBA staff, working on BEACONING has access to the server files and can give access to other project members, if they are the owner of the data or it is reasonable due to task allocation.

2.2 Data Backup Plan

Certain data, such as login data and the users' progress in tasks, needs to be backed up within the system. Otherwise, it might happen that students cannot access their account or have to repeat a whole mission again, if a server crashes.

Therefore, the following **Data Backup Plan** shows how often data will be backed up in order to ensure BEACONING runs reliably.

The initial BEACONING architecture run by ATS provides that data is backed up daily on external storage mediums that are rotated weekly to a secondary offsite location. The external storage mediums are encrypted and recovery certificates can only be accessed by enterprise system administrators.

Some piloting partners will run their own instance of BEACONING, which means that they will have complete control of the infrastructure. Therefore, the following paragraphs describe how these pilots plan to manage data and carry out backups.

The pilot run by Heriot-Watt University focuses on Vocational Education Training (VET). VET GLP data will be digitised with indexable referencing but contain no personalised information. Present data concerns only those relating to questionnaires answered during the VET GLP pilots. The digital data is stored locally and also backed up to HWU research server once a month. Only authorised personnel can access the data. Hard copies of questionnaires are secured within the facility and only accessible by personnel directly working on BEACONING. Hard copies will be kept for the duration of the project and no longer than two years post project. Where changes to VET GLP requires re-trial, all prior data will be destroyed. All digitised questionnaire data will be transferred to the BEACONING central server when it is ready. VET game traces will be handled as per Section 2.1.

The pilot run by INESC TEC focuses on programming education at college level and will run on ATS servers. BEACONING data will have user IDs but no personal information, which will remain in the college-controlled systems. Association between BEACONING IDs and college IDs will not be part of the BEACONING data but managed by college-controlled systems, and under its own organizational backup procedures. This association will be kept for five years to comply with current legal requirements of assessment tracking, and subsequently destroyed.

The pilot run by SEBIT will couple SEBIT's national platform with BEACONING so that user authentication will be on SEBIT's platform and BEACONING lesson plans (GLPs) will be presented alongside others (marked as Beta). When users choose BEACONING lesson plans, they will be handed over to the BEACONING ecosystem. The data generated in such lesson plans will be reported in BEACONING and kept there. If the demand exceeds the capacity provided by ATS, a BEACONING instance can be installed in local servers, and the data management procedures by ATS can be replicated locally. However, SEBIT will not process the data for any other purpose than legally allowed. BEACONING software will process the data, report to the user or use it to adapt the lesson flow/materials.

De-personalized questionnaires and answers are separate from the core system and run on a BIBA server. The data gets backed up once a day. Only authorised BIBA personnel has access to the backup server and can recreate the data for BEACONING.

3 FAIR DATA

The following chapter describes updates in the FAIR Data plan, which is about making research data "findable, accessible, interoperable and reusable" [1].

3.1 MAKING DATA FINDABLE

Since each component belonging to the BEACONING platform handles different kinds of data, the following paragraphs will describe the component-specific data management scenario in detail.

3.1.1 Minigames

Regarding the minigames component there are two types of data that will be stored in the minigames backend:

- Game data generated by the users (teachers and players)
- Minigames' source code and documentation

Regarding the first point, according to the minigames component architecture detailed in the technical deliverable D3.6, minigames handle only anonymous game data, a user identifier token, and a game session identifier will be sent to the minigame client in order to let the game load the correct configuration. All the other relevant in-game player's metrics (points, levels, time spent, correct or wrong answers, etc.) will be sent to the Learning Analytics platform and will not be stored into the minigames backend. The minigame backend only stores the games configuration instances created by the teachers.

More in detail, the games configuration instances metadata stored in the minigames backend are the following:

- **Anonymous OAuth2 user token:** This ID identifies the player anonymously inside the authenticated session.
- **GLP ID:** This ID identifies the GLP the minigame instance belongs to.
- **Author ID:** Field aimed at storing access control metadata at authoring time. This ID will be used by the minigames to call an external core service to check if the author ID (provided by the Authoring Tool) is authorized to modify or edit the selected minigame instance.
- **Minigame configuration instance ID:** This ID identifies the specific minigame instance. It can be passed to the minigame by the meta game web view in order to launch a specific minigame instance.
- **Minigame configuration content:** List of fields in JSON notation with all the settings of a specific minigame instance (e.g. language, topic, sub topic, questions text, answers text, timers, bonuses for the player, etc.)
- **Last update timestamp:** Time of the last update action on a specific minigame instance.
- **Learning Analytics flags:** A list of optional KPIs relevant for the teacher. Using this fields at authoring time will be possible for the teacher tell the minigame that some metrics such as the overall time spent on the game, or the number of bonuses used must be tracked and sent to the Learning Analytics platform.

The minigames' client source code will be made available in the open BEACONING repository. Third party stakeholders can use or modify it without asking permission. The minigames backend will not be made available as an open asset since it is built upon proprietary technology, but due to the standard and decoupled architecture, it will be easy for third party developers to adapt their web-based minigames' client to other custom backends.

The minigames configuration documentation will be made available in the BEACONING open repository and could be used by third party developers to learn how to define, for each minigame, a set of configuration files that will make these minigames "authorable" using the official BEACONING authoring tool.

3.1.2 Asset Library

A detailed description of the asset management can be found in D4.1, the deliverable describing the Integrated BEACONING Ecosystem. The BEACONING platform allows the use of implicit and explicit metadata. Whereas implicit metadata originates by the file's physical characteristics, such as the name or size, explicit metadata is generated by a person or an automated process judging the asset; this could include a ranking of a file or a categorization.

Besides the metadata which is generated by the users, collected information about the usage of each asset will be stored automatically. To enhance the search function of the platform, metadata of assets is used to create relationships between assets.

3.2 MAKING DATA OPENLY ACCESSIBLE

As part of the ORDP, the aim of BEACONING is to make as much research data as possible openly accessible for third parties to enhance the progress and speed of research. The BEACONING consortium will use the green open access route, meaning that the project members will take care of granting open access to their publications via an online repository [1].

Reviewed publications (papers, articles, book chapters, etc.):

As described in the H2020 Programme Guidelines [1], the publications must be deposited in an online repository not later than the day the scientific article is officially published (Please see the "Guidelines on FAIR Data Management in Horizon 2020" [1] for data format regulations). The BEACONING consortium will use one repository for all their publications: ZENODO. It can be reached by following this URL:

https://zenodo.org/communities/beaconing_eu

The benefit of this repository is that it comprises a holistic way to deposit scientific publications, as well as research data in one place.

Underlying data:

Data which is needed to validate the scientific publications will also be deposited in ZENODO at the date the article is published at the latest.

Embargo time:

The consortium reserves the right to use the authorised embargo time of 6 months, if needed. This means, the deposited publications and underlying data must be made openly accessible not later than 6 months after the official publication.

Open access:

Open access allows third parties to “access mine, exploit, reproduce and disseminate (free of charge for any user) this research data” [2]. For this purpose, BEACONING will attach an appropriate Creative Commons Licence to the deposited data.

Research data:

It is uncertain yet, what other data will be produced during the BEACONING project by each partner. Data might be gathered during the pilots but it has not been decided what data will be saved for what reason. The consortium agrees on never giving access to raw data and to use the right of the embargo time for research data.

4 ETHICAL GUIDELINES

The BEACONING small scale pilots started at the end of June 2017. Therefore, the ethical guidelines have been revised for each pilot in order to ensure that all pilots comply with regulations, legislations and deadlines for applications.

Partners provided input for modifications or completions that had to be made to the descriptions in Deliverable D1.7 and Deliverable D1.8, which can be seen in the list below. The entire ethical guidelines for each pilot can be seen in ANNEX I: Ethical Guidelines.

Overall changes: Due to organisational reasons, the suggestion of D1.7 to collect in addition to written also oral consent from full-aged participants is removed. Participants of legal age will only sign a pilot specific consent form.

- 1. United Kingdom:** The pilot leaders apply for ethics through their universities by filling out an ethical form. If working with minors, a Disclosure and Barring Service (DBS) check [3] will be conducted, unless the pilots will be guided through the teachers.
- 2. Germany:** As described in D1.7 and D1.8.
- 3. France:** As described in D1.7 and D1.8.
- 4. Greece:** The planning is not fully finalized yet as the pilot conditions can still vary in their details. Therefore, the complete ethical guidelines are not listed the Annex and will be delivered in D1.10, subsequently, at the end of the project.
- 5. Turkey:** Pilots led by SEBIT will incorporate BEACONING lesson plans in their own widely used system, which has many lesson plans embedded that are used by students across the nation. The Turkish ethical committee states that students using the system, as well as their parents and the according schools accepted to use the lesson plans served by SEBIT. Therefore, the BEACONING lesson plans will inherit the same consent, which means permission will not be asked again, as those large-scale pilots will not gather any user data. Small-scale pilots will adhere to the process as described in D1.7 and D1.8.
- 6. Portugal:** The pilot will involve college students, which are likely or mostly adults. In case the pilot works with minors, the Comissão Nacional de Protecção de Dados (CNPD) [4] will be contacted.
- 7. Romania:** Minor participants will not provide verbal consent before participating in the pilot, as this would require additional consent from the parents. Instead, they will be provided with a separate consent form (additional to the one filled out by the parents), as it must be ensured that the students understand the instructions and that they agree to participate in the workshops. Therefore, this form will be signed by the students.
- 8. Italy:** The small-scale pilot in Italy is newly added and will work with underage students as well as teachers. The school has already provided a letter of intent to the partner in charge of this pilot (IMA). The format will be a short series of workshops, some meetings with students and teachers will be organised in order to let them test and evaluate the BEACONING platform from both the teacher and the student side. These workshops will be carried out as a traditional in-classroom activity, potentially extended to some intra school missions to test out also the location-based component. All these activities will

be carried out under the presence of teachers, and considered that no in-game data will be stored, but only an anonymous product feedback survey will be required to be completed; there is no need for the school to ask for a formal consent to students' parents. According to the outcomes of the first meetings it will be decided if an extra school location-based mission will be organised. In this case, a specific agreement from parents will be provided.

5 CONCLUSION

This deliverable puts its focus on the Data Management and Ethics in BEACONING. It also describes the ODRP and its realization in the project. It is an indicator on which terms all members of the consortium agreed on regarding how we handle data, store it, which kind of data and when it will be accessible for third parties.

This deliverable shows the advances in the fields of data management and data security that have been made during the last 11 months. Ethical Guidelines have been developed in close collaboration with the ethical committees, in order to ensure that all pilots comply with national laws and regulations before starting their workshops. All of our work has been done according to D1.7 and D1.8. Therefore, all generated and collected data is FAIR to the highest extent possible and abides the Horizon 2020 guidelines.

The next deliverable will be provided in month 36. This is aligned with the end of the project and will therefore show the final decisions regarding FAIR data, Ethical Guidelines and the Data Management Plan.

6 REFERENCES

1. European Commission (2016, July 26). H2020 Programme: Guidelines on FAIR Data Management in Horizon 2020 (Version 3.0). Retrieved October 13, 2017, from: http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf
2. European Commission (2017, March 21). H2020 Programme: Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020 (Version 3.2). Retrieved October 13, 2017, from: http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf
3. Wikipedia (2017, October 11). Disclosure and Barring Service. Retrieved October 13, 2017, from: https://en.m.wikipedia.org/wiki/Disclosure_and_Barring_Service
4. Comissão Nacional de Protecção de Dados. Retrieved October 13, 2017, from: https://www.cnpd.pt/english/index_en.htm

ANNEX I: ETHICAL GUIDELINES

Ethical Guideline – United Kingdom – Coventry

Checklist

- Ensure all members of the project received the introduction on Ethical Guidelines for the BEACONING project, as described in D1.7 chapter 2.2
- DBS check for working with minor, unless the pilot will work through the teachers
- Letter to headteacher / principal of school
- Apply for ethics through university
- Letter to parents, including consent form.
- Inform all participants (oral & written) as described in D1.7 Chapter 2.2.3
- Always get written informed consent from participants BEFORE starting the experiment.
 - In case the participant is either minor or a vulnerable adult, written consent is needed from parent/carer/responsible.

The minor/vulnerable adult must give additional consent verbally (Full name and declaration that (s)he understood the process, risks and options of the experiment and agrees with all of this). This consent must be recorded and safely stored.
 - Participants who may be classed/class themselves as vulnerable, may request the presence of an advocate when considering participation in the study.
 - Individuals may also request the presence of an advocate during the trial. In this case a disclosure statement will be required for the advocate in their observer role.
- Store the written consents locally in a secure place and the digital oral consents encrypted on a local device. Send an encrypted scan of all informed consents to the project manager.
- Whenever a participant withdraws, it is her/his decision whether the data collected so far will be used for research purposes. If not, all data will be destroyed (paper forms) or deleted (electronic data).
- No payment of incentives or rewards to participants will be made.

Ethical Guideline – United Kingdom – HWU

Checklist

- Ensure all members of the project received the introduction on Ethical Guidelines for the BEACONING project, as described in D1.7 chapter 2.2
- Letter to headteacher / principal of school
- Fill out ethical form.
- Inform all participants (oral & written) as described in D1.7 Chapter 2.2.3
- Always get written informed consent from participants BEFORE starting the experiment.
- Store the written consents locally in a secure place and the digital oral consents encrypted on a local device. Send an encrypted scan of all informed consents to the project manager.
- Whenever a participant withdraws, it is her/his decision whether the data collected so far will be used for research purposes. If not, all data will be destroyed (paper forms) or deleted (electronic data).
- No payment of incentives or rewards to participants will be made.

Ethical Guideline – Germany

Checklist

- Ensure all members of the project received the introduction on Ethical Guidelines for the BEACONING project, as described in D1.7 chapter 2.2
- Letter to head of institution about BEACONING installations within the building
- Inform all participants (oral & written) as described in D1.7 Chapter 2.2.3
- Always get written informed consent from participants BEFORE starting the experiment.
- Store the written consents locally in a secure place. Send an encrypted scan of all informed consents to the project manager.
- Whenever a participant withdraws, it is her/his decision whether the data collected so far will be used for research purposes. If not, all data will be destroyed (paper forms) or deleted (electronic data).
- No payment of incentives or rewards to participants will be made.

Ethical Guideline – France

Checklist

- Ensure all members of the project received the introduction on Ethical Guidelines for the BEACONING project, as described in D1.7 chapter 2.2.
- Send a declaration to CNIL regarding the data collection on students.
- Letter to headteacher / principal of school.
 - Include the information that the usage of mobile devices could be allowed during a precise timeframe.
- Letter to parents, including consent form.
- Inform teachers and students about the BEACONING installation before they will enter the covered area (e.g. central notice, email or poster on the relevant classroom door).
- Inform all participants (oral & written) as described in D1.7 Chapter 2.2.3
- Always get written informed consent from participants BEFORE starting the experiment.
 - In case the participant is minor, written consent is needed from parent/carer/responsible.

The minor must give additional consent verbally (Full name and declaration that (s)he understood the process and risks of the experiment, as well as and the option to withdraw at any time and agrees with all of this). This consent must be recorded and safely stored.
- Store the written consents locally in a secure place and the digital oral consents encrypted on a local device. Send an encrypted scan of all informed consents to the project manager.
- Whenever a participant withdraws, it is her/his decision whether the data collected so far will be used for research purposes. If not, all data will be destroyed (paper forms) or deleted (electronic data).
- No payment of incentives or rewards to participants will be made.

Ethical Guideline – Turkey

Checklist

- Ensure all members of the project received the introduction on Ethical Guidelines for the BEACONING project, as described in D1.7 chapter 2.2
- For experimentation purposes:
 - Letter to headteacher/Principal of school
 - Letter to parents, including consent form.
 - Inform all participants (oral & written) as described in D1.7 Chapter 2.2.3
 - Always get written informed consent from participants BEFORE starting the experiment.
 - In case the participant is minor, written consent is needed from parent/carer/responsible.

The minor must give additional consent verbally (Full name and declaration that (s)he understood the process, risks and options of the experiment and agrees with all of this). This consent must be recorded and safely stored.
 - Store the written consents locally in a secure place and the digital oral consents encrypted on a local device. Send an encrypted scan of all informed consents to the project manager.
- For large-scale pilots with exploitation purposes:
 - Users (students, parents, schools) already accepted the use of SEBIT lesson plans. BEACONING lesson plans will fall into this category and “inherit” the consent.
 - No user data will be collected by the pilot leaders. User data is only used by the system in a closed loop to give feedback for users.
- Whenever a participant withdraws, it is her/his decision whether the data collected so far will be used for research purposes. If not, all data will be destroyed (paper forms) or deleted (electronic data).
- No payment of incentives or rewards to participants will be made.

Ethical Guideline – Portugal

Checklist

- Ensure all members of the project received the introduction on Ethical Guidelines for the BEACONING project, as described in D1.7 chapter 2.2
- Inform the CNPD
- Letter to headteacher/principal of school/rector/college president
- For users that are minors, letter to parents/guardian, including consent form.
 - The minor must give additional consent verbally (full name and declaration that (s)he understood the process, risks and options of the experiment and agrees with all of this).
- Inform all participants (oral & written) as described in D1.7 Chapter 2.2.3
- Always get written informed consent from participants BEFORE starting the experiment.
- Store the written consents locally in a secure place and the digital oral consents encrypted on a local device. Send an encrypted scan of all informed consents to the project manager.
- Whenever a participant withdraws, it is her/his decision whether the data collected so far will be used for research purposes. If not, all data will be destroyed (paper forms) or deleted (electronic data).
- No payment of incentives or rewards to participants will be made.

Ethical Guideline – Romania

Checklist

- Ensure all members of the project received the introduction on Ethical Guidelines for the BEACONING project, as described in D1.7 chapter 2.2
- Letter to headteacher/Principal of school
- Inform teachers and students about the BEACONING installation within the school, where it is localized and what it is used for.
- Letter to parents, including consent form.
- Inform all participants (oral & written) as described in D1.7 Chapter 2.2.3
- Always get written informed consent from participants BEFORE starting the experiment.
 - In case the participant is younger than 16, written consent is needed from parent/carer/responsible.

The minor must give additional consent verbally (Full name and declaration that (s)he understood the process, risks and options of the experiment and agrees with all of this). This consent must be recorded and safely stored.
 - In case of participating students with special needs, the supervising teacher needs to obtain the acceptance of the students' parents/carer/responsible.
- Store the written consents locally in a secure place and the digital oral consents encrypted on a local device. Send an encrypted scan of all informed consents to the project manager.
- Whenever a participant withdraws, it is her/his decision whether the data collected so far will be used for research purposes. If not, all data will be destroyed (paper forms) or deleted (electronic data).
- No payment of incentives or rewards to participants will be made.

Ethical Guideline – Italy

Checklist

- Ensure all members of the project received the introduction on Ethical Guidelines for the BEACONING project, as described in D1.7 chapter 2.2
- Letter to headteacher / principal of school
- Letter to parents, including consent form, if an extra geolocalised game will be conducted. If no in-game data will be saved, no consent from parents is needed.
- Inform all participants (oral & written) as described in D1.7 Chapter 2.2.3
- Always get written informed consent from participants BEFORE starting the experiment.
 - In case the participant is minor/vulnerable adult (s)he must give additional consent verbally (Full name and declaration that (s)he understood the process, risks and options of the experiment and agrees with all of this). This consent must be recorded and safely stored.
- Store the written consents locally in a secure place and the digital oral consents encrypted on a local device. Send an encrypted scan of all informed consents to the project manager.
- Whenever a participant withdraws, it is her/his decision whether the data collected so far will be used for research purposes. If not, all data will be destroyed (paper forms) or deleted (electronic data).
- No payment of incentives or rewards to participants will be made.