



Dublin City University  
School of Computing  
ETHICS COMMITTEE (SEC)

NOTIFICATION FORM FOR LOW-RISK  
PROJECTS AT UNDERGRADUATE OR  
TAUGHT MASTERS LEVELS

**Please read the following information carefully before completing your application. Failure to adhere to these guidelines will make your submission ineligible for review.**

1. Download this form, complete the appropriate fields, attach additional pages (e.g. plain language statement) as appropriate and save as a PDF file
2. Completed applications must be uploaded to your School of Computing GitLab repo, and must be located in "docs/ethics.pdf".
3. Your SUPERVISOR will then be notified automatically and must approve your approach initially.
4. Your application should consist of **one electronic file (PDF) only**. The completed application must include this form and also must incorporate all supplementary documentation, especially that being given to the proposed participants e.g consent forms, plain English language statement. It must be proofread and spell-checked before submission.
5. All sections of the application form must be answered as instructed and within the word limits given.
6. Your ethics approval submission will be circulated to the School's Research Ethics Committee and you will be notified if/when it is approved
7. All projects must have either a derogation from an ethics approval requirement (as determined by your supervisor) OR must have an approved ethics submission (this form), before work with human subjects commences.

Applications which do not adhere to these requirements will not be accepted for review and will require resubmission

Applications must be completed on this form; answers in the form of attachments will not be accepted, except where indicated. No hard copy applications will be accepted. **The project must not commence work with human subjects until written approval has been received from the School of Computing Ethics Committee (SEC).**

PROJECT TITLE	ICE
PROJECT SUPERVISOR(S)	Renaat Verbruggen
START AND END DATE	27-01-20 to 11-05-20

Please ensure that **all** supplementary information is included in your application (in one electronic copy). If questionnaire or interview questions are submitted in draft form, please indicate this by putting (draft) after YES. A copy of the final documentation must be submitted for final approval when available.

<b>My application has been collated as one electronic file which includes the following documentation:</b>	<b>INCLUDED (mark as YES)</b>	<b>NOT APPLICABLE (mark as N/A)</b>
Bibliography		N/A
Recruitment advertisement (How are you getting volunteers?)		N/A
Plain language statement/Information statement	<b>YES</b>	
Informed consent form	<b>YES</b>	
Personal Data Security Schedule <a href="https://www.dcu.ie/sites/default/files/info/3_blank_data_security_schedule.xls">https://www.dcu.ie/sites/default/files/info/3_blank_data_security_schedule.xls</a>		N/A
Evidence of external approvals related to the research		N/A
Questionnaire/Survey		N/A
Interview/Focus Group Questions		N/A
Debriefing material		N/A
Other (e.g. local government approval )		N/A

Please note:

- Any amendments to the original approved proposal must receive prior SCEC approval.
- As a condition of approval investigators are required to document and report immediately to SCEC any adverse events, any issues which might negatively impact on the conduct of the research and/or any complaint from a participant relating to their participation in the study

## 1. ADMINISTRATIVE DETAILS

Project Type (select one): Undergraduate Project – Final Year

YES

Undergraduate Project – non-final Year

Taught Masters (Practicum)

(projects at other levels, e.g. PhD or research Masters, should be approved by the University's REC if necessary)

### 1.1 INVESTIGATOR CONTACT DETAILS

**SUPERVISOR(S):** *Your supervisor and other academic staff who are assisting, it should be clear who is the person who is carrying out the research procedures.*

NAME	SCHOOL/UNIT	EMAIL
Renaat Verbruggen	School of Computing	renaat.verbruggen@dcu.ie

**STUDENT(S):**

NAME	SCHOOL/UNIT	EMAIL
Catherine Mooney	School of Computing	catherine.mooney33@mail.dcu.ie
Hannah O'Connor	School of Computing	Hannah.oconnor26@mail.dcu.ie



---

**DECLARATION BY SUPERVISOR(S)**

*The information contained herein is, to the best of my knowledge and belief, accurate. I have read the University's current research ethics guidelines, and accept responsibility for the conduct of the procedures set out in the attached application in accordance with the form guidelines, the SCEC guidelines (<https://www.dcu.ie/researchsupport/researchethics.shtml>), the University's policy on Conflict of Interest, Code of Good Research Practice and any other condition laid down by the Dublin City University Research Ethics Committee. I have attempted to identify all risks related to the research that may arise in conducting this research and acknowledge my obligations and the rights of the participants.*

*If there exists any affiliation or financial interest for researcher(s) in this research or its outcomes or any other circumstances which might represent a perceived, potential or actual conflict of interest this should be declared in accordance with Dublin City University policy on Conflicts of Interest.*

*I and my co-investigators or supporting staff have the appropriate qualifications, experience and facilities to conduct the research set out in the attached application and to deal with any emergencies and contingencies related to the research that may arise.*

**Electronic Signature(s):**

Supervisor(s): \_\_\_\_\_ *Renaat Verbruggen* \_\_\_\_\_

Print Name(s) here: \_\_\_\_\_ Renaat Verbruggen \_\_\_\_\_

Date: \_\_16/03/2020\_\_

## 2. PROJECT OUTLINE

### 2.1 SIMPLE DESCRIPTION (Max. 300 words)

*Please outline, in terms that any non-expert would understand, what your research project is about, including what participants will be required to do. Please explain any technical terms or discipline-specific phrases.*

ICE is a cross-platform iOS and Android personal safety mobile application. Upon downloading, each user would sign up with their details (E.g Name, Age) and a phone number. For the phone number, we would have a drop down of country codes to choose from for their supplied phone number. Before the user can access the app, they will receive a verification code. Once verified, the user will be unable to log out, as each account is directly linked to a specific phone number. Once the phone number is verified, they will automatically be directed to their SMS application on their mobile, where the correctly formatted text will be available to register them to 112, the emergency text service.

The user will then be logged in and allowed to edit their app. They will have the option to add a profile picture and edit their medical information which will be stored in the app. The user's home screen will contain spaces where they can add other users to their circle of trust, and an emergency button, where once activated will contact, if available, the member of the user's chosen circle of trust.

In terms of user testing, we plan to conduct focus groups and questionnaires based on their experience. We ourselves will perform cognitive walkthroughs, by entering random details and not using any real personal information.

### 2.2 AIMS OF AND JUSTIFICATION FOR THE RESEARCH (Max. 400 words)

*State the aims and significance of the project. Where relevant, state the specific hypothesis to be tested. Please provide a brief description of background research, a justification as to why this research project should proceed in that context and an explanation of any expected benefits to the community. NB – all references cited should be listed in an attached bibliography.*

Safety has always been a big concern and priority for adults and their children. From doing regular day to day errands, to making your way home, alone, especially at night. Parents are constantly worried about where their children are and if they made it to their destination ok. Young girls have the constant fear of getting into taxis unaccompanied or walking down unlit streets. Men and women of all ages are aware of the on-going dangers faced by society today. It's inevitable that people have to make trips alone, be it short or long journeys. But it wouldn't be near as daunting if you have reassurance that your guardians know where you are and that help is easily accessible. While we have many uses for our smartphone devices, one thing that it could have great purpose for is personal safety. This is where our application comes into use, providing that reassurance and extra comfort for those within today's society, through your phone.

The name comes from the well known 'In Case of Emergency' and we took inspiration from the name ICE for the app's logo. The app will be designed for all types of user, with the idea being that only those within your trusted circle of contacts can monitor your real time location, communicate and be updated with notifications and alerts about your current status. Our mission is to establish a platform aiding those without protection and help to make a difference to when a situation could get serious. We plan to develop a simple web application alongside this, one that can be accessed via phone or desktop as another means of receiving updates from those within your inner circle. The central idea behind the application is that the app can provide a variety of personal safety features rather than just containing an SOS button and GPS tracking. Most personal safety apps developed globally are delivered on a subscription basis and we believe that the price of safety should be free of cost.

### 2.3 DESCRIBE THE METHODOLOGY BEING USED TO ACHIEVE YOUR STATED AIMS

*Provide an outline of the proposed method and state who is doing which task – include details of data collection techniques, the tasks participants will be asked to do, the estimated time commitment involved, and how data will be analysed. If the project includes any procedure which is beyond already established and accepted techniques please include a description of it. There should be enough detail provided to facilitate ethical review, but applicants are encouraged to keep it as succinct as possible.*

When first using the app, users need to register before being able to login. The registration form requires the new user to enter a valid mobile number. This step is crucial as it is how we will ensure the student can access the app, as the app is linked to one mobile number and you are unable to log out. The telephone number must be in the correct format, so we have provided a drop down list of country codes that the user must choose from. Other basic information is required, like name, age, etc. After successfully registering, each user will have the option to upload a profile image of their choice, and record a safe word, however, these steps are not required. Upon users requesting others to join their network, their profile information (which includes their name, profile image) and location is required to be shared with the relevant users. The user must be aware of said persons phone number, in order to request them to join their network. The users location will be made available for those members of the specific network, and they can be tracked only when they have specifically requested.

### 2.4 PARTICIPANT PROFILE

*Provide the number, age range and source of participants. Please provide a justification of your proposed sample size. Please provide a justification for selecting a specific gender, age, or any other group if this is done in your project.*

For this, our plan is to solely use mocked test data. Given that our application deals with medical information for instance, we find that it would be inappropriate to ask for such personal data. In spite of that, once the application is completed and published, regular user data will be encrypted. The main requirements for our test profiles would be a valid mobile phone number. Within our backend provider, Firebase, we have the ability to include test phone numbers as an alternative. Our application doesn't specify any age or gender that must be required, just that an age must be entered and one of the genders must be chosen. Other required user input required upon registration would include: password, date of birth, full name, medical information (optional), profile picture (optional), defined user safe zone (e.g Home, also optional). The goal for this section of development is to create enough mocked user profiles to establish a complete circle of trust with the aim to test it's overall functionality.

For the completely anonymous questionnaires, the source of our participants will be our course peers. We can expect a number of 20 or less participants with a assumed age range of 20 to 25.

Given that we are recruiting our families, friends and peers as the source for the cognitive walkthroughs, we can expect around 10 or less participants with a bigger diversity among the age groups and genders, where the age of any given participant could be within the range of 20 to 60.

#### 2.4(a) PARTICIPANT VULNERABILITY

*Are some or all of participants vulnerable in any way? (e.g by virtue of the group they belong to, people who have undergone traumatic or adverse emotional events, people with diminished cognitive ability, power relations between researchers and participants etc.)? If they are, state what this vulnerability (or vulnerabilities) is and justify why this research is being done with such participants.*

As discussed in the previous sections, participants will not be found vulnerable given our decision not to use real user data for testing the applications functionality. Also, our application will tackle user vulnerability in the sense that if they feel unsafe in any way, our application provides multiple means to notify their network of trust and/or emergency services.

**2.4(b) CHILD PARTICIPANTS (anyone under 18 years old)**

If your participants include children, you **must** confirm that you are in compliance with the research specific guidelines as detailed in "Keeping Children Safe - Policies and Procedures supporting Child Protection at DCU" - available at: [https://www4.dcu.ie/sites/default/files/policy/157%20-%20child\\_protection\\_handbook\\_rev1%282%29%281%29.pdf](https://www4.dcu.ie/sites/default/files/policy/157%20-%20child_protection_handbook_rev1%282%29%281%29.pdf)

We won't be using child participants in the conduction of this user testing.

Please indicate your compliance with the following guidelines:	Mark here
We confirm that we have read and agree to act in accordance with the DCU Child Protection policy and procedures	N/A
We confirm that we have put in place safeguards for the children participating in the research	N/A
We confirm that we have supports in place for children who may disclose current or historical abuse (whether or not this is the focus of the research)	N/A

**2.5 EXPLAIN HOW PARTICIPANTS ARE TO BE RECRUITED**

Please provide specific details as to how you will be recruiting participants. How will people be informed that you are doing this research? How will they be approached and asked if they are willing to participate? If you are mailing or phoning people, please explain how you have obtained their names and contact details. If a recruitment advertisement is to be used, please ensure you attach a copy to this application.

For our 1-1 cognitive walkthroughs, participants will be chosen through word of mouth. Those being our families, friends and peers and will be supplied with the necessary user consent form.

**2.6 PLEASE EXPLAIN WHEN, HOW, WHERE, AND TO WHOM RESULTS WILL BE DISSEMINATED, INCLUDING WHETHER PARTICIPANTS WILL BE PROVIDED WITH ANY INFORMATION AS TO THE FINDINGS OR OUTCOMES OF THE PROJECT?**

For the cognitive walkthrough testing, we will be directly addressing the participant feedback to improve our application, hence the actual information won't be given but instead our participants will have the opportunity to view our finish product that was based on the entire participant feedback.

**2.7 ARE OTHER APPROVALS REQUIRED TO GAIN ACCESS TO ANOTHER LOCATION, ORGANISATION ETC.? (e.g. a School or company)**

YES or NO

NO

(If YES, please specify from whom and attach a copy of the approval documentation. If this is not yet available, please explain when this will be obtained.)

### 3. RISK AND RISK MANAGEMENT

#### 3.1 JUSTIFICATION OF STATED LEVEL OF RISK TO RESEARCH PARTICIPANTS

*You must provide a justification for the stated level of risk, as indicated on the cover page of your application. Note that the level of risk may be influenced by the vulnerability of the research group, the methods employed and the nature of the research itself. For further information on risk levels, please refer to the Levels of Review information on the website: <https://www.dcu.ie/researchsupport/researchethics.shtml>*

The level of risk to the research participant is associated with the data entered into the app. However we will not be using any real user information so no actual personal information will be stored in our database.

Participant users who would use this app will do so voluntarily. However, basic information including their phone number, name, etc, is required upon registration. We require approval for this app as users are sharing that personal information and location with the app, which is stored within its database and is able to be viewed by other users within their personalized circle of trust. (There will be an optional toggle for the user to disable location to any of the circles members). User's location is shared among a user's circles, in order for those within it to be aware of their real time current location on a private map. We will be using google maps to power this. The phone number of users is needed for signing up purposes and we will be leveraging a user's device SMS functionality for inviting others to their private circle and/or sending an emergency text. For android users, this aspect will be completely programmatically and for iOS, the SMS message can be initialized but cannot be sent on behalf of the user (they must click send).

For the social media feed aspect of our application, no user information, including phone numbers, will be shared within it. Our plan is to develop it as an anonymous feed. It's used for the posting of safety posts to members given a certain geographical area in the hopes of benefitting our users.

#### 3.2 DOES THE RESEARCH INVOLVE:

	YES or NO
• use of a questionnaire? (attach copy)?	NO
• interviews (attach interview questions)?	NO
• observation of participants without their knowledge?	NO
• participant observation (provide details in section 2)?	YES
• audio- or video-taping interviewees or events?	NO
• access to personal and/or confidential data (including student, patient or client data) without the participant's specific consent?	NO
• administration of any stimuli, tasks, investigations or procedures which may be experienced by participants as physically or mentally painful, stressful or unpleasant during or after the research process?	NO
• performance of any acts which might diminish the self-esteem of participants or cause them to experience embarrassment, regret or depression?	NO
• investigation of participants involved in illegal activities?	NO
• procedures that involve deception of participants?	NO
• administration of any substance or agent?	NO
• use of non-treatment of placebo control conditions?	NO
• collection of body tissues or fluid samples?	NO
• collection and/or testing of DNA samples?	NO
• participation in a clinical trial?	NO
• administration of ionising radiation to participants?	NO

#### 3.3 POTENTIAL RISKS TO PARTICIPANTS AND RISK MANAGEMENT PROCEDURES

*Identify, as far as possible, all potential risks to participants (physical, psychological, social, legal, economic, etc.), associated with the proposed research. Please explain what risk management procedures will be put in place to minimise these risks.*



As discussed, each participant will be supplying “fake” profiles into the app. In the case where the application requires adding members to their circles, the contacts being read from the device will belong to those said profiles. The only real user data to be required in our testing will be pseudonymized, that is users’ mobile phone number. Read/Write rules have been strictly enforced within the app’s database where the data kept and it is too encrypted as an extra measure.

**3.4 ARE THERE LIKELY TO BE ANY BENEFITS (DIRECT OR INDIRECT) TO PARTICIPANTS FROM THIS RESEARCH?**

YES or NO  
YES

*(If YES, provide details.)*

The main benefit being that they can contribute to this future application through providing their feedback. As developers we can take that feedback directly and improve it accordingly.

**3.5 ARE THERE ANY SPECIFIC RISKS TO RESEARCHERS?**

*Examples include use of dangerous materials, asking certain types of questions, research being undertaken in certain locations, researchers working alone in isolated areas, etc.*

YES or NO  
NO

*(If YES, please describe and explain what risk management procedures will be put in place to minimise these risks.)*

**3.6 DEALING WITH ADVERSE/UNEXPECTED OUTCOMES**

*Please describe what measures/protocols you have put in place in the event that there are any unexpected outcomes or adverse effects to participants arising from involvement in the project.*

The users will be provided with a means of contacting the app developers directly through the ICE application. Users will not be expected to perform cognitive walkthroughs or follow me sessions or any map functionalities, these details will be performed and entered manually by the developers to ensure the users safety.

**3.7 HOW WILL THE CONDUCT OF THE PROJECT BE MONITORED?**

*Please explain how the supervisor will monitor the conduct of the project (especially where several people are involved in recruiting or interviewing, administering procedures, etc.) to ensure that it conforms with the procedures set out in this application*

We will meet face-to-face with our supervisor on a regular basis throughout the semester and are also able to connect virtually via email. Throughout the meetings, we are advised on anything we require along with documenting and critiquing our progress at each phrase, ensuring that we stay on track.

### 3.8 SUPPORT FOR PARTICIPANTS

*Depending on risks to participants you may need to consider having additional support for participants during/after the study. Consider whether your project would require additional support, e.g., external counselling available to participants. Please advise what support will be available.*

Throughout the development process and after the successful completion of our project, if any participants were to have any related queries or concerns, there will be a private email address supplied within the User consent form in which they can contact either developers.

### 3.9 DO YOU PROPOSE TO OFFER PAYMENTS OR INCENTIVES TO PARTICIPANTS?

YES or NO

NO

*(If YES, please provide further details.)*

### 3.10 DO ANY OF THE RESEARCHERS ON THIS PROJECT HAVE A PERSONAL, PHILOSOPHICAL, FINANCIAL OR COMMERCIAL INTEREST IN ITS OUTCOME THAT MIGHT INFLUENCE THE INTEGRITY OF THE RESEARCH, OR BIAS THE CONDUCT OR REPORTING OF THE RESEARCH, OR UNDULY DELAY OR OTHERWISE AFFECT THEIR PUBLICATION?

YES or NO

NO

*(If YES, please specify how this conflict of interest will be addressed.)*

## 4. CONFIDENTIALITY/ANONYMITY

### 4.1 WILL THE IDENTITY OF THE PARTICIPANTS BE PROTECTED?

YES or NO

YES

*(If NO, please explain why.)*

IF YOU ANSWERED YES TO 4.1, PLEASE ANSWER THE FOLLOWING QUESTIONS:

### 4.2 HOW WILL THE ANONYMITY OF THE PARTICIPANTS BE RESPECTED?

*Please bear in mind that where the sample size is very small, it may be impossible to guarantee anonymity/confidentiality of participant identity. Participants involved in such projects need to be advised of this limitation in the Plain Language Statement/Information Sheet. If you intend to fully anonymize the data, please provide details*

We will provide users with various predefined use cases that they themselves can enter along the application, no users will have to provide their actual personal information. Regardless, we will ensure that inputted data into our application and database is encrypted. We only wish to meet with our participants on an individual basis hence we can ensure that information won't be shared among two or more users. The given user information from the cognitive walkthroughs won't be mapped to any participant, ensuring that the feedback they give is confidential between them and the developers.

#### 4.3 LEGAL LIMITATIONS TO DATA CONFIDENTIALITY

Participants need to be made aware that confidentiality of information provided cannot always be guaranteed by researchers and can only be protected within the limitations of the law - i.e., it is possible for data to be subject to subpoena, freedom of information claim or mandated reporting by some professions. This information should be included in your Plain Language Statement and Informed Consent Form. Depending on the research proposal and academic discipline, you may need to state additional specific limitations.

State how and where participants will be informed of these limitations

This is stated explicitly within the plain language statement.

### 5. PERSONAL DATA - COMPLIANCE WITH THE GENERAL DATA PROTECTION REGULATION

Personal data is data relating to a living individual (i.e. the 'Data Subject') who is, or can be, identified either from the data itself or from the data in conjunction with other information that is in, or is likely to come into, the possession of the 'Data Controller' (i.e. DCU and its constituent units e.g. research teams etc.). Further information on personal data is available from the DCU Data Protection Unit at <https://www.dcu.ie/ocoo/dp/guides.shtml>

#### 5.1 IS PERSONAL DATA BEING PROCESSED AS PART OF THIS PROJECT?

YES or NO
YES

If YES, Please indicate your compliance with the following guidelines:	Mark here
We confirm that we have read and agree to act in accordance with DCU Data Protection Unit guidance and procedures regarding personal data	YES
We confirm that we have put in place a Personal Data Security Schedule (PDSS) for the project and have attached it to this application	YES

Please see the GDPR and the Research Ethics Process section of the [SCEC main webpage](#) for guidance

IF YOU ANSWERED YES TO 5.1, PLEASE ANSWER THE FOLLOWING QUESTIONS:

#### 5.2 WHAT KIND OF PERSONAL DATA IS BEING PROCESSED?

Note special categories of personal data include health data, genetic data and/or data relating to ethnicity/race of participants, their sex lives and/or sexual orientation

The app is just looking at general personal information which will all be necessary for the user to get the most out of the applications functionality. This includes: full name, and optional profile picture, phone number, age, sex and device location. No other unnecessary information will be required.

In terms of the medical data, it can be optionally inputted. The sole purpose of it being that in the worst case scenario for a user their medical profile could be supplied to emergency services. As mentioned previously, this data will be encrypted, hence it won't be viewable or used by the developers.

However, for the purpose of our app, the only real information entered will be the users phone number, the rest will be made up.

5.3 WILL ANONYMISATION/PSEUDONYMISATION OF THE PERSONAL DATA BE UNDERTAKEN?

YES or NO

YES

(If NO, please explain why.)

6. DATA/SAMPLE STORAGE, SECURITY AND DISPOSAL

For the purpose of this section, "Data" includes that in a raw or processed state (e.g. interview audiotape, transcript or analysis). "Samples" include body fluids or tissue samples.

6.1 HOW AND WHERE WILL THE DATA/SAMPLES BE STORED?

Note that the SCEC recommends that all data be stored on campus – please justify any off-site storage.

The sampled data will be stored within Google's Firebase Real-time cloud Database and Storage. Given that both the database and multimedia storage is cloud hosted, the data is not confined to any given location.

6.2 WHO WILL HAVE ACCESS TO DATA/SAMPLES?

If people other than the main researchers have access, please name who they are and explain for what purpose.

Only the main two developers of the app will have access to the data samples. Users are able to view their own information entered upon registration and set up within their personal profiles and/or in various other user functions on the app only. No app user will have access to our database. We've set the Firebase Realtime Database Rules to securely determine only the app developers, us, have strict read and write access.

6.3 HOW LONG IS THE DATA TO BE HELD/RETAINED FOR?

Note that with very few exceptions **personal data** may not be retained indefinitely. It is up to the unit or research team to establish an upper retention limit for each category of personal data under its control.

We only require that the sampled data should be kept for the duration of our project development. After the completion of our project demonstration in May and following our results in June, all user data will be removed

6.4 IF DATA/SAMPLES ARE TO BE DISPOSED OF, PLEASE EXPLAIN HOW, WHEN AND BY WHOM THIS WILL BE DONE?

Note that simply deleting files is not sufficiently secure. The additional steps to be taken to maintain data security should be given. **Personal data** must be disposed of in a safe and secure manner at the end of its retention period. If the data is stored in a: a) paper based format then shredding or disposal via a secure bin is recommended; or b) if it is stored in an electronic based format then deletion of the record or full anonymization of the data is recommended. If data/samples are NOT being disposed of, please justify this decision.

If any member wishes to delete their account on this app, they will be given the functionality in order to do so. By doing so, their phone number will be removed from our Firebase authentication library and their corresponding information within the Firebase real time database & storage will be removed also, according to their unique user ID (which is generated alongside their phone number) & firebase function calls. All traces of the specific user will be wiped.

7. PLAIN LANGUAGE STATEMENT (Attach to this document. Approx. 400 words)

A Plain Language Statement (PLS) should be used in all cases. This is written information in plain language that you will be providing to participants, outlining the nature of their involvement in the project and inviting their participation. The PLS should

*specifically describe what will be expected of participants, the risks and inconveniences for them, and other information relevant to their involvement. Please note that the language used must reflect the participant age group and corresponding comprehension level – if your participants have different comprehension levels (e.g. both adults and children) then separate forms should be prepared for each group. The PLS can be embedded in an email to which an online survey is attached, or handed/sent to individuals in advance of their consent being sought. See link to sample templates on the website:*  
<https://www.dcu.ie/researchsupport/ethicsapproval.shtml>

## PLAIN LANGUAGE STATEMENT

**Research Study:** User Testing for ICE

**Department:** DCU School of Computing

**Supervisor:** Renaat Verbruggen

**Researchers:**

- Hannah O'Connor( [hannah.oconnor26@mail.dcu.ie](mailto:hannah.oconnor26@mail.dcu.ie))
- Catherine Mooney([catherine.mooney33@mail.dcu.ie](mailto:catherine.mooney33@mail.dcu.ie) )

This project is a safety application for users of all ages and gender. It is a cross platform application meaning it can be used on both android and IOS, as well as certain functionality available on web browser.

It's purpose being to help people feel secure in the knowledge their phones can be used as a safety device and help is just a click away. It also ensures that their network of trust can be provided with reassurance and extra comfort that their loved ones are safe.

The research to be undertaken is for the purpose of gathering user feedback on the app's design and functionality and how we can improve its overall user experience. We assume that most people have never used an application like this, apart from the safe zone app in DCU. However, ours provides extra functionality, like that of the user tracking for example.

Our User testing will mainly consist of Cognitive walkthroughs. Here, the user will use the app for the first time, testing out its functionality and will also be required to enter information upon signing up, such as Name, Age, Phone number, profile picture( optional), etc. We request the user enters mock data and does not provide any personal details. The information will be made available to other users on the basis that they have added a contact to their network of trust. User locations will only be required when the user chooses to share it with their network if they have started a follow me session, as to provide safety to the user.

The data in which the app stores will only be retained for a short period. That is, after our project has been presented in mid May. Taking part in this user testing is completely voluntary and if any participant wishes to no longer be included, they can withdraw freely and their data will be destroyed. The user will have the option within the app to remove themselves or it can be done for them on request. For additional precautions, any data that is stored in our database is encrypted, so the developers cannot access it.

Confidentiality of information provided cannot always be guaranteed by researchers and can only be protected within the limitations of the law - i.e., it is possible for data to be subject to subpoena, freedom of information claim or mandated reporting by some professions.

***If participants have concerns about this study and wish to contact an independent person, please contact:***

*The Secretary, Dublin City University Research Ethics Committee, c/o Research and Innovation Support, Dublin City University, Dublin 9. Tel 01-7008000, e-mail [rec@dcu.ie](mailto:rec@dcu.ie)*

**PLEASE CONFIRM WHETHER THE FOLLOWING ISSUES HAVE BEEN ADDRESSED IN YOUR PLAIN LANGUAGE STATEMENT/ INFORMATION SHEET FOR PARTICIPANTS:**

	YES or NO
Introductory Statement (Supervisor and student names, school, title of the research)	YES
What is this research about?	YES
Why is this research being conducted?	YES
What will happen if the person decides to participate in the research study?	YES
How will their privacy be protected?	YES
How will the data be used and subsequently disposed of?	YES
What are the legal limitations to data confidentiality?	YES
What are the benefits of taking part in the research study (if any)?	YES
What are the risks of taking part in the research study?	N/A
Confirmation that participants can change their mind at any stage and withdraw from the study	YES
How will participants find out what happens with the project?	N/A
Contact details for further information (including SCEC contact details)	YES
Details relating to GDPR Compliance if Personal Data is being sought	YES

*If any of these issues are marked NO, please justify their exclusion:*

## 8. INFORMED CONSENT FORM *(Attach to this document. Approx. 300 words)*

*In most cases where interviews or focus groups are taking place, an Informed Consent Form is required. This is an important document requiring participants to indicate their consent to participate in the study, and give their signature. If your participants are minors (under 18), it is best practice to provide them with an assent form, while their parents/guardians will be given the Informed Consent Form. In cases where an anonymous questionnaire is being used, it is enough to include a tick box in the questionnaire (underneath the information section for participant), where participants can indicate their consent.*

*See link to sample templates on the website: <https://www.dcu.ie/researchsupport/ethicsapproval.shtml>*

## User Testing Informed Consent Form

**Research Study Title:** "ICE" a personal safety cross platform mobile application.

**Department:** DCU School of Computing

**Developers/Researchers:**

- Hannah O'Connor( [hannah.oconnor26@mail.dcu.ie](mailto:hannah.oconnor26@mail.dcu.ie))
- Catherine Mooney([catherine.mooney33@mail.dcu.ie](mailto:catherine.mooney33@mail.dcu.ie))

This is a study about a personal safety application “ICE” carried out by Hannah O’Connor and Catherine Mooney. It is being conducted as part of our final year project work.

Our goal is to utilize users phones as a personal safety device, while still ensuring that this app is user friendly. Your participation will help us achieve this goal in terms of its correct design and functionality.

In this testing, it will consist of Cognitive walkthroughs. You will be working with our application for less than 10 minutes. Here, we’ll ask you to perform tasks that are expected and to act as a regular user of the application. Such tasks would include: signing up, creating a Safe Zone, creating your circle of trust (consented network of trustees which is to be selected by the user), messaging another user in your circle, viewing your various circle’s private map, accept/decline another user’s circle request. After the time is up, you will be asked how we could improve the functionality or enhance the user experience.

Locations will be required while the application is running on a given device. However, for the purpose of this user testing, given that the testing process will be conducted at given location, the user won’t be tracked. The main purpose is for you to report to developers on how easy/difficult the process of creating circles and safe zones are. Along with providing productive criticism on the use of the interactive private circle of trust map.

The developers of this application will sit alongside you, observing and documenting your tasks and the responsiveness of the app. They will also be able to guide you if at any point you are lost.

The data to be used within this testing will be mocked use cases supplied for you to enter. All that information gathered from the application will be stored until the demonstration of the project in mid May, and will be used for internal purposes until then. After that, the data will be destroyed. Your feedback on the app will be used to help improve the overall design of the application, it will be kept anonymous and will not include your name or be shared to any other participant in this testing.

The goal is to test the application, and not the users themselves. We want to inspect how the application can be made to make your experience all the better. You will be allowed to drop out at any given time during the testing process, and if so, any personal data collected from within the application or through feedback, will be destroyed.

For the purpose of this application, we require you to be over 18 years old. If you do not have either an android or iOS device, you will be given the optional to test the application on a virtual device.

#### **User Statement**

*Participant – please complete the following (Circle Yes or No for each question)*

<i>I have read the Plain Language Statement (or had it read to me)</i>	<i>Yes/No</i>
<i>I understand the information provided</i>	<i>Yes/No</i>
<i>I have had an opportunity to ask questions and discuss this study</i>	<i>Yes/No</i>
<i>I have received satisfactory answers to all my questions</i>	<i>Yes/No</i>

I have read and understood the information in this form. My questions and concerns have been answered by the researchers, and I have a copy of this consent form. Therefore, I consent to take part in this research project

**Participants Signature:** \_\_\_\_\_

**Name in Block Capitals:** \_\_\_\_\_

**Witness:** \_\_\_\_\_

**Date:**\_\_

**Developer/Researcher Statement**

I believe that this user has given their consent to partake in the user testing of this study.

**Developer/Researcher Signature:** \_\_\_\_\_

**Name in Block Capitals:** \_\_\_\_\_

\_\_\_\_\_

**Date:**\_\_

**NB – IF AN INFORMED CONSENT FORM IS NOT BEING USED, THE REASON FOR THIS MUST BE JUSTIFIED HERE.**

--