Privacy Measures for The Big Data Show

Version 0.5 26th July 2019

v0.5
26th July 2019

Contents

1. Introduction

This document has been prepared and approved by the Ethics Committee, taking on advice and guidance from key partners including Police Scotland. It presents the privacy and data protection measures adopted by *The Big Data Show* (TBDS).

TBDS performances will involve the use of a smartphone app ("the app"), which is being designed and implemented with the help of Orthrus Studios, a specialist in Serious Games and software development.

Up to 24 shows will be presented in Perth, Glasgow, Edinburgh and 3 additional cities in the North of England in June and July 2020. There will also be in-school workshops delivered to each participating school before and after the show in the Spring and Autumn terms of 2020.

The producers of TBDS aim to improve the data literacy and cyber resilience of pupils who take part in the project and particularly to inspire young women and BAME people to consider careers in digital technologies.

Outcomes for: children, teachers, education system, government, Civic Digits

Short-term outcomes (immediate):	**Medium-term outcomes (eg after six months):**	**Long-term outcomes (after a year):**
Awareness of cyber issues is raised Ethical hacking careers are better understood Learners achieve SCQF credit Teachers feel supported to deliver curriculum Curriculum delivery is recognised as being creatively enhanced Funders' requirement are fulfilled	Cyber awareness is raised Children have progressed onto further cyber-related/digital or STEM learning opportunities as a result of TBDS Interest in cyber/digital/STEM careers is increased A model of creative delivery of STEM learning is available, with evaluation Teachers have explored more	This approach is common and growing in Scotland's schools Children are on the path to further cyber/digital/STEM learning The model has run successfully outwith Scotland We have concrete evidence of an increase in learning and achievement and aspiration from the children in this area

	opportunities to bring creative digital/STEM learning into the curriculum (eg cross-departmentally within the school) Scotland's progressive approach in creatively teaching cyber/digital awareness is recognised	We have evidence of increased capacity in schools and between schools and other organisations to deliver curriculum in a creative way.

This risk assessment has been written by Dr Clare Duffy, Artistic Director of Civic Digits with Rupert Goodwins, co-writer of *The Big Data Show*.

This is a dynamic document and will be reassessed on at least a bi-annual basis.

2. Organisational Structures

2.1. TBDS Ethics Committee and Education Steering Committee

Ethics Committee

Person	**Affiliation**	**Role**
(EK) Prof. Ewan Klein (Chair)	University of Edinburgh	Use, interpretation and social embedding of different forms of data advisor
(NC) Dr. Natalie Coull	Abertay University	Ethical Hacking Skills Advisor
(LP) Dr. Lynn Parker	Abertay University	Games development advisor
(DS) Daniel Sellers	Scottish Government:	Cyber Resilience Learning and Skills Policy Adviser

(FO'B) Freda O'Byrne	Independent Artist Co-founder Prewired	Theatre In Education advisor
(LG) Liz Green	Youth Link Scotland	National digital youth work adviser

Education Steering Committee

The Education Steering committee are convened to help us achieve our long term aim to embed TBDS into the education fabric of Scotland and the UK and to advise on the educational outcomes of the project. They are

Caroline Donald (Chair)	Head of learning and Engagement	Edinburgh International Festival
Kirsty McFaul,	Senior Officer for Digital	Education Scotland
Scot Hunter	Internet Safety Officer	Education Scotland
Debbie Bentley	Drama Teacher	Firhill School Edinburgh

2.2. **Civic Digits Team**

Person	Role
(CD) Clare Duffy	Creative Director Civic Digits, Associate Artist Perth Theatre, Co-director Unlimited Theatre. Project manager
(SG) Suzy Glass	Executive Producer
(RG) Rupert Goodwins	CTO and Co-writer

2.3. **Orthus Studio**

Director Oliver Smith: Delivery of the app for use in live performance and workshops.

3. Stakeholders

3.1. Internal Stakeholders

Co-Producers

- Civic Digits C.I.C
- Perth Theatre
- Unlimited Theatre

Partners

- Edinburgh International Festival (Creative Learning)**,**
- The Citizens' Theatre (Glasgow, Creative Learning)
- The Lyceum Theatre, (Edinburgh)
- TBDS Ethics Committee (Details given above)
- The Educational Steering Committee (Details given above)

3.2. External Stakeholders

- Schools: 15, five each in Edinburgh, Glasgow and Perth.

- Education Scotland
- Funders: Creative Scotland, Scottish Government. Cyber Resilience Unit
- The University Edinburgh.
- Business sponsors: Skyscanner
- Advisers: police, press contacts,
- Martin Beaton, ScotlandIS: Scotland lead for EIT Digital

4. Policy

4.1. Child Protection

Clare Duffy is a registered STEM Ambassadors and therefore has an up to date PVG Disclosure. Other members of the creative team such as actors, co-writers and other creatives do not require PVG disclosure for accompanied, one off visits to schools.

4.2. Privacy Statement

Civic Digits has a Privacy Statement which conforms with the requirements of GDPR. Civic Digits will hold data about teachers, schools and public audience members who consent to it but will not share any of this personal data with any third parties without consent.

Civic Digits will share anonymised data about audience and participant numbers, age groups, and geographical location of performances for research and evaluation purposes, for example with funding bodies such as Creative Scotland and with academic institutions. The privacy statement will be available on a website before the workshops begin. 'Plain language' Privacy Statements will also be given out to audiences at the end of each show to make it clear that no personal data has been seen or collected by Civic Digits though the process of delivering the show.

4.3. Terms of Service for the app

Civic Digits have written a statement of Terms of Service for using the app, with the guidance and final approval of the Ethics Committee. The aim of the Terms of Service is to replicate as much as possible the typical experience of a user downloading and using an app from Google Play or the Apple App Store. We also want to use this document to show how the language and form of these terms can be very hard to understand by including absurd and/or silly statements. These absurd statements will be referred to in the workshop and there will be further suggestions of ways to explore them as part of our challenge to the users to think critically about their relationship with the makers of apps.

4.4. IP and Licensing

The intellectual property for the app is shared equally between Civic Digits C.I.C and RG. Civic Digits C.I.C and RG propose to release any source code for the app that does not already fall under previous licences under the GPL4 Licence. This source code will either be available via the website or by email request.

Confidentiality

All participants will be informally asked to agree not to disclose the way this project and performance works. Much of the delight and magic of the experience is based on testing what the participants do in a typical online situation. Alerting the audience to 'the game' would

genuinely spoil the experience. However, we will not require participants to sign a non-disclosure agreement.

4.5. Project Evaluation

Quantitative evaluation.

The project will offer 30 pupils per school the opportunity to achieve the SCQF-credit rated award certificates. This data will be managed through a SQA centre.

This 'Introduction to Digital Citizenship' course will involve participation in 2 workshops (before and after the show) and will also require outside of direct contact with Civic Digits the sharing of creative work using data with the rest of the school and gathering feeback.

Qualitative evaluation

The production team delivering the shows will create a 'show report' for every show in the tour . This will reflect the whole team's assessment of how the participants responded to each element of the workshop. This will not include any personal data from participants.

The workshop leaders will assess and award the SCQF certificates in the second workshop and will record details about how learners experienced the project.

4.6. Social Media

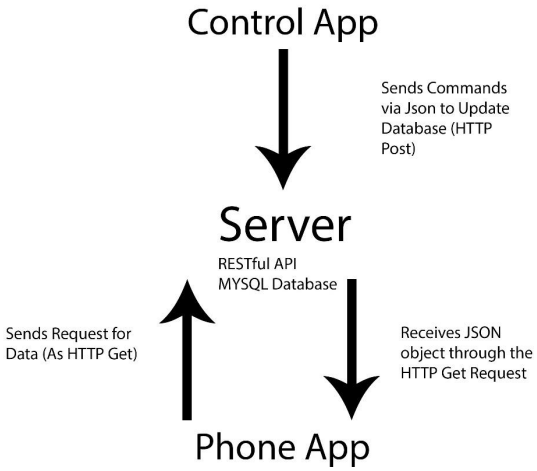
TBDS has a Twitter account, namely @bigdatashowtime. It is likely that Civic Digits and TBDS will create a variety of social media profiles in the future. Social media platforms sell, use and/or share data which can identify individuals and threaten their privacy and security for financial and potentially other reasons. Civic Digits' aim is that the work we do will contribute to the debate about the role and responsibility of us as citizens and the organisations who offer these platforms to know about how they use (personal) data and how that affects privacy and security online and offline.

4.7. Customer Relationships Management (CRM) of Data for schools

Civic Digits will keep a CRM-style database of the schools and teachers it has contact with to maintain communication throughout the project. In some cases, this will include personal telephone numbers for teachers. Consent to hold this data will be requested with booking instructions.

5. Functionality and Data Handling of the app

5.1. System Data Flow



An overview of the data flow is shown in the accompanying diagram. In this diagram, the app described elsewhere in this document is referred to as “the Phone App”.
The Control App does not ever interact directly with the Phone App, but sends data to the Server (which can be on the same machine or separate). The Server stores this data in a database. During a TBDS performance, the Phone App connects regularly with the Control Application, but only explicitly to "ask" it what scene it should be displaying, whether it should be playing a sound effect or triggering any other "magic tricks". It does not share any User information. Data extracted from the database by the Sever is sent to the Phone App as a text object (JSON).

RG as CTO is responsible for writing a security design specification which will be included in the contract for Orthrus. RG will also have eyes on the code for the app.

5.2. App Permissions

The app will ask the user to allow access to data such as GPS. However, the app will not in fact be able to collect this data either, in the core code or via Android data access permissions as the functionality required to collect this data will not be programmed into the app. According to the Android documentation,[1] these are permissions

> *to access sensitive user data (such as contacts and SMS), as well as certain system features (such as camera and internet). Depending on the feature, the [Android] system might grant the permission automatically or might prompt the user to approve the request.*

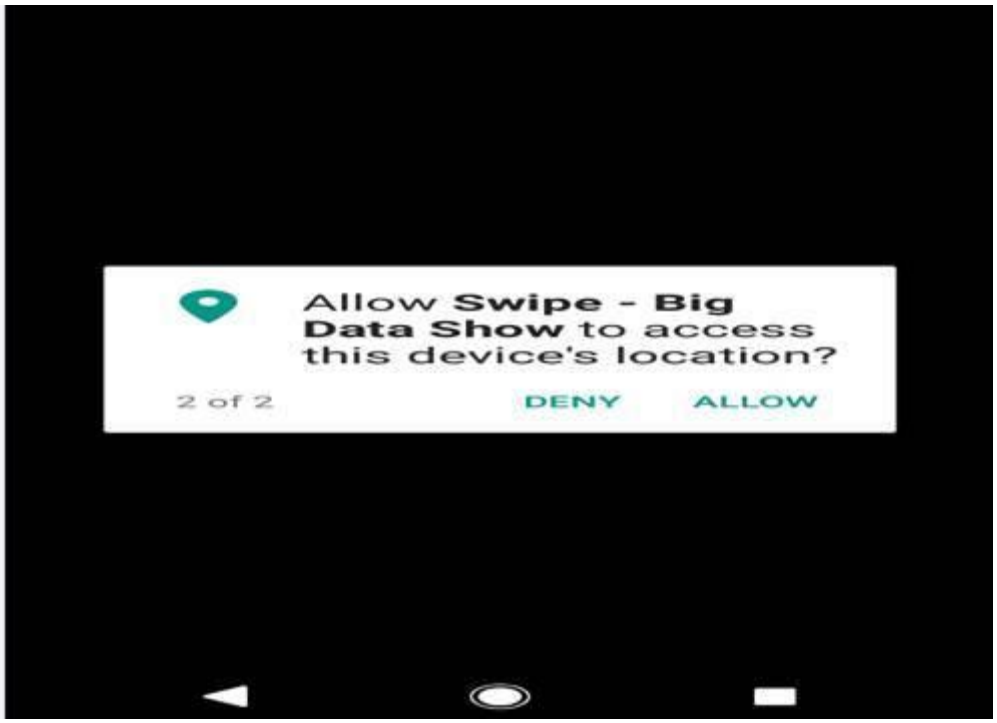
We consider it unethical to allow our app to have the functionality to request data access in this way, since if there was a malicious act on the phone, the data could be exploited.

When first downloaded, the app asks for permissions to access storage and network connections.

[1] https://developer.android.com/guide/topics/permissions/overview

This is a standard for Apple and Google Play and beyond our ability to change. However, our app will not access these areas. If we made this clear before the show we believe this would destroy the potential learning impact of the experience. For this reason we will distribute a simple and 'Plain English' Privacy policy/declaration to all pupils after the show.

5.3. App Data Collection



No user data is transferred from the user's phone via the app. The only information that will be recorded from the user is their GPS location. This data will be stored locally (within the user app file structure on the user's phone) and never leaves the phone. This GPS data will be deleted as soon as it has been used in the show.

For players of SWIPE who do not attend the show, the app will be updated at the end of each tour. Every up date or re-installation automatically delates previously collected data.

All analytic data recording has been disabled for the app itself. Some analytic data may be recorded by the Operating System (Android or iOS) or by the devices themselves (for example the Apple App Store may record when the application was downloaded) but this is standard for all phone apps, is outside of our control and is GDPR compliant.

The app's "Leaderboard" function will collect the user's scores but shows it on the phone next to fake data instead of those of other pupils so no personal data relating to scores is transferred to or from the app.

There will be a competition at the start of the show to find 'The Swipe Champion'. This will be announced by a message sent to the highest scorer and will not require any personal data to be seen or collected.

5.4 Live looking over the shoulder of other audience members

There is the risk that an audience member can see data 'over the shoulder' of a class mate when the GPS data of the user is presented to them in the form of a map of where the user was

when they played SWIPE. The map is specifically designed to show the user where they were, but to make it difficult for a glance to reveal very much information. Each point on the map is visited for only a few seconds and there are no place identifies such as street names or organisations addresses (for example an LGBT youth club). The resolution of the map is not particularly fine grained, each view of the map representing approximately 0.25 km.

Privacy Risk Register

Note: Risks are ranked on a 1—5 scale. Exposure is an estimate of the combined effect of Impact and Likelihood.

Risk description	Inherent Privacy Risk			Options for avoiding or mitigating this risk	Risk Owner
	Impact	Likelihood	Exposure		
Reputational risk to Civic Digits if there is a perceived risk (e.g., via press or social media) of privacy invasion.	**Mild (2)**	**Mild (2)**	**Mild (2)**	Ensure demonstrable adherence with data protection legislation Ask a highly qualified ethics committee to support the project and think through all of the risks.	**CD**
Spoof versions of the app are installed on the Apple and/or Android app stores and allow malicious code to be installed on users' phones.	**Low (1)**	**Low (1)**	**Low (1)**	Ensure clear branding and make it as fool proof as possible for TBDS participants to only download the correct app On a par with any other app in the ecosystem. It is difficult to assess impact as a spoof app could do anything it liked, but TBDS presents no more risk here than do other apps.	**CD/RG**
Faulty implementation of the app allows personal data to be transferred to the system Server.	**Low (1)**	**Low (1)**	**Low (1)**	Server is protected by strong passwords, and is only physically accessible to authorised members of the team. TBDS does not collect any personal data on the phone beyond some GPS tracking. The architecture of the system, the configuration of the server and the functionality of the back-end system do not collect or store any data of any kind during operation, so it's not as if there's a pathway which could malfunction - there is no pathway.	**RG/CD**
Insecurities with and on the server allow third parties to tamper with the Server routines to send malicious payloads to the user app.	**Low (1)**	**Low (1)**	**Low (1)**	The server will always be in the physical possession of either Rupert Goodwins or a production manager who is responsible for the setting up of the control system. Rupert will encrypt the server software. The server is configured with standard, latest-patch Linux and Windows security features enabled, and proper account/password management.	**CD/RG**

				There is no pathway to explicitly send code or data to the mobile app; the server is a source of control messages only which the app uses to set internal state, and has no special privileges or access to the phone or app beyond those.	
Insecure data transfer between user app and Server is breached and malicious payloads are transferred to the user's phone.	**Mild (2)**	**Mild (2)**	**Mild (2)**	No user data is transferred between the server and the mobile app, and there is no pathway for malicious data onto the app. There is a risk that an unknown vulnerability in the app could be exploited by a custom-designed attack, but that's true for all apps. As the total expected audience for the app is small, compared to most apps, and the audience is mostly school children with little economic or political impact. It is considered unlikely that it would repay the resources required to attack it.	**CD/RG**
Malicious code on user's phone is able to access private data stored on the app's local file store.	**Low (1)**	**Low (1)**	**Low (1)**	The only private data stored is recent GPS tracking, which is hard to exploit in any harmful fashion for our audience, and thus presents little motivation to any malicious attacker to invest the resources in extracting it.	**CD/RG**

Malicious software on one user's phone attacking another phone on the TBDS hotspot.	**Mild (2)**	**Mild (2)**	**Mild (2)**	All the phones are on the same local network, so are directly accessible to each other. This risk is roughly the same as for any group of devices on a hotspot, and could result in degraded performance - sluggishness or unresponsiveness - in the target phone, or the whole network. More severe risks to personal data are less likely, and would require further security failures outside the remit of the BDS software or network.	CD/RG