Digital safeguarding tips and guidance

Girl Effect

This document offers practical tips and guidelines for safeguarding children online digitally in Girl Effect's programmes and platforms, including how to safeguard personal and/or sensitive data collected from or about children throughout the data lifecycle. It does not constitute legal advice in any way and you are encouraged to seek your own advice to ensure your own specific circumstances have been taken into consideration in how you approach digital safeguarding. The report is based on Girl Effect's learning and experiences over the past 4 years and builds on an earlier Principles and Practices document published by Girl Effect in 2016. Produced by Girl Effect. Author: Linda Raftree. Cover Photo: Girl Effect.

A girl's safety and wellbeing is the purpose of our work.

Every decision made will reflect this.

From design to development to how we measure impact,

we will not compromise a girl in any way.

We will not opt for solutions that cut costs at the expense of her safety.

The girl will sit at the core of every decision made –

exactly where she needs to be.

Girl Effect, Digital Safeguarding Guidelines (2016)

Table of Contents

Terminologies and definitions

The terminologies and definitions below are aligned with Girl Effect's Safeguarding Policy and the European Union's General Data Protection Regulation (GDPR).[1][2][3]

Abuse includes physical abuse, emotional ill-treatment, sexual abuse, neglect, commercial or other exploitation. It includes harm that is caused intentionally or unintentionally, directly or indirectly. Abuse is harm that is so severe or persistent that it is likely to have a lasting effect on the health and development of the child or young person.

Active data collection happens when a user deliberately offers or shares personal data, for example when filling out a registration form or when posting a comment on a website.

Anonymous data refers to data or data sets that have been amended in such a way that no individuals can be identified (directly or indirectly). Data protection regulations in the EU do not apply to data that is rendered anonymous in such a way that individuals cannot be identified from the data.

Best interest decisions refer to the principle that decisions that affect children or young people should be made based on consideration of their physical and psychological well-being and the need to prevent harm to them or others. Best interest decisions should be reached in consultation with both the child/young person and those responsible for their care.

Child refers to anyone under the age of 18, in line with the United Nations Convention on the Rights of the Child (1989)

Consent refers to any freely given, specific, informed and unambiguous indication of wishes, either by a statement or by a clear affirmative action, signifying agreement – in this case agreement to a person's data being processed.

Data controller refers to an entity that alone or jointly with others determines the purposes and means of the processing of personal data.

Data privacy refers to a person's ability to know how their personal information will be collected, shared and used, and for them to exercise choice and control over its use.

Data processor refers to an entity that processes personal data on behalf of a data controller.

Data security refers to protection against unauthorised or unlawful processing and accidental loss, destruction or damage of data. It covers actions taken to maintain the confidentiality, integrity, availability and resilience of data systems. Data security encompasses the practices and processes that are in place to ensure that data is not being used or accessed by unauthorised individuals or parties. Data security includes aspects of collecting only the required information, keeping it safe, and destroying information that is no longer needed.

Data subject rights refer to a person's particular rights with regards to the processing of their data. Under the 2016 EU Regulations, a data subject has eight fundamental rights. See page 23 for more detail.

Design and content partners are organisations or individuals who design and produce content for Girl Effect products and campaigns. They may have direct contact with children and young people as well as an indirect impact on children and young people through materials they produced.

Direct contact with children and young people refers to being in the physical presence of a child or young person in the context of Girl Effect's work, whether the contact is occasional or regular, short or long term. Direct contact also includes interaction with children and young people via the internet or telephone, even if a physical meeting never takes place.

Disclosure refers abuse or harm being directly or indirectly reported or referred to, for example in a comment, when a girl is being interviewed, or when she is participating in a workshop.

---

1 Raftree, L (2016) children and young people' Digital Privacy, Security and Safety Guidelines, Girl Effect, London, UK

2 Terminology is aligned with the European Union's General Data Protection Regulation (GDPR) (2016) https://www.eugdpr.org/

3 Girl Effect (2017) Global Safeguarding Policy. Girl Effect, London, UK https://www.girleffect.org/safeguarding/

Due diligence refers to Girl Effect's responsibility to ensure that the organisation's funds are used properly and for verifying who partners are, assuring they have the capacity and skills to deliver initiatives safely, and monitoring their activities and conduct.[4]

Duty of care is Girl Effect's legal and moral obligation to:

- Take all reasonable steps to prevent foreseeable harm in any activity or interaction for which we are responsible
- Only act within our competence and not initiate operations we cannot do safely
- Always act in the best interest of children and young people

Financial partners are those organisations or individuals who invest or co-invest, either financially or through in- kind donations, in Girl Effect initiatives but have no direct contact with our staff, operations or children and young people.

General Data Protection Regulation (GDPR) is a law, passed by the European Union (EU) in 2016 and in effect as of May 25, 2018, to which entities who are established in the EU or who process EU data subject data must adhere.

Implementing partners are organisations or individuals who are responsible for implementing or co- implementing Girl Effect initiatives who have either direct or indirect contact with children and young people. For example, research agencies collecting data directly from children and young people or agencies responsible for facilitating events or activities with children and young people.

Indirect contact with children and young people refers to having access to personal information (data) on children and young people in the context of Girl Effect's work such as names, locations, responses to research questions, photographs, videos or case studies. This also includes data generated or shared by children and young people via digital applications, tools or platforms.

Lawful basis for data collection refers to one of six reasons, as outlined in the GDPR, that legally allow for processing of personal data. These are: consent, contract, legal obligation, vital interests, public task, and legitimate interests. We explore these further on page 22.

Passive data collection is that which occurs without any overt user interaction, and usually without a user's knowledge. It includes capturing user preferences and usage behavior, and may encompass location data, IP addresses, browser type and plug-in details, device type (eg desktop, laptop, tablet, phone, etc), operating system and local time zones. This type of data is gathered by Google Analytics, Facebook, and data analytics firms, for example, to profile and better target content or advertisements to users of websites. It can also be used to make improvements to the user interface to enhance design and user experience.

Personal data means any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Portfolio partners are organisations or individuals who invest or co-invest either financially or through in-kind donations in Girl Effect and work in collaboration with Girl Effect in ensuring delivery on the ground. This may include both direct and indirect contact with children and young people through the co-design and delivery of initiatives.

Processing means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences,

---

4 Adapted from Charity Commission (2011) Charities: due diligence, monitoring and verifying the end use of charitable funds. https://www.gov.uk/government/publications/charities-due-diligence-checks-and-monitoring-end-use-of- funds

interests, reliability, behaviour, location or movements.

Pseudonymous data includes data or sets of data that have been amended so that no individuals can be directly or indirectly identified from those data without a "key" that allows the data to be re-identified. Pseudonymous data are treated as personal data because it is still possible to identify individuals using the key.

Safeguarding refers to the safety and protection of all children and young people with whom Girl Effect engages. This includes:

- promoting of the welfare of children and young people and enabling them to achieve the best outcomes
- preventing harm through proactive measures to identify and mitigate risks
- protecting children and young people by responding quickly and effectively whenever harm or abuse is identified

Safeguarding demands attention to all types of harm (physical, sexual, emotional, neglect, exploitation) whether these reach the threshold of significant harm or not.

Sensitive personal data are: personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; and genetic data or biometric data. Data relating to criminal offences and convictions is also considered sensitive. Children's data is also considered sensitive due to their age and/or because they are too young to consent to its collection or processing.

Signposting in our case refers to giving a child or young person information about a local agency or organisation that can provide support or help. It is then up to the child or young person to then make arrangements to access that support.

Young person (for the purposes of these guidelines) is defined as anyone aged 18 - 25. Guidance and procedures contained within this policy also apply to our engagement with young people unless we specifically note otherwise.

Background

Girl Effect is an organisation with expertise in media, mobile, brand, and international development. Founded by the Nike Foundation in 2004, today Girl Effect is an independent, creative non-profit working from nine global locations and active in 66 countries. Girl Effect creates for young people, building vibrant, interactive youth brands that shine a light on the issues a girl faces, telling her story in her words, and bringing girls' experiences to life through the media and mobile tech that unites girls and boys.

Because we begin with deep local insight into girls' lives, we're able to root our platforms in their culture, needs and behaviours. We design our platforms to help girls overcome specific challenges, so they can build the confidence to create positive changes in their lives. We focus on a girl's whole world, along her entire journey to adulthood, and we create with her, so she can tell her story. Through our work a girl can start to express herself, value herself and build relationships. With the belief and support of those around her, she can then seek out the things she needs – from vaccination to education. This is how we start to create change from within – by girls, with girls and for whole communities.

Mobile technology is putting unprecedented power in a girl's hands. She can now find things out, talk to others and express herself in ways never before possible. Through locally rooted, girl-powered culture brands like Yegna in Ethiopia, Ni Nyampinga in Rwanda, and Zathu in Malawi, Girl Effect inspires girls and those around them with drama, journalism, and music. Social media, SMS and messenger platforms help us to spread this content and more deeply engage with our audience.

Our global mobile-first platform Springster digitally connects marginalised and vulnerable girls around the world. Featuring content designed for girls and created by girls, the platform puts essential, tailored information directly into their hands, and helps them find meaning and strength in each other's experiences.

On Girls Connect, dial a number and listen to pre-recorded stories containing inspiring, entertaining and educational lessons about their lives. They can then connect through to a role model with whom they can anonymously discuss issues of growing up in challenging circumstances, anonymously, on their own terms, and free from any fear of judgment.

TEGA (Technology Enabled Girl Ambassadors) empowers adolescent girls to conduct research, via innovative mobile technology, to provide safer, faster, more scalable and authentic research into young people's lives around the world. This girl-led mobile operated research app is used by some of the world's leading development organisations.

Digital platforms have enabled us to expand our reach and to engage girls and gatekeepers in vibrant and exciting ways. They also provide up-to-date and detailed data that can lead to rich insights into girls behaviours and opinions. But these new channels bring with them a host of new safeguarding challenges. For this reason, over the past few years, Girl Effect has been modernising its approach to the safeguarding of children and young people.

In this document we offer digital safeguarding tips and guidance to Girl Effect staff and partners. It emerges from our experiences designing and implementing mobile first platforms over the past four years and builds on a set of digital privacy and security guidelines that we originally produced in 2016.

Here we focus on keeping children and young people, especially girls and young women, safe while they are

- using our digital tools and platforms or otherwise engaging with us digitally or
- when we are accessing and processing their personal data.

Please see our Global Safeguarding Policy for broad guidance on safeguarding children and young people.

How to use this document

Digital safeguarding for Girl Effect includes both traditional safeguarding as well as new elements of safeguarding that we must consider in our work as we increasingly engage with children and young people on digital platforms and use their data to inform our work.

Our comprehensive global safeguarding policy [5] covers how we keep children and young people safe overall. The current document is not a policy. Rather, it offers teams additional considerations and operational guidance on two specific areas of the global policy:

- Safeguarding children who engage digitally in our programmes and platforms -- including during design, though moderation and community management, by signposting to relevant services, and by offering child-friendly content about digital privacy and security.

- Safeguarding personal and/or sensitive data collected from or about children – whether analogue or digital, including audio-visual – by ensuring data privacy and security throughout the data lifecycle and extending our data policy and practice to our partners.

These tips and guidelines are tailored for Girl Effect, and they serve as a benchmark for the levels of safeguarding that we aim to achieve in all of our work. The guidance draws on earlier work and builds in our own experiences and learning about digital safeguarding over the past four years as well as new legislation, such as the General Data Protection Regulation (GDPR), which puts much clearer and stricter guidance in place regarding data privacy and security.

The document is organised into 8 sections that aim to align with Girl Effect's product development cycle:

1. Before we start: What's the big picture?
2. Safe research and evidence building
3. Baking privacy and safety into platforms and products
4. Conducting a risk assessment
5. Protecting and securing data
6. Legalities
7. Content considerations
8. Working with partners, third parties, and social media

Each colour coded section can be used as a stand alone guide or checklist for a particular phase of product development, or the full set of tips and guidelines can be used. We've included stand-out boxes that offer background information and further details. We've also included links to core documents in case additional details are needed.

It is important to note that this document does not constitute legal advice. Rather it aims to offer tips and guidance that can support teams who are designing and implementing digital products and programs. For each situation, please consider whether you also need specific legal advice or further input from other teams such as digital, safeguarding or governance and reach out where required.

5 Our global safeguarding policy can be found here: https://prd-girleffect-corp.s3.amazonaws.com/documents/Girl_Effect_Global_Safeguarding_Policy_2017.

Girl Effect's principles

Girl-driven - In order to keep a girl safe, we must understand her whole reality. This means actively engaging girls and boys and creating spaces where they feel valued, can voice their concerns and needs without fear, and are connected to others who will help keep them safe and protected.

Pioneering - Breaking new ground inevitably involves confronting new risks. Together we will draw on our creative spirit to mitigate these risks and develop new approaches to ensuring the safety of children and young people.

Decisive - Ensuring children and young people's safety requires all staff and representatives of Girl Effect to be well informed, confident and decisive in their actions. This document aims to provide all representatives of Girl Effect with the information and guidance they need to take decisive action on digital safeguarding.

Tech-smart - Girl Effect uses technology to accelerate change for girls. We aim to pioneer new measures that go beyond simply managing the risks associated with technology and proactively harness the potential of technology to keep children and young people safe.

One - Every child and young person has the right to protection and to a life free from violence and maltreatment. Upholding this right is everyone's responsibility and requires collaboration across boundaries to solve problems and address risks.

1 Before we start: what's the big picture?

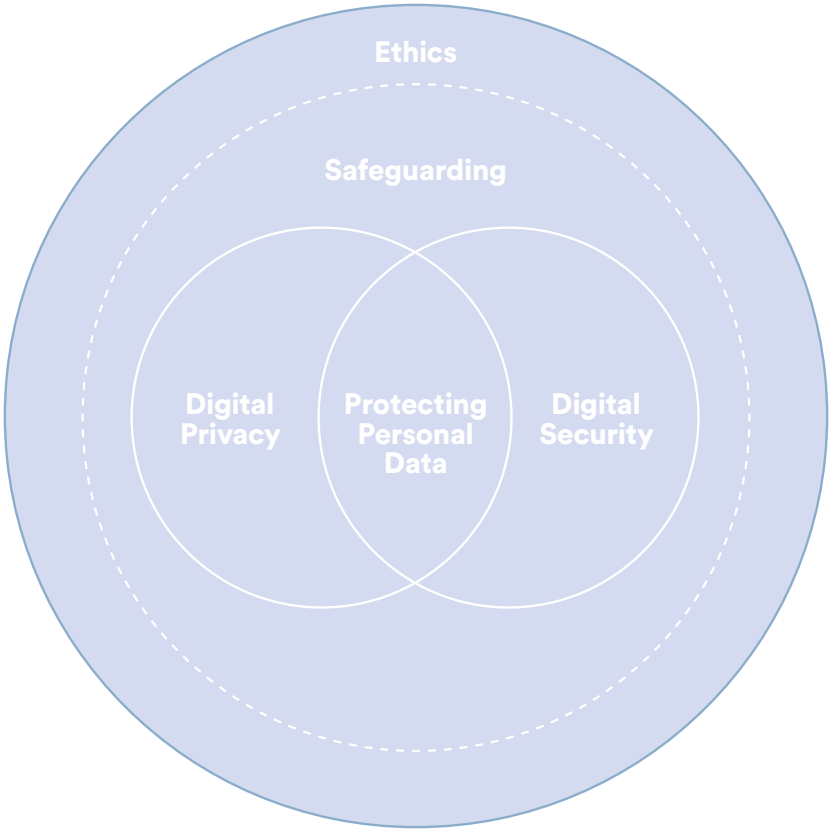
Safeguarding is a critical part of the design phase, whether it's the design of research, a monitoring and evaluation plan, or a product, platform or service. By baking privacy and safety in from the very start, we can both reduce the potential for harm to children and head off legal and safeguarding challenges. That way we can ensure that children and young people's safety remains at the core of all we do; not to mention, we won't be held up when we're ready to launch or haunted by safeguarding and data protection issues later on!

Users will feel more comfortable about an activity, a study, a mobile service or a platform that offers them a friendly experience and where they trust that their privacy is not going to be violated.

But before we even start researching or designing, we should ask ourselves a few questions about the big picture, and then document our answers...

Is embarking on this effort, project, or product ethical?

- Is this really a problem for the people we aim to create for? How do we know? Have we asked?
- What is our underlying motivation? Is there a genuine need or do we have a solution waiting for a problem?
- How does it link with Girl Effect's Theory of Change?
- Has someone done this before? What do we know about how it went? What can we learn?
- Is the problem ours to address? How are local actors involved and driving the effort?
- Are we getting in the way of others whose ideas or approaches might address the problem in a better or more sustainable way?
- Broadly, who does this initiative benefit? Who could it put at risk?
- Do we feel confident that the benefits for children and young people, especially girls and young women, outweigh the risks?
- Are we generating expectations or demand that cannot be met and could lead to apathy or harm?
- Have we thought about possible unintended consequences of embarking on this project?
- What will happen if/when our funding runs out and the product or service goes away?



2

Safe research and evidence building

Our work at Girl Effect involves a lot of research including formative research, user experience research, insights work, co-design workshops, ongoing measurement, and impact research. This means we collect and use loads of data, both qualitative and quantitative. Data helps us to learn about the lives of girls, their ideas and opinions, and to shape the design of products and programs.

Research, measurement and evaluation help us course correct technology tools, interface, look and feel, channel choices, messages, and ideas. They help us better understand what content to create and how well girls and others are responding to that content. Contributing to the evidence base enables both GIrl Effect and others to continuously learn and improve our work. Lastly, consultation with children and those around them means we can better understand context, uncover potential safeguarding issues, and understand people's views and practices around safeguarding and digital privacy.

What safeguarding mechanisms should be in place when we conduct research?

- Background checks and appropriate due diligence on research partners.
- Clear contractual agreements with partners related to data access, transmission, storing, sharing and retention/deletion; this includes any data shared during the recruitment process.
- A risk assessment for both the wider exercise and/or for specific activities (such as a workshop with girls or a mobile survey).
- Consent processes and procedures (see Boxes 1, 2, 4, 7 and 8 on consent).
- Partners trained on Girl Effect's Global Safeguarding Policy, code of conduct, and data privacy and security procedures.
- Incident reporting protocols in place, point persons established and trained (see Global Safeguarding Policy, page 23).
- Local service providers identified for signposting (see Global Safeguarding Policy, page 28).

What should we try to learn about safety and privacy during research?

- What are the national or regional laws, frameworks and/or protocols related to child safeguarding and to data privacy and security?
- What are phone access and use patterns and how might these impact on safety and privacy?
- What gendered and/or age-related factors contribute to access and use? How does this link with privacy and safety?
- Are there specific attitudes related to girls' and boys' access and use of mobile, the internet, or social media? What are they and who holds them? Why? What are the drivers?
- What are the potential risks to children and young people of possessing or using a mobile phone, using the internet or participating on social media?
- What support services are available to children and young people who experience abuse?
- What knowledge, attitudes and behaviors can we uncover specifically related to girls and boys and online/mobile safety and data privacy? How do children and young people navigate the risks and what strategies do they use to keep themselves safe?

Consent

Consent must be a freely given, specific, informed and unambiguous indication of wishes, either by a statement or by a clear affirmative action that signifies agreement. Information about consent and privacy must be given in plain, simple language. Consent must not be bundled up with other types of information or a requirement for accessing rights or receiving benefits.

Age of consent for data processing (including when it's for research purposes)

The GDPR stipulates that children over the age of 16 can consent to data processing, yet individual EU countries can establish a lower age limit, as long as it's not below 13. In the UK, this age of consent is currently established at 13 for online services. When Girl Effect conducts in-person formative research with anyone under 18, however, we request consent from both the child or youth participant as well as the caretaker. We also ensure that consent language is clear, concise, and culturally relevant. Consent forms are always translated into local language.

This consent provides a useful tool to ensure our participants and their caretakers have fully understood what it is we are doing, what they are being asked to give us and what we will then do with their data. However, it will not always be the 'lawful basis' on which we are relying for the data processing, for example, in cases where our lawful basis is performance of a contract or where legitimate interest is applicable. (See page 16 for a sample consent form.)

The following points are to be included in our consent forms or processes

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- With whom will it be shared?
- What will be the effect of this on the individuals concerned?
- How long will personal data be retained?
- Is the intended use likely to cause individuals to object or complain?
- What are their rights related to their data and this research?

We also:

- Inform participants and their caretakers that they may, at any time, withdraw their consent or request that we remove their data or stop processing it.

- Provide them with contact information should they wish to get in touch with a local partner to enact any of their rights related their data. This contact information should also include a general contact route to avoid issues when particular staff move or leave.

- In the case of audio or video interviews on sensitive subjects, consent is confirmed a second time post-interview to ensure that interviewees have understood and still agree to their information being used for the research.

- In some cases, we will also ask permission to get in touch with participants again for follow up in person or via a mobile/digital channel, such as WhatsApp, and check that it's OK that we retain their contact details for that purpose.

- When we are interested in having consent for both data processing (eg for research) and for media or communications purposes, these very different requests should form the basis of separate consents so that the request for media consent does not contaminate or bias the research process.

Box 2

Sample consent form for research with children under 18s

(A full set of consent forms is available in the Safeguarding folder on the shared drive.)

Girl Effect is an organisation that works to improve the lives of girls and their communities. We are conducting research with [local research partner name] to find out more about [Add research topic].

We would like to invite you to take part in an interview/group discussion on this topic. The interview/group discussion will last approximately [Add duration]. [If discussing sensitive issues, add details here].

If you tell us that you or someone else is at immediate risk of being harmed, we will inform our safety officer who will help decide how to keep everyone safe.

Your opinions will help us [add objective]. Our findings will be used to create a [add what the output will be e.g. report] which will be shared with [add internal & external stakeholders]. We will not include your name or any other details that could identify you [edit as appropriate] in the report.

Girl Effect will not use the findings for the profit of any business.

Your participation is voluntary and you will not receive any payment for being part of Girl Effect's research. If you are under the age of 18, we need both your and their permission to participate in the research.

It is up to you to decide to take part, you can withdraw at any time without giving us a reason. This will not affect your relationship with us.

We will store all the information we collect from you in a secure place for [add time period]. After this time, we will securely destroy or anonymise all the records containing your individual responses.

If you want us to remove your identifiable information before then, you can contact us using the details below.

If you have any questions or concerns, please contact:

(ADD DETAILS OF GIRL EFFECT CONTACT - include a specific person but also general contact details to avoid any issue when people move/change roles or leave)

Child's Consent

I have understood the above information and I agree to take part Yes / No
I am happy for Girl Effect to contact me in the future if they need to Yes / No

Printed Name: ..... Signature: .....

Date: Contact Number:

Parental Consent – for children under the age of 18

I confirm that I am the parent/guardian of.....
I have read and understood the above information and confirm that I consent for my child to take part in the Girl Effect research. Yes / No

Printed Name: ..... Signature: .....
Date:

Phone Number and Address:

How can we build privacy, security and safety into our research design?

- Make sure children, young people, and their families (and other community members depending on the context) know ahead of time that the research is happening, why, for whom, for what purpose, and if/how Girl Effect will feed back the research results.
- Be sure that the community and research participants are comfortable with the research approach. There may be uncertainty about the use of digital devices and filming/photos, or it might be uncommon for girls in particular to assemble or to meet with people from outside of the community.
- Where possible, do a participatory risk assessment of the research process together with girls and others who have a stake in the research.
- Do the research in a private and secure environment, where children and young people can speak freely.
- Set up an alert mechanism and a reporting system so that team members or managers can be react quickly to any danger for the interviewer or respondent or respond and signpost any disclosures or other signs of harm.

What safeguarding mechanisms should be in place when we conduct research?

- In cases where topics are extremely sensitive, determine the least risky form of digital data collection (eg video may be higher risk than audio only, text may be higher risk than audio).
- Provide mobile devices for the research and sufficient training (do not have researchers use their own phones).
- Secure any devices, networks, servers, and other tools by which data is collected or stored. For example:
  - Password protect and auto-lock on devices
  - Devices encryption to 128 level at a minimum
  - Remote wiping
  - Auto deletion of data upon successful transmission to a central database
  - Encrypted transmission through a secure network
- Categorise data into different levels of risk and always restrict access based on a need to know basis.
- Anonymise or pseudonymise as much data as possible as early in the process as possible (See Box 3 on data anonymisation and pseudonymisation).
- Avoid storing data on phones, USBs or flash drives as these could be lost, stolen or seized.
- Train data collectors to disable wi-fi, cellular data signals and GPS during the data collection process unless specified in the data collection protocol.
- Limit questions that include highly sensitive information that could put participants at great risk now or in the future, such as religious affiliation, ethnicity, political affiliation, sexual orientation, sexual conduct, illness or disability that stigmatises, or situations of violence, assault, conflict or other sensitive or taboo topic.
- Avoid capturing any data that is not required.

Pseudonymisation and anonymisation

The GDPR recommends both pseudonymisation and anonymisation as ways to improve data privacy and security. These two techniques are different and imply different actions with data.

Pseudonymisation replaces the most identifying fields in a database with artificial identifiers, or pseudonyms. For example a name could be changed to a unique number. The point is to make the data record less identifying, thereby reducing concerns about data sharing and data retention. It's important to know that pseudonymised data is not the same as anonymised data. Pseudonymised data retains a certain level of detail that allows tracking back of the data to its original state, whereas in anonymised data the level of detail is reduced so much that rendering a reverse compilation is impossible.

Care must be taken with personal data because patterns in data can allow for reconstruction of the source data. In a pseudonymised data set from a small, named village that removes the names of individuals but mentions a woman with 12 children, including two sets of twins, the woman may be easily identified from among other women in the village. An "anonymous" survey that masks names and emails but requests people to categorise themselves by longevity would quickly identify the only male at a company who has worked there longer than 40 years.

Thus, pseudonymisation includes both removing or obscuring direct identifiers (such as names or social security numbers) and also certain indirect identifiers that if combined could reveal a person's identity. These data points are then held in a separate database that could be linked to the de-identified database through the use of a key, such as a random identification number or some other pseudonym.

It's important to note that GDPR regulations do apply to pseudonymised data, whereas they do not apply to data that has been sufficiently anonymised. The key distinction is whether the data can be re-identified with reasonable effort considering the costs and amount of time that would be required for identification, the technology available at the time of the processing, and foreseen technological developments.[6]

Data anonymisation aims to conceal identity and identifiers such as family names, postal addresses, email addresses, telephone numbers, postal codes and city, identification numbers. A number of techniques exist for anonymising data, however it should be noted that many believe that true and total anonymisation of data is (or will soon be) almost impossible. Thus in some cases, we should aim to avoid collecting personal data at all if risk levels are extremely high should the data become re-anonymised at some point. The Millennium Challenge Corporation's guidelines for de-identification of data is a helpful resource for thinking about how to treat data in ways that reduce risk of re-identification.[7]

6 See https://www.pseudonymised.com/ for further information on pseudonymisation. See the IAPP's note on the GDPR and Pseudonymisation https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/

7 See the Millennium Challenge Corporation's guidelines for de-identification of data https://www.mcc.gov/resources/doc/guidance-evaluation-microdata-guidelines

How can we design safe self-reporting and feedback?

Sometimes we ask children and young people to self-report. This might be through handwritten media diaries, through phones that we provide them, or via polls and surveys on IVR lines, WhatsApp or other platforms that we've created. Things to think about when asking for self reports or feedback include:

- Will a family member or someone else be able access to the responses, for example on a shared or borrowed phone? Would that put children and young people at any type of risk? How can we mitigate the risk?
- Is there any stigma or stereotype associated with a girl having or using a phone that could affect her reputation?
- If we provide phones, do we have consent and agreement with children and their guardians regarding appropriate use, potential loss, privacy and data costs?
- Are we equipped to manage any disclosures that we might receive if there is open text on the self-reporting system?
- How are we protecting user identities and/or personal information from potential abuse? (For example, phone numbers are visible on WhatsApp, profile information is visible on social media sites)
- Do we have moderation in place to manage any disclosures, bullying, infiltration, or abusive behaviors?
- Have we tested the frequency and content of polls and surveys to ensure that they are not becoming a nuisance to users?
- Do children and young people understand that we will be using their answers for research and/or potentially to profile them? Have we obtained consent in cases where it's required? Does the consent clearly outline the core points around how we would use and share responses?
- Have we reviewed the channels we are using so that we have a clear understanding of the pros and cons with relation to data privacy and security?[8] For example, for one-to-one messaging, SMS is less secure than USSD, and USSD is less secure than WhatsApp, because WhatsApp has end-to-end encryption. These considerations of course need to be balanced with aspects of user access to different channels, cost, and other capabilities of these channels.
- In cases where we are selecting particular children and young people to receive polls and surveys or other types of invitations to self-report, have we reviewed our selection and profiling approach and our subsequent use of their data to be sure that it is legal and compliant with GDPR and other national regulations?
- Do we have a plan in place to manage data destruction on the devices after use or in case of loss or theft?

8 For more in-depth guidance of privacy and security features on SMS and messaging apps, see the International Committee of the Red Cross' "Humanitarian Futures for Messaging Apps" 2017 publication https://www.icrc.org/en/publication/humanitarian-futures-messaging-apps. Measure Evaluation also has several publications that go in-depth on managing sensitive data collection processes, data privacy, and data security on mobile devices. https://www.measureevaluation.org/resources/publications/ms-17-125a. Also see the World Food Program's 2017 guide on Conducting Mobile Surveys Responsibly. https://documents.wfp.org/stellent/groups/public/documents/manual_guide_proced/wfp292067.pdf

What should we be thinking about with respect to user profiling and data mining?

If research is being done through data mining of users' accounts or information they have volunteered through an application or a social network, the GDPR mandates that we are clear and transparent from the start (ie before we collect any data) and that we've assessed the benefits and risks that could result from profiling and/or data mining. In the case of big data and data science methods for research and evaluation, there are tangible privacy harms, but also intangible and abstract privacy challenges.

Intangible risks include the unfair discrimination or exclusion that can result from big data algorithms and automated decision making. Abstract privacy challenges include things like 'filter bubbles' and threats to wider democracy that have been identified as a result of targeted social media content and behavior change approaches.

The GDPR limits profiling and gives people significant rights to limit or avoid profiling-based decisions. Data processing is categorised as 'profiling' when it involves automated processing of personal data and when that personal data is used to evaluate certain personal aspects relating to a natural person.

Examples include analysing or predicting "aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." Profiling, then is not only 'tracking' but tracking that is done with the intention of making decisions regarding a data subject or predicting their behaviors and/or preferences.

Profiling is not necessarily illegal, but the GDPR provides people with rights related to profiling. We don't need to completely shy away from profiling, but we need to transparent about it and be very mindful that there is a real benefit to the individual whose data we are using if we use it for profiling.

User rights around profiling include the right to be informed at the time data is collected of not only the fact that profiling will occur, but of the logic involved and the foreseen consequences of such processing. A data subject can ask for details about how they are being profiled and request confirmation of such data processing, including profiling and its consequences, at any time. If a data subject objects to profiling, the processing must stop unless the data controller can prove "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject."[9]

Some tips if we are thinking about data profiling and data mining:

- Conduct a risk assessment (see Section 4) and have it reviewed by our DPO and/or legal counsel. Here we should account for both "traditional" risks, and also think about the unique intangible and abstract risks with big data and data science approaches. The Future of Privacy Forum offers guidance on Benefit-Risks Analyses for Big Data Projects[10] and the UK Cabinet Office offers a Data Science Ethical Framework that may also be useful.[11]
- Pay special attention to any sensitive data that we may be using for profiling.
- Collect the least amount of data possible for the exercise and keep for the shortest time possible.
- Be transparent with users of our products and platforms about our use of their data and any potential consequences or harms that could result.
- Be transparent about user rights to refuse profiling and other data rights (See Box 4).

---

9 International Privacy Professionals Association (IAPP) (2017) 10 Operational Impacts of the GDPR Part 5: Profiling https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-5-profiling/

10 Future of Privacy Forum (2016) Benefit-Risk Analysis for Big Data Projects https://fpf.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf

11 UK Cabinet Office (2016) Data Science Ethical Framework https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/524298/Data_science_ethics_framework_v1.0_for_publication__1_.pdf

3

Baking privacy and safety into platforms and products

Privacy by design is a way to ensure that a digital platform, tool, or service has privacy 'baked in', rather than simply tacked on in the end. Privacy by default is a mindset where design of every part of a product uses the highest level of privacy as the default setting. A "Data Privacy Impact Assessment" or "DPIA" (see Section 4) can help us ensure that we've taken all possible measures to design for privacy and safety. This again really just comes back to looking at the overarching principles of privacy and data protection right at the start of any given project.

Minimise the amount of data collected

- Only collect the data that is strictly necessary for legitimate business purposes such as:
  - Providing, operating or maintaining a site or application
  - Meeting an identified business purpose that the user is informed about (this can include research, monitoring and evaluation to improve content or measure impact)
  - Meeting legal obligations
- Only use data for purposes that users would expect, based on the information provided when they sign up or join, eg through Terms and Conditions and a Privacy statement.

Develop privacy and consent language and settings that are simple and transparent

- Create transparent and clear communication with users about the personal data that we collect and process, including information in culturally, age, and channel-appropriate ways about:
  - What information is being collected?
  - Who is collecting it?
  - How is it collected?
  - Why is it being collected?
  - How will it be used?
  - With whom will it be shared?
  - What will be the effect of this on the individuals concerned?
  - How long will personal data be retained?
  - Is the intended use likely to cause individuals to object or complain?
  - What are user rights related to their data?
  - Can they expect any feedback or response related to data they have provided? When?
- Ensure that consent for collecting and using personal data is 'opt in', not assumed or 'opt out'.
- Make it clear when we are relying on any other lawful basis for the collection and processing of personal data.
- Design consent processes in ways that help users understand privacy and data uses (see Box 8).
- Choose the most private rather than the most open settings during design.
- Disable location settings or ensure that users understand and consent if we are tracking them.
- Allow users to delete or remove their photos, comments, profiles and any other data.

Determine what systems we will use to protect, store and maintain the data

- Are we able to ensure the rights of data subjects in our system? (See Box 4).
- Will our backend systems enable us to securely record, manage and trace consent? (see Box 11).
- Do we have data agreements in place with any third parties who will have access to the data? (See Section 8 and Annex 1 for a sample data sharing agreement).
- Do we have a plan in place, with responsibilities assigned, to manage a data breach?

Box 4

Data subject rights

The GDPR lays out the following data subject rights that must be upheld when processing data.[12]

Right to be informed about the collection and processing of their personal data. The information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Data controllers must provide information to data subjects within one month of receiving a request.

Right of subject access meaning that a person has the right to obtain a copy of their personal data, along with an explanation of the categories of data being processed, the purposes of processing, the categories of third parties to whom the data may be disclosed, the period for which the data will be stored (or criteria for determining that period), and information about other rights of data subjects.

Right to rectification meaning a data subject can request any errors in their data to be corrected.

Right to erasure (aka the 'right to be forgotten') meaning that data subjects can request deletion of their personal data if it is no longer needed for its original purpose or where processing is based on consent and the person withdraws their consent (and no other lawful basis for processing exists).

The right to restrict processing meaning that a person can request that their data is no longer processed or that its processing is limited, even if it is still stored by a data controller/processor.

Right to data portability meaning that data subjects can receive from the data controller a copy of their personal data in a commonly used machine-readable format, and to transfer it from one data controller to another or have the data transmitted directly between data controllers.

The right to object to processing of their personal data on certain grounds in addition to the right to object to processing carried out for the purposes of profiling or direct marketing. In this case, for a data controller to continue processing, it must demonstrate that it either has compelling grounds for continuing the processing, or that the processing is necessary in connection with its legal rights.

The right not to be evaluated on the basis of automated processing meaning that (with a few certain narrow exemptions), data subjects have the right not to be subject to decisions based solely on automated processing which significantly affect them.

12 See the Information Commissioner's Office 2017 guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

4 Conducting a risk assessment

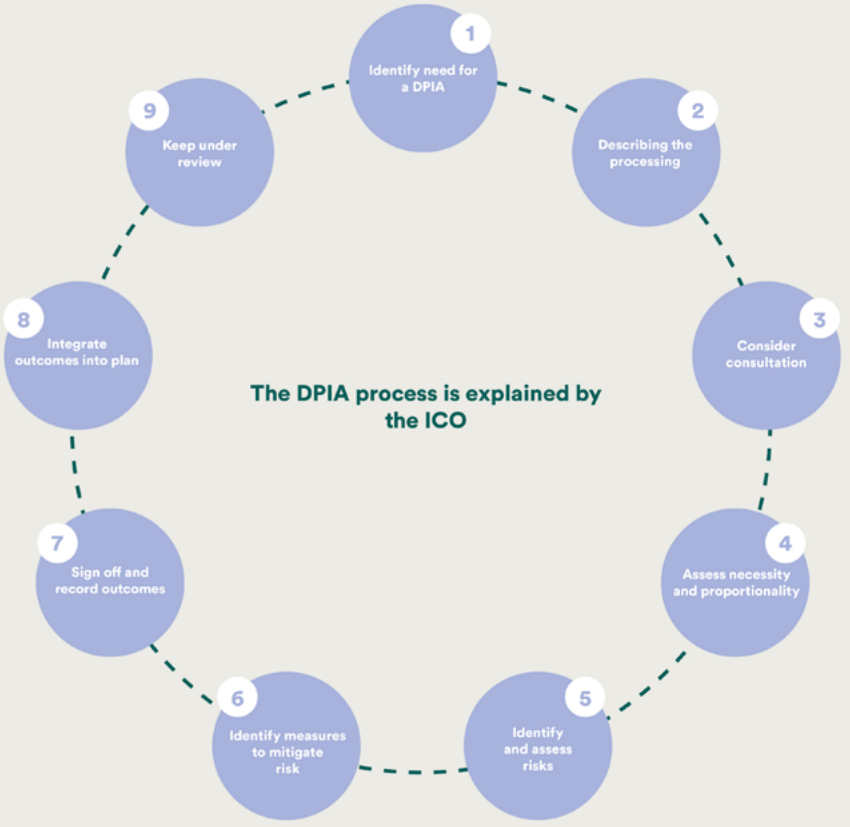
Risk assessments allow us to systematically assess whether we've addressed all the potential risks in our initiative and have documented the decisions taken and any remaining risk and the mitigations to be put in place to minimise these. The GDPR recommends a Data Privacy Impact Assessment (DPIA)[13] for any data processing that involves vulnerable individuals, children, or sensitive data and mandates their use in some cases such as when processing children's personal data for profiling or automated decision-making or offering online services directly to children. In the case of Girl Effect, we combine our overall risk assessment process with our DPIA so that we have a holistic view of safeguarding risks.

Girl Effect's Risk Assessment Form is where we:

- Highlight any risks that result from research, or from the digital tool, service or platform that we are designing. This includes overall risks, both online and offline, as well as data and privacy-related risks. It should have a strong gender lens.
- Assess the likelihood and severity of those risks, including to individuals' rights and interests as relate to data.
- Identify measures to avoid, eliminate, mitigate or manage risks, and document by when those measures need to be in place, and who is responsible and accountable.

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include the steps below:

Box 5



13 For a full overview of the DPIA process, see the Information Commissioner's Office (2017) DPIA Guidance. https://ico.org.uk/media/about-the-ico/consultations/2258459/dpia-guidance-v08-post-comms-review-20180208.pdf

We should conduct a risk assessment for every product, service or feature:

Because Girl Effect works with vulnerable populations, we collect and process personal and sensitive data of children and young people, we do so at a relatively large scale, and in some cases we use the data for profiling, we require a risk assessment/DPIA for our products, services and features. (See the ICO's DPIA guidance for more information)[14] We should also do a "light-touch" risk assessment whenever new or updated features are being introduced and when substantive changes are made to the data that we collect. (See Annex 4 for a sample risk assessment form.)

In the risk assessment, describe the nature, scope, context and purposes of data processing, including:

- List the personal data we plan to collect and process and determine whether any of it is sensitive (eg data from or about children or vulnerable groups). See Annex 3 for an example of how we've done Data Mapping Workshops in the past to generate this data as a team.
- Describe the processing activities, who will do the processing, and what are the associated risks.
- Check whether the data processing is necessary for and proportionate to the purpose; and, if not, make adjustments.
- Determine our lawful basis (or bases) for data collection (see Box 6).
- Describe our data protection and compliance efforts.
- Explain what will we do with the data? Will we use it for profiling?
- With whom will we share it? (see Section 8).
- Where will we store it? How will we secure it?
- Will we transfer or share it? With whom? Why?

The team conducting the risk assessment should:

- Work together with or ask for advice from Girl Effect's data protection officer (DPO).
- Record and file the outcome of the assessment, including any difference of opinion with the DPO.
- Implement the mitigation strategies and measures identified.
- Revisit them periodically or when a change in the product or the context triggers a review, for example, when a new feature is added or if censorship increases in a particular country.

Risk assessment preparation should be led by the product or brand team with support from the Safeguarding Focal Point. The risk assessment should be reviewed by a member of the safeguarding team who supports the specific product/brand. It should have sign off from the product/ brand director and the DPO or legal counsel where necessary.

The team conducting the risk assessment should document:

- The name and details of our business.
- Any controllers on whose behalf we are acting (if we are processing data for others).
- Our representative and the data protection officer.
- Categories of the processing carried out.
- Details of data transfers to third countries, including documentation of the transfer mechanism safeguards in place, if applicable.
- A general description of technical and organisational security measures.

The ICO can request to see risk assessment/DPIA documentation if ever they have cause to question our data protection and privacy practices.

---

14 Organisations with less than 250 employees need to keep these records if their data processing activities are not occasional; if they could result in a risk to the rights and freedoms of individuals; or if they involve the processing of special categories of data (sensitive data or children's data). See the Information Commissioner's Office (2017) DPIA Guidance. https://ico.org.uk/media/about-the-ico/consultations/2258459/dpia-guidance-v08-post-comms-review-20180208.pdf

Box 6

Determining a lawful basis for data processing

For each digital product or service, Girl Effect needs to determine the lawful basis under which it is collecting and/or processing data. There are six different lawful bases listed in Article 6 of the GDPR, but only the following three currently apply to Girl Effect's activities[15]:

Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party (unless there is a good reason to protect the individual's personal data which overrides those legitimate interests).

Though consent is one possible lawful basis for processing children's data, it is not the only option. Relying on consent as a lawful basis for processing personal data when offering an online service directly to a child is tricky because only children aged 13 or over are able provide their own consent. (This age limit is subject to legislative change and varies by territory.) For children under 13, consent needs to be obtained from whomever holds parental responsibility for the child - unless the online service being offered is a preventive or counselling service.

An alternative basis such as legitimate interest may be more appropriate and provide better protection for the child. Legitimate interest may be the best lawful basis if an organisation can assume control over the processing and take responsibility for demonstrating that it is in line with people's reasonable expectations and wouldn't have an unwarranted impact on them. Children, however, still require specific protection if their personal data is used for marketing purposes or creating personality or user profiles.

Since Girl Effect also collects data from vulnerable children (special category data), we will likely need to choose a lawful bases from Article 6 and also one from Article 9 (2). Below are listed the secondary circumstances that Girl Effect may wish to rely on in order to lawfully process special categories of data:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(e) processing relates to personal data which are manifestly made public by the data subject.[16]

---

15 See the Information Commissioner's Office (2017) Children and the GDPR. https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf

16 See the Information Commissioner's Office (2017) guidance on accountability and governance. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

Box 7

Consent and parental consent for digital platforms and services

Regardless of the basis for processing, we need to be transparent from the start about the data we collect, what we will do with it, who we'll share it with, and for how long we'll keep it. We also need to inform people about their rights with regard to the data we have about them (see Box 4). In some cases, we may need consent from a parent or guardian in order to collect and process children's data. Girl Effect takes reasonable and proactive measures to ensure that its users have understood the age limitations, data collection, and data processing done through or by any of its products. We also take additional steps in any situation where such collection and processing poses a substantive risk to the child's privacy.

Conducting a data map and risk assessment (see Section 4) allows us to clarify and document the flow of data in and out of our product or platform so that we can determine whether consent is needed and so that we can create transparent consent processes. The Data Protection Officer should review and confirm whether consent and/or parental consent are necessary.

The Article 29 Working Party published additional guidance on consent in April 2018.[17] They note that:

"...When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities.

If the users state that they are over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful.

If the user states that he/she is below the age of digital consent then the controller can accept this statement without further checks, but will need to go on to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility."

The GDPR does not say how to obtain parental consent, but the Working Party guidance recommends the adoption of a proportionate approach. In other words, getting parental consent could involve collecting a limited amount of information, such as contact details of a parent or guardian. What is

considered reasonable depends upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification by email may be sufficient. But in high-risk cases, it may be appropriate to ask for more proof so that parent or guardian consent can be verified and retained."

Here's an example of how a parental or guardian consent process might work:

"An online gaming platform wants to make sure underage customers only subscribe to its services with the consent of their parents or guardians. The controller follows these steps:

Step 1: ask the user to state whether they are under or over the age of 16 (or alternative age of digital consent) If the user states that they are under the age of digital consent:

Step 2: service informs the child that a parent or guardian needs to consent or authorise the processing before the service is provided to the child. The user is requested to disclose the email address of a parent or guardian.

Step 3: service contacts the parent or guardian and obtains their consent via email for processing and takes reasonable steps to confirm that the adult has parental responsibility.

Step 4: in case of complaints, the platform takes additional steps to verify the age of the subscriber.

If the platform has met the other consent requirements, it can comply with "proportionate effort" through the above process."

---

17 Article 29 Working Party "Guidelines on consent under Regulation 2016/679" revised and adopted on 10 April 2018. https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf

Box 8

Good practice for consent

Regardless of whether consent is given by a child or by a parent or guardian, it must be a clear "opt-in" process, not a pre-ticked box or an assumption that "by using this site you consent to…." Consent information needs to be in a format that people can easily comprehend.

Some good practices for designing transparent, digestible, and effective consent processes include[18]:

Upfront consent is a notice that shows up early in the relationship. It is separate from the Terms and Conditions and it focuses on specific data processing activities.

Layered consent is when a short and simple version of Terms and Conditions and/or a Privacy Policy are provided, with progressively more detail or links to full versions so that people can find out more if they'd like.

Just in time consent is a consent notice that you see right before a particular kind of data collection or process happens, so that a person can make a choice in the moment. An example of "just in time" consent is when you see a pop-up box on your mobile phone when an application would like to access your location or your photos.

Audio consent is used by Girl Effect's TEGA Recruitment App. Simplified consent terms are played on a mobile for guardians and girls. These can be replayed if needed.

Quizzes are a way to check whether the person has understood what is meant by consenting. After playing the audio consent in the case of TEGA, the person giving consent takes a quiz.

Cartoons to explain consent are another option, in that they can make consent more understandable.

18 For more tips on designing good consent, see Nathan Kinch's May 2018 series on on "Data Trust, by Design: Principles, Patterns and Best Practices (Part 2 -- Up Front Terms and Conditions) https://medium.com/greater-than-experience-design/data-trust-by-design-principles-patterns-and-practices-part-2-up-front-terms-and-conditions-337c6b37552d and Part 3 -- Consent https://medium.com/greater-than-experience-design/data-trust-by-design-principles-patterns-and-best-practices-part-3-consent-70ccdb085f73

5

Protecting and securing data

Data security is an umbrella term for the different steps and processes that an organisation takes to protect data and keep it private. It encompasses things like IT (information technology) tools, the use of cloud based services, back up mechanisms, and the storage of hardware in secure locations. Data security also includes IT security and the choice of software, encryption, firewalls, vetting of staff, and staff access to data.

IT security is a field unto itself and we do not cover it in full here. Our organisational IT policies will cover aspects such as securing laptops and devices, secure data storage, and organisational data privacy and security.

In most situations, Girl Effect will serve as a "data controller" and our technology partners will be "data processors" (see Box 9). The GDPR outlines specific responsibilities for each of these roles in terms of data privacy and security, and both are liable in the event of a data security breach.

When developing our privacy policies or consent processes, we'll need to be able to ensure people know that we and any partners have adequate security in place. Assessing a partner's data security capacity is thus a critical task before any partnership agreements are signed (See Section 8).

Box 9

Data controllers and data processors

- The GDPR defines the two main roles with regard to data as the "data controller" and the "data processor".[19]
- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

Here are some general privacy and security practices that teams should consider:

- Do we and our partners have state of the art technical measures and up-to-date good business practices to ensure that data is transmitted, stored and managed in a secure and safe way, including but not limited to:
  - Password protected devices
  - Encryption and pseudonymization
  - Data risk management policies and procedures
  - Data breach management policies and procedures
  - Staff training on IT security, data privacy, and who/how to notify in case of a data breach
- Is access to personal data restricted to a 'need to know' basis, taking into consideration sensitivity of and potential risks related to the data? Do we regularly review who has access? (See Box 11 on Safety, security, and consent management on the back end).
- How and when will we anonymise, retain, maintain, and delete or destroy data? Note: our DPO is responsible for data governance and managing data retention overall. A product level lead should be assigned for each data-related exercise. (See Box 10 for tips on Data retention policies).
- See Section 8 for more detail on what partners should have in place.
- The ICO offers in-depth guidance for overall organisational security measures.[20]

19 Information Commissioner's Office (ICO) (2017) Guide to the General Data Protection Regulation (GDPR). https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

20 The Information Commissioner's Office (ICO) provides more detail on security measures organizations should have in place. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/#_What_are_%E2%80%98confidentiality,

Box 10

Data retention

Data retention policies should reflect the fundamental principles of GDPR in capturing only that data which is required, keeping that data for as short a period as possible in the circumstances and keeping it as secure as possible at all times. Whilst retention periods for each team, product and data type will vary, this overarching tenet should apply to all.

Personal Data retention periods should be determined by reference to the following checklist:

- [ ] Data source (who/where we are collecting the data from)
- [ ] Type of data
- [ ] Reason for keeping data
- [ ] Personally Identifiable Information (PII) (Y/N)
- [ ] Will data be aggregated or anonymised? (and thus not subject to retention period)
- [ ] Length of time data is to be held
- [ ] How will data be destroyed

Safety, security, and consent management on the back end

As part of Girl Effect's efforts to better manage our data, we've updated our core infrastructure and our content hub. The core infrastructure enables us to centralise all of our applications and services into one global cloud-based solution. The TEGA content hub set up ensures that our video materials are securely stored and managed. Both of these systems are designed with state of the art industry level security that allows us to keep data secure and manage privacy. They also allow us to record, trace and manage consent and to fulfill data subject rights (see Box 4).

What is the core infrastructure?
The core infrastructure centralises all Girl Effect's applications and services into a global cloud-based solution where all of Girl Effect's current and future applications will be hosted. These core services will offer centralised authentication and storage of system and end users which will allow us to secure databases in one environment. By centralising the user data and providing single sign-on functionality we enable better insight into user behaviour across portals in cases where users are uniquely identified.

What is the user data store?
The user data store is part of the core infrastructure. It provides Girl Effect and relevant third parties a safe, secure and central data store for all the user-related data we collect. Having all user data together on one platform and in one service means we have centralised monitoring, maintenance and security. Data fragmentation and duplication is reduced. The central user data store also helps any future business information systems gather relevant data.

What is the data platform?
The data platform allows us to collect and store all of the data from various sources in a central platform and then connect analysis and analytics tools through a single connection. This also automates the collection of data from various sources and allows us to report on metrics in near real time.

What is the content hub?
The content hub is where we hold TEGA data. It is accessible by a limited number of users based on their role. Within the hub, content from interviews with girls can be flagged if safeguarding concerns are noted. Translation happens within the hub so that interview content does not need to be downloaded. Translators are only able to hear audio; they do not see the face of the person being interviewed.

How does the infrastructure help us keep children and young people safe and manage consent?
Industry leading practices have been employed to ensure we keep the user data and the integrity of our applications intact. For authentication and access control, we make use of an industry standard called OpenID Connect, which we combine with the well known Role-Based Access Control (RBAC) model, with a clear separation in the responsibilities that lie with our system and that of application developers. We are also able to delete users that have withdrawn consent or request to have their accounts deleted. Having all user data stored centrally makes this process more effective and efficient.

6 Legalities

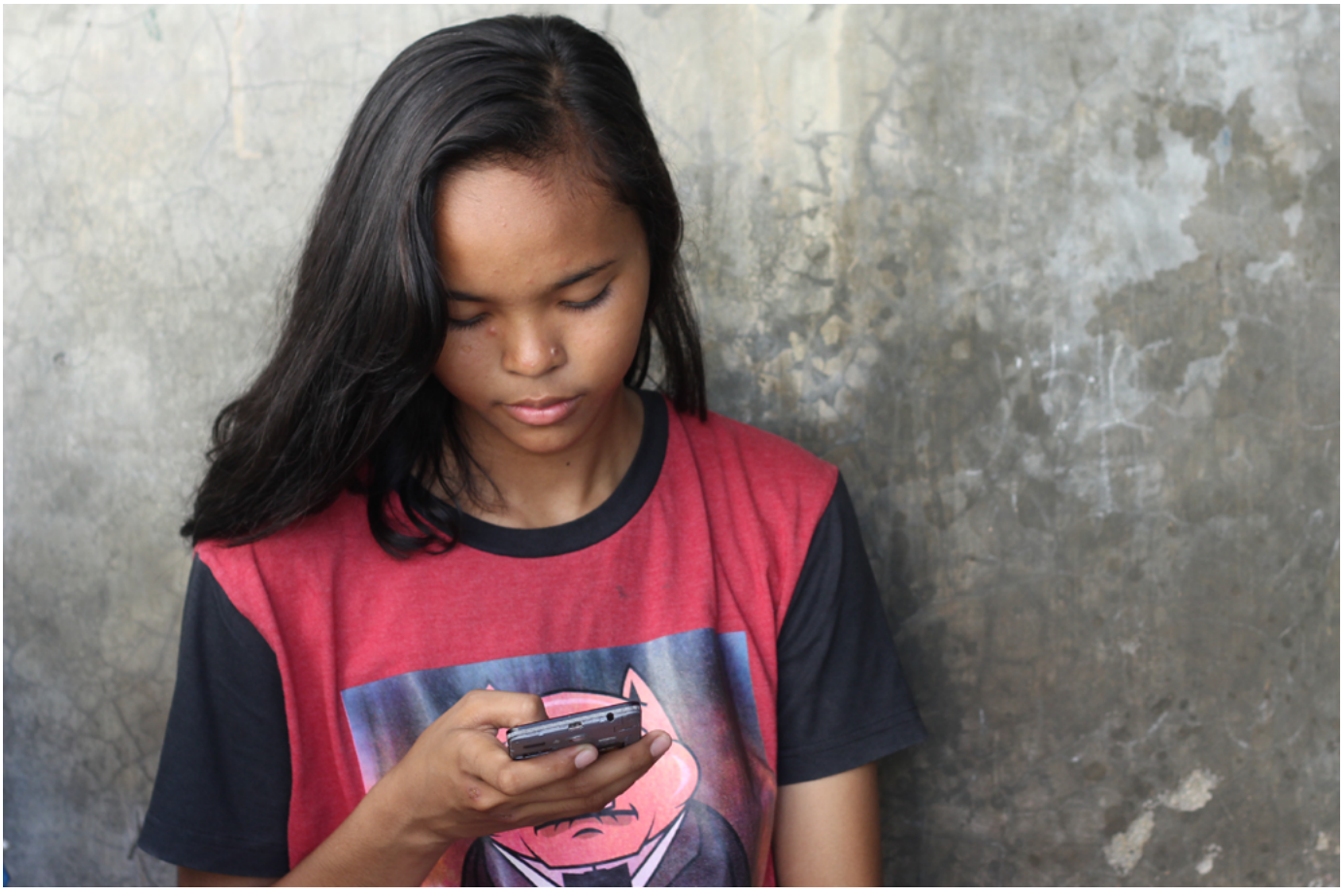
Many countries have specific laws and regulations relating to child safeguarding, child protection, mandatory reporting of incidents of child abuse, and data privacy. The European Union's General Data Protection Regulations (GDPR), South Africa's Protection of Personal Information Act (POPI) and Rwanda's Data Revolution Law are examples of local data legislation.

More and more countries are enacting this type of legislation, which sometimes includes provisions relating to whose data can be collected, what type of data can be collected, and whether data can be transmitted outside of the country and in which cases. There may also be laws related to children's data; direct marketing, spam or e-privacy; age of consent; research and media; use of images, and blasphemy and libel. It's important to be aware of these and check compliance to avoid fines, being shut down, or putting children and young people at risk through the use of our products and services. The Privacy and Electronic Communications Regulation (PECR) is one such piece of legislation that applies to all electronic communications with cross over with GDPR in this area.

Girl Effect may need to secure local counsel to ensure that we maintain compliance with local laws, are updated when new laws are introduced. We also may need to seek specific advice around application where EU/UK and national laws are contradictory. We will also want to design in ways that take these laws into consideration and review content that may be affected by these laws and regulations.

Some useful websites and publications include:

- DLA Piper's Data Protection Laws of the World
- GDPR orientation from the UK's Information Commissioner's Office (ICO)
- Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey



7 Content considerations

As part of our work, Girl Effect produces, curates, and shares content. We encourage children and young people to do the same. For this reason, we need to ensure that our content does not create risk for them, Girl Effect or its donors, and we need to also set up processes that protect children and young people when they share or produce content. This includes protecting them from inappropriate or harmful content; reducing risks when they produce content for our platforms; and helping them stay safe when they participate and share their ideas, opinions and content through our platforms and products and/or those of partners.

Some good practices for reducing risk to children and youth and to Girl Effect overall include:

Foster debate on contentious topics; yet promote positions based on globally recognised girls' rights

- Review existing research, do additional desk research, and conduct formative research (see Section 2) to gain insights into the context in which girls live, social norms around them, and the barriers and issues they face.
- Work closely with local partners who understand the landscape and context.
- Ensure that we are guided by our Theory of Change to determine an appropriate appetite for risk in our content choices.
- Assess how the channels and platforms that we are using influence the format of the content and the levels of risk that girls may be exposed to. For example, in some cases, if girls are anonymous on a platform, the risk to them may be lower. However, in other cases anonymity has led to greater trolling of girls and women.

Actively manage the community and ensure engaged moderation

A safe community for users of a platform or site requires active creation of a safe and supportive environment, clear rules, and good moderation. Moderation ensures that the environment is positive and uplifting for participants because moderators help facilitate meaningful conversations. They also create safe spaces for engagement by removing offensive or upsetting comments, harmful content, and managing trolling and other behaviours that make the community unsafe.

Below are some general tips for moderation and community management. Girl Effect's Moderation Guidelines offer detailed orientation on moderation and community management.

- Conduct a risk assessment and do not launch a community or open commenting until we are satisfied that risks can be managed.
- Create child-friendly / girl-friendly community guidelines so that expected behaviors are clear.
- Create or adapt a list of online situations that require response or escalation.
- Identify and train moderators.
- Agree on the frequency and style of moderation.
- Ensure that response procedures are in place, including reporting protocols and signposting. These need to be adapted and contextualized to each product or country (see Box 12 for an example of reporting protocols).
- Maintain a moderation register.
- Conduct regular reviews and spot checks.
- Feedback to the content team so that they can adjust the content.
- Use automated flags to catch sharing of location, contact details and personal information.

Moderation on third party social media platforms

Most social media sites link to personal profiles, and these often reveal personal data such full names. They may also link to opinions, comments, or photos that contain sensitive information.

Some additional aspects to keep in mind, depending on the social media platform, include:

- Reminding users that their comments can be seen by others (especially if they are navigating from an anonymous site such as Springster and a social media platform with visible profile information).
- Keeping a close eye on any suspicious behaviors of users.
- Frequently posting content about how to stay safe online and how to manage privacy settings.
- Ensuring that any one-to-one (private) channels are regularly moderated by more than one team member, to avoid any potential for staff-user abuse.
- In the case of messaging platforms that do not have an option for masking user phone numbers and/or profiles, extreme care should be taken.

Moderator Code of Conduct

Whether moderating on a platform designed by Girl Effect or on a social media site, some core aspects that moderators should know include:

- Never go behind a user's back to access her contact details or personal data.
- Never share users' personal details with others.
- Never befriend or accept contact requests from users on a personal social media account.
- Never share personal details about yourself or your colleagues with users.
- Never speak on behalf of Girl Effect unless this is part of your role and has relevant approval.
- Never ignore content or behavior that could upset or harm user.

Talk about it

In addition to moderation, it's important to constantly remind users what the "community rules" are and to share content related to online safety, such as:

- Signaling and discussing the risks of participating and sharing information online.
- Reminding and alerting users about which information is private and which is public, especially if we have linked a Girl Effect site (which is more private) to a social media site (which may be more public or open).
- Including content about online safety and privacy in the mix of other content.

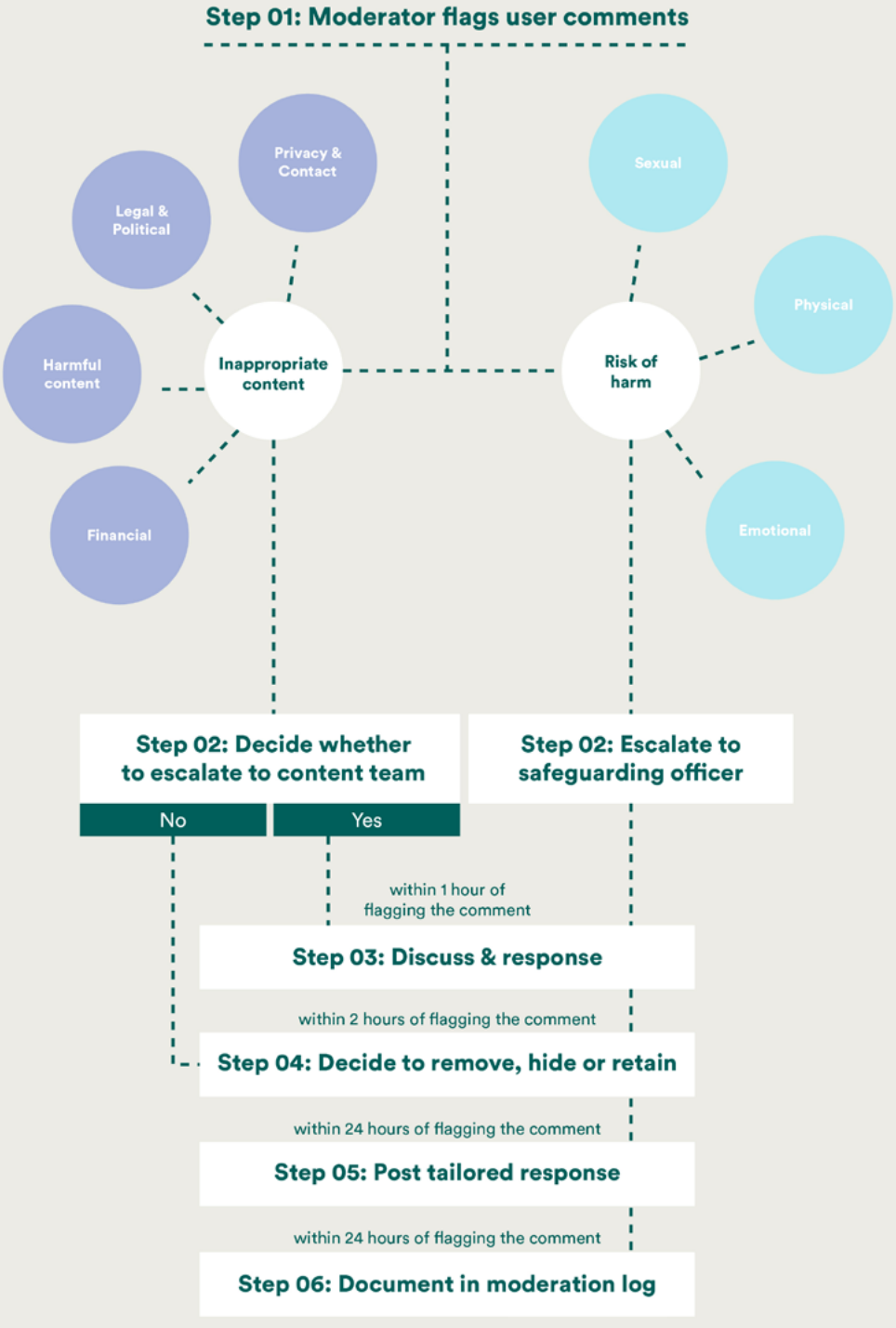
Signposting

The platforms and services that Girl Effect develops and runs are digital. Whenever possible, when creating content, we should signpost users to relevant local support services. Responsible signposting involves:

- Setting criteria for vetting girl-friendly or child-friendly services, or verifying services that have been vetted by a trusted, local partner.
- Mapping child protection services (where possible) so that signposting can be done where necessary and/or in case of disclosures.
- Regular checks and services vetting.
- Providing links to vetted service providers in stories and other content so that users know where they can find support.
- Informing partners that they may experience a higher demand and verifying their capacity to manage an influx in requests.
- Making sure it is clear that we are not a helpline and that we can only share information and ideas for users to take steps on their own towards addressing the issue.
- Making decisions to not post content on sensitive topics if we do not have anywhere to signpost.

Box 12

Sample reporting protocol: Springster



User-generated stories

On our platforms, we encourage girls and boys and young people in general to share their stories. At times, these stories could bring risk to an individual, for example if the topic is sensitive or stigmatising, or if she reveals personal information. Children and young people, however, do have a right to own and control their own stories, so balancing this right to control and ownership with risk mitigation and safeguarding can be tricky.

Some ways to manage risk related to user stories include:

- Create clear and meaningful terms and conditions and consent processes for use of the story.
- Assess the level of potential risk that a story might bring to a child or young person:
  - Does it offer information that would enable someone to locate them (whether this appears in writing or in photos)?
  - Does it reinforce harmful gender stereotypes, gender norms, or ideologies?
  - Does it make unfounded accusations or lay one-sided blame?
- Attribute the story according to its potential risk; for example:
  - If a story is highly sensitive, anonymise it by changing details, using a pseudonym and age, changing the location, and not informing the child or young person that their story was used.
  - If a story is low-risk, only use a first name, country, sketched image (no photo) and age. In this case, it may be fine for a children or young person to retain ownership.
  - This may need a case-by-case review, as in some cases it may be acceptable to share a child or young person's identity if an full assessment of potential risks has been done.

Accountability and complaints

In addition to ensuring that we take data subject rights (see Box 4) seriously, we need to be accountable to girls and other users of our platforms and products for what happens while they are using them. For this reason, it's important to have a way for a user to get in touch with us should they wish to report something about the site or how we are treating them on the site. We also need to be sure that we are thinking long-term and have a plan in place for what happens if and when the platform or product closes down.

In order to be accountable, we should have the following in place:

- A clear and visible way for users to lodge complaints about the use of their data or any other aspects of the platform or service.
- Procedures in place for receiving and responding to complaints, with clear timeframes for action.
- A plan for responding to a data breach.
- A plan for informing users of a data breach that may lead to harm (see the GDPR for more on determining whether, how and where to report).
- A plan for how we will manage users' information, user-generated content, content and any support services if/when the project ends or the platform or service closes down.

8 Working with partners, third parties, and social media

Girl Effect works with several types of partners -- financial partners, portfolio partners, design & content partners, implementing partners. We also link with third party technology platforms and social media sites in order to reach more people, better understand our audience, and drive traffic to our products and platforms. Both Girl Effect's Safeguarding Policy and the EU's General Data Protection Regulation (GDPR) provide clear orientation on how to engage with partners to keep children and young people and their data safe.

Box 13

Types of partners

Financial partners: Organisations or individuals who invest or co-invest, either financially or through in-kind donations, in Girl Effect initiatives but have no direct contact with our staff, operations or children and young people.

Portfolio partners: Organisations or individuals who invest or co-invest, either financially or through in-kind donations, in Girl Effect and work in collaboration with Girl Effect in ensuring delivery on the ground. This may include both direct and indirect contact with children and young people through the co-design and delivery of initiatives.

Design & content partners: Organisations or individuals who design and produce content for Girl Effect products and campaigns. This may include direct contact with children and young people as well as an indirect impact on children and young people through the materials that are produced.

Implementing partners: Organisations or individuals who are responsible for implementing or co-implementing Girl Effect initiatives who have either direct or indirect contact with children and young people. For example, research agencies collecting data directly from children and young people, technology companies who process or analyse data for us, and agencies responsible for facilitating events or activities with children and young people.

Third party platforms and social media sites: Technology firms, data analysis platforms and social media sites who have direct access to our users' personal and sensitive data. In some cases, we have a contact point and a contract. In other cases we are users of a platform or site without a direct contractual agreement (eg when we create a Facebook page or an Instagram account)

Before working with a partner:

- The ethical implications of working with the partner should be discussed by senior leadership. (See Global Safeguarding Policy, page 12). This should cover aspects such as the privacy risk and benefits to children and young people from the partnership and any use, share, or monetizing of data.
- The partner should go through appropriate due diligence (see Annex 2 for an example of how Girl Effect conducts due diligence).
- Conduct reference checks for any local partner staff working on a Girl Effect project who handle data and/or engage children and young people.
- Any partner that will have access to children in person or through a product, platform or service must have a safeguarding briefing and training and sign a safeguarding agreement.
- Any partner that will have access to children's data should provide sufficient guarantees about its security measures. We can request copies of any security assessments as proof and, where appropriate, visit their premises.
- Any partners and or affiliates working directly with children must sign off on Girl Effect's Code of Conduct (see Global Safeguarding Policy, page 14).
- Data sharing agreements must be developed and signed off if partners have access to any personal data, child or young person data (see Annex 1 for sample data agreement language).
- If there is any data sharing, this must be transparently included in the terms and conditions and privacy policy that accompanies the product and/or service that shares the data.
- In the case of partners with lower capacities, we will need to evaluate the potential risks and determine how much time or resources we are willing to invest in ensuring that child safeguarding, data privacy, and data security are covered. This should be documented and filed in case it is needed for future reference.

What to ask before contracting a data processor:

When assessing whether to work with a data processor, some things to ask include:[21] [22] [23]

- What measures do they have in place to ensure and demonstrate compliance with GDPR principles? Do they maintain records of their processing activities that are compliant with GDPR requirements? Can they produce those if asked?
- Are they planning to work with any sub-processors?
- How are they equipped to deal with subject access requests? (See Box 4 and Box 11).
- Who has access to the data and how is this determined? What controls are in place?
- What experience do they have with conducting data privacy impact assessments?
- Are they prepared to approach the work from the lens of privacy by design / privacy by default?
- What information security compliance measures are in place? Do they stress test their systems?
- Have there been any past security issues, data breaches or criticisms of their tools and services? How, and how quickly, did they respond?
- How do they govern their data? Who is responsible for data security and data breaches?
- What are their data security breach management and notification policy and procedures?
- Have any of their staff been trained on GDPR? How have they prepared internally for GDPR compliance?
- How likely is it that the vendor will be around in the long-term? If they close down, what will happen with the data they are holding?
- Do they have a privacy policy? Do they share or sell data to third parties? How do they make their money?

What about third party platforms, apps, and social media sites?

The situation is less clear when working with other mobile or online platforms, apps or social media sites. GDPR is less clear when it comes to this type of relationship, and we may not have a formal relationship with this type of third party site other than a page or an account. These partnerships may encourage children and young people to share data in ways that may create risk or we might be opening them up to being unethically profiled or that may violate their privacy rights.

Some steps we can take to better assess decisions about these partners:

- Conduct a review and assessment of their terms and conditions and privacy policies to see what their policies are and whether they are GDPR compliant.
- Try to get in touch with someone from the third party who can discuss data privacy and security, children, and the GDPR.
- Conduct a thorough risk assessment (eg data privacy impact assessment / DPIA) to weigh the benefits and the risks of these third party platforms, apps or sites. (See Annex 4 for a sample risk assessment form).
- Consult with the Data Protection Officer or legal counsel.
- Make the decision that holds the most benefit for our children and youth users.

---

21 See the ICO's draft guidance on contracts and liabilities between controllers and processors for more detail https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

22 See 7 questions you should ask technology vendors about GDPR for an example of how one data company has worked to comply https://www.episerver.com contentassets/17e94626cd544011810e82dee0868a24/gdpr_whitepaper_7_questions_to_ask-technology_vendors.pdf

23 The Electronic Frontier Foundation (EFF) has an in-depth piece from 2018 with a nice checklist on How to Assess a Vendor's Data Security https://www.eff.org/deeplinks/2018/01/how-assess-vendors-data-security

Annexes

Sample data sharing agreement language

This data processing addendum is made on the ___ day of _____ 2018

Parties

(1) [insert organisation's details], a limited company and a [Organisation] registered in England, United Kingdom ([Organisation] no.1141155) with its registered address at [insert full address] (the "[Organisation]")

(2) [insert data processor's details] (the "Supplier")

Background

A. The [Organisation] and the Supplier have already entered into a contract (defined below as the Main Contract) for the provision of services by the Supplier to the [Organisation].

B. This agreement is an addendum to the Main Contract to ensure that it is compliant with new data protection legislation which applies to both parties.

C. It is acknowledged by the Parties that given the location of the Supplier and the data subjects

Agreed Terms

1. Definitions

1.1 In this Addendum the following definitions shall apply:

"Data Protection Legislation" means all legislation regulating the processing of personal data as may be applicable from time to time in the United Kingdom, which at the date of this Agreement includes the Data Protection Act 1998 and the EU General Data Protection Regulation 2016/679 (GDPR), and any successor legislation.

"Data Controller", "Data Processor", "Data Subject", "Personal Data Breach" and "processing" shall have the same meanings as used in the Data Protection Legislation and derived terms shall be construed accordingly.

The "Main Contract" means the MSA contract and any associated Work Order thereunder between the [Organisation] and the Supplier dated [insert date] relating to [the provision of xxx services].

"Personal Data" means personal data (as defined in the Data Protection Legislation) which is processed by the Supplier under or in connection with the Main Agreement and this Addendum.

2. Introduction

2.1 The Parties agree that the [Organisation] is the Data Controller and the Supplier is the Data Processor in respect of all Personal Data for the term of the Main Agreement.

2.2 Both Parties will comply with all applicable requirements of the Data Protection Legislation in the processing of the Personal Data.

2.3 The Schedule to this Addendum sets out information relating to the Personal Data and its processing under the Main Agreement that the Parties are required to set out under the Data Protection Legislation.

3. Obligations of the Supplier

3.1 The Supplier shall process the Personal Data only for the purposes of performing the Main Agreement and this Addendum and only in accordance with instructions therein or received from the [Organisation] in writing, unless it is required to process the Personal Data by law in which case the Supplier shall inform the [Organisation] (to the extent permitted by law) of that legal requirement before carrying out the relevant processing.

3.2 The Supplier shall comply with all reasonable instructions given to it in writing by the [Organisation] relating to the processing of the Personal Data.

3.3 The Supplier shall ensure that all members of staff who have access to the Personal Data are obliged to keep the Personal Data confidential, and that the Personal Data is only accessible to those members of staff who need access to it in order to perform the Main Agreement or this Addendum.

3.4 The Supplier shall implement appropriate technical and organisations measures to protect the security of the Personal Data. These measures must ensure a level of security appropriate to the risk, taking into account the state of the technological developments, the costs of implementation of any such measures and the nature, scope, context and purposes of the processing, as well as the harm that might result from any unauthorised or unlawful processing of the Personal Data and from its accidental or unlawful destruction, loss, damage, alteration or unauthorised disclosure.

3.5 The measures referred to in clause 3.4 may include pseudonymising and encrypting the Personal Data, measures to ensure confidentiality, integrity, availability and resilience of the systems and services, the ability to restore access to the Personal Data in a timely manner in the event of an incident, and regularly assessing the effectiveness of any such measures.

3.6 If the Supplier wishes to engage a sub-contractor to process the Personal Data:

3.6.1 It may only do so if it has the [Organisation]'s written consent;

3.6.2 The Supplier must have a written agreement in place with the sub-contractor governing the terms of the processing, which must offer at least the same level of protection for the [Organisation] as the terms set out in this Agreement, and must meet any other requirements of the Data Protection Legislation from time to time; and

3.6.3 The Supplier shall remain liable to the [Organisation] for all acts or omissions of its sub-contractor or those employed or engaged by the sub-contractor as if they were the Supplier's own acts or omissions.

3.7 The Supplier shall:

3.7.1 Notify the [Organisation] without undue delay if it becomes aware of any Personal Data Breach relating to the Personal Data;

3.7.2 Notify the [Organisation] promptly, and in any case within 5 days, of any communication from a Data Subject relating to the processing of his/her Personal Data, or any other communications that it receives regarding either party's obligations under the Data Protection Legislation in respect of the Personal Data; and

3.7.3 Assist the [Organisation] with its obligations under the Data Protection Legislation, including in relation to any requests from Data Subjects, to data security, the notification of Personal Data Breaches to supervisory authorities and Data Subjects, data protection impact assessments, and consultations with supervisory authorities or regulators.

3.8 The Supplier shall within one month of termination of the Main Agreement, or at any time when requested in writing by the [Organisation], delete or return all Personal Data and any copies to the

[Organisation]. The Supplier may retain Personal Data only to the extent, and for such period, required by law.

3.9 The Supplier shall not transfer any Personal Data anywhere else out of the European Economic Area unless:

3.9.1 It has obtained the prior written consent of the [Organisation];

3.9.2 The Supplier ensures an adequate level of protection of the Personal Data that it is transferring to ensure the [Organisation]'s compliance with the Data Protection Legislation; and

3.9.3 The Supplier complies with any written instructions from the [Organisation] relating to the transfer or to the requirements in clause 3.9.2 above.

3.10 The Supplier shall keep accurate records to demonstrate its compliance with this Addendum and the Data Protection Legislation, and must allow audits and inspections by the [Organisation] in relation to the processing of the Personal Data.

3.11 The Supplier must tell the [Organisation] without delay if it is asked to do something that infringes the Data Protection Legislation.

3.12 The Supplier shall indemnify the [Organisation] against any loss or damage howsoever arising suffered by the [Organisation] in relation to any breach by the Supplier of its obligations under this Addendum.

4. Relationship between this Addendum and the Main Contract

4.1 This Addendum is intended to add to the Main Contract. In the event that any of the terms in this Addendum conflict with those in the Main Contract, the terms of this Addendum shall override those of the Main Contract to the extent of any such conflict.

5. Governing law and jurisdiction

5.1 This Addendum and any dispute or claim (including non-contractual disputes or claims) arising in connection with it shall be governed by and construed in accordance with the law of England and Wales. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising in connection with this Addendum.

6. Counterparts

6.1 This Addendum may be executed in any number of counterparts, each of which when executed and delivered shall constitute a duplicate original, but all the counterparts together shall constitute a single agreement. Transmission of the executed signature page of a counterpart of this Addendum by fax or email shall take effect as delivery of an executed counterpart of this Addendum.

This Addendum has been entered into on the date stated at the beginning of it.

Signed by ..... for and on behalf of [Organisation]

Signed by ..... for and on behalf of Quilt

Sample due diligence procedures for Girl Effect partners

Purpose

Prior to entering into a partnership with another organisation, Girl Effect reserves the right to conduct some basic checks to ensure that:

- There is a satisfactory financial and governance structure in place and the organisation is compliant with legal and regulatory requirements.
- The organisation is ethically sound and has sufficient safeguarding measures in place to ensure that it does not represent a risk to children or young people.

When due diligence checks are required

Due diligence checks are required when any of the following criteria are met:

- The value of the partnership exceeds £100k.
- The partner will be implementing activities directly with children and young people.
- The partner will be handling personal data relating to children and young people.

Depending on the nature of the partnership, it may not be necessary to complete all sections of the due diligence form. Please follow the guidance at the start of each section. Due diligence checks should be completed before any contractual arrangements are finalised.

Roles & responsibilities

The project manager:
- Coordinating the due diligence process and ensuring it is completed in a timely manner.
- Requesting all supporting documentation.
- Seeking final approval from the director of finance & operations.

Operations manager:
- Completing Section A where required.
- Making a recommendation regarding approval.

Finance manager:
- Completing Section B where required.
- Making a recommendation regarding approval.

Safeguarding officer:
- Completing Section C where required.
- Making a recommendation regarding approval.

Director of finance and operations:
- Final approval.

Partner details

Name of organisation:
Address:
Phone:
Organisation Registration No.:
Organisation's legal status:
Website:

Main contact name:
Role Title:
Email:
Phone:

Chief Executive Officer:
Email:
Phone:

Chief Financial Officer:
Email:
Phone:

Details of proposed partnership

Product:
Country of Operation:
Responsible Manager/Director:

Key Activities:

Partnership value:
Proposed start date:
Duration:

SECTION A: ORGANISATIONAL STRUCTURE & EXTERNAL COMPLIANCE

This section must be completed if:

- The value of the partnership exceeds £100k
- The partner will be implementing activities directly with children and young people
- The partner will be handling personal data relating to children and young people

Responsible for Completion

- Operations Manager in London or in country

Documents to be requested	Date received
Copy of registration documents with government departments (e.g. incorporation documentation, charity registration, business registration, tax registration etc)	
Staff Organisational Chart, including governance structure	
Copies on any policies in relation to governance, anti-corruption/bribery	
Copies of relevant insurance documents	

Key questions	Source of evidence	Observations	Recommendations • Approval • To achieve approval
Is the organisation registered with appropriate regulatory bodies?	Copy of registration documents		
Does the organisation have a board of trustees/board of directors who are separate from the day-to-day management team?	Org Chart Enquiry		
Are there the appropriate level of staff within the organisation with financial / governance skills	Org Chart Enquiry		
Are relevant legal regulations being adhered to e.g. regarding how staff are appointed, how they are paid, how their work is monitored?	Enquiry		
Does the organisation have adequate insurance in place for the activities it is being ask to complete for Girl Effect?	Policy Review Enquiry		
Other:			

Overall Recommendation:

Name: **Role:**

Signature: **Date:**

SECTION B: FINANCIAL MANAGER

This section must be completed if:

- The value of the partnership exceeds £100k

Responsible for Completion

- Finance Manager in London or in country

Documents to be requested	Date received
2 years of independently audited accounts	
Financial Procedures Manual or related policies (Should include procurement, authorisation of expenditure, bank payments (cheque, foreign payments, online and so on), cash payments (petty cash), payroll payments (bank, cheque, cash), reconciliations of cash floats and bank accounts)	
Sample report format to be used to monitor project income & expenditure	

Key questions	Source of evidence	Observations	Recommendations • Approval • To achieve approval
Is finance manual &/or accounting policies & procedures adequate to ensure good financial management?	Review of finance manual Enquiry		
Could the organisation be vulnerable to attempts at fraud, corruption or money laundering?	Review of finance manual Enquiry		
Do audited financial statements show sound financial management?	Audited accounts		
Is there any evidence of fraud or mismanagement in the past two years?	Audited accounts		
Are management accounts produced monthly with appropriate review? How are these accounts prepared?	Enquiry		
Are there separate bank accounts or accounting procedures for restricted funds?	Enquiry		
Will the income & expenditure for this project be separate & identifiable in accounting system.? Will the system produce financial reports which compare actual & budgeted expenditure.	Sample Report Format Enquiry		
Is the organisation compliant with all financial regulation – filing accounts, annual returns, tax returns etc	Sample Report Format Enquiry		
Other:			

Overall Recommendation:

Name: **Role:**

Signature: **Date:**

SECTION C: ETHICAL & SAFEGUARDING CONSIDERATIONS

This section must be completed if:

- The partner will be implementing activities directly with children and young people
- The partner will be handling personal data relating to children and young people

Responsible for Completion:

- Safeguarding Officer in country or Global Lead for Safeguarding

Documents to be requested	Date received
Copy of Safeguarding/Child Protection Policy, including Code of Conduct	
Reference from existing partner or donor. To include questions about safety & any contact with children	
Reference from local stakeholder. To include questions about safety & any contact with children	

Key questions	Source of evidence	Observations	Recommendations • Approval • To achieve approval
Has the organisation ever been associated with investments or operations which exploit or harm children either directly or indirectly? If so, how have these been addressed?	Online Search / Dirty Word Search		
Has the organisation committed any legal, ethical transgression or been subject to negative media attention that may impact the reputation of Girl Effect?	Online Search / Dirty Word Search		
Does the organisation have any strong political or religious affiliations?	Online Search		
How does the organisation vet it's staff and volunteers and ensure they are suitable for the work?	Enquiry / Policy Review		
Does the organisation's website, social media & other communication materials uphold the dignity, privacy & safety of children?	Online Search		
Does the organisation have a good reputation locally? Is the organisation seen as "child-safe"?	Reference		
Other:			

Overall Recommendation:

Name: **Role:**

Signature: **Date:**

Final Approval: **Role:**

Data Mapping Workshop

Objectives: To unpack why we collect data, what data, from whom, where it flows, and more
Materials: Index cards with the data lifecycle steps written on them; lots of post-its and markers
Works for: Discrete teams (one product team) and support persons (IT, data managers, M&E)
Time required: 3 – 4 hours
Preparation: Data lifecycle on one wall; user journey on another wall; empty space on other walls

Steps:

1. **10 minutes: Introductions and short exercise/icebreaker to get people thinking about data.**

2. **20 minutes: Thinking about our lawful basis for collecting data**

Background

The GDPR Guidance on Children's Data says:

– "You can use any of the lawful bases for processing set out in the GDPR when processing children's personal data. But for some bases there are additional things you need to think about when your data subject is a child.
– If you wish to rely upon consent as your lawful basis for processing, then you need to ensure that the child can understand what they are consenting to, otherwise the consent is not 'informed' and therefore invalid. There are also some additional rules for online consent.
– If you wish to rely upon 'performance of a contract' as your lawful basis for processing, then you must consider the child's competence to agree to the contract and to understand the implications of this processing.
– If you wish to rely upon legitimate interests as your lawful basis for processing you must balance your own (or a third party's) legitimate interests in processing the personal data against the interests and fundamental rights and freedoms of the child. This involves a judgment as to the nature and purpose of the processing and the potential risks it poses to children. It also requires you to take appropriate measures to safeguard against those risks."
– Background information here: https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf

Discuss

- If we consider our lawful basis to be "legitimate interest," then we must make a judgment call and weigh the risks to children of our collection of their data.

- If we decide to obtain consent, we must ensure that it is informed and traceable.

Decide

- What is the most appropriate basis for this particular data initiative?

3. **10 minutes: Review the data lifecycle...**

- The data cycle should be up on Wall 1

- Review the various steps and tasks included in each stage (Plan/Design, Collection, Analyze/Use, Transmit/Store, Share, Maintain/Retain/Destroy)
  (note – this is illustrative and the steps / order may shift or double back and repeat)

- Note that our discussion today will revolve around:
  - why we collect data
  - when/how often/from whom
  - tracing the data's journey through the lifecycle
  - understanding where we require consent or better privacy/security mechanisms
  - identifying where we need legal support to answer questions about our data and GDPR

4. 20 minutes: Why do we collect data?

- What are the "big questions" we want to answer? For example:
  - How should we tweak and improve the system?
  - What behavior change impact is the platform having on our users?
  - How can we encourage users to come back and continue using our site?

- What are the processes we run that require or generate user data to answer these questions?
  - Operational data collection and systems data (auto-generated)
  - M&E, polls, surveys, research efforts
  - Nudging or marketing
  - Anything else?

- On the wall, small groups from process owners/teams identify and organize the main buckets of data that we collect for each of these teams/processes; for example:
  - Operations/System: Phone number, time of call, location, duration of call, etc.
  - M&E: Name, age, gender, location, demographics, survey questions about a, b, c,

5. 1 hour: Our Data Collection: What data? Whose data? When?

- Wall 2 should have a representation of the user journey laid out

- Based on the data generating/data collection processes identified above, dig deeper into:

  - Whose data are we collecting? What data & what is the source of the data?

  - For each of the "big question" areas (e.g., operational/M&E/Marketing) above, small groups list on post-it notes the data that are collected and when.
  - Post these on Wall 2.
  - Align with the user journey to help to stimulate thinking/recollection of which data are collected at what points of the user journey
  - Note which data is "auto-collection" by the system vs which is requested directly from the user
  - Note whether it contains personal or sensitive data (such as that below) and flag if so:
    - Personal data
    - Financial data
    - Children's data
    - Images/voice recordings
    - Due diligence / authentication data (ID number, KYC data)
    - IP address or mobile phone number
    - Criminal convictions / offences
    - Biometric data
    - Education and training or employment details
    - Other sensitive information (based on context or vulnerability)
    - "Special category of data:" racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life)

  - When? Discuss - at which point along the user journey do we collect data? How often?

– Do we need to get consent? If so, have we obtained adult consent for children under the age of 16? How do we evidence that consent has been given? (child/guardian). If that is extremely difficult, then….
– If we're not getting consent, are we abiding by the Legitimate Interest framework? If so, we need to ensure that we have the necessary data privacy and security in place and to conduct a Privacy Impact Assessment or a Risks-Benefits analysis to document that we are protecting children's / users' data.
– Are we abiding by local legal frameworks?

6. 1 hour: Where and how does it flow? - Data Lifecycle Mapping

- For each of the "big questions" or processes (operations/systems, monitoring/evaluation, marketing/nudging), take a look at the data lifecycle again…. (Plan/Design, Collection, Analyze/Use, Transmit/Store, Share, Maintain/Retain/Destroy)

- We talked a lot about collection, now we'll talk about the rest – the data flows

- As a group, on Wall 3, map the data from the user's phone to wherever it goes…. Discuss these questions along the way:
  - Where does it go first? Second? How is it transmitted?
  - Where do we store it?
  - Who do we share it with?
  - How do we use it?
  - Maintaining/Retaining/Destroying - For how long do we keep it? Raw? Aggregated?
  - To whom may it be disclosed and why?
  - Who can access it?
  - How long will we retain it?
  - Who manages the security and access for these processes?

- Also consider…. (we may not have answers to these questions, but we need to find out)
  - If manual, where is it collected and where/how is it stored?
  - If electronic, note: is it collected and/or stored on or shared via:
    - Organizationally managed laptops/computers/phones?
    - Bring your own device / remote working?
    - Organizationally managed system(s)?
    - Third-party managed system(s)?
    - Internally hosted? Jurisdiction?
    - Externally hosted? Jurisdiction?
    - Cloud service? Jurisdiction?
    - How interoperable is it with other data we're collecting or with the wider sector?
    - Will it be opened or shared? What needs to happen in order to share/open it?
    - How will the format change over time? (raw -> aggregated, etc.)
    - Do we have a consent process in place that matches and can we prove it?
    - Or if not, have we conducted a privacy impact assessment or risks-benefits-harms analysis?
    - What other local laws govern this process? (Child or consumer protection?)
    - Do we have justification for our retention or destruction time frames?

This information can help teams to understand the gaps and where data privacy and security needs to be improved, and where consent or privacy impact assessments are needed to comply with the GDPR.

7. 30 minutes: Next steps: Work on an action plan with the team to fill in missing information and address the various gaps.

Sample risk assessment form

RISK ASSESSMENT FORM FOR ONLINE/OFFLINE ACTIVITIES (1/2)

Safeguarding Goals:
- Promote a safe and trusted environment;
- Prevent exposure to risk or harm;
- Protect children and young people who experience or report abuse.

Project Name:

Activity or area of work	**Area/ type of risk**	**Describe the Risk** Consider various elements for the organization, for participating girls (or children or youth) and/or partner organizations. These might include risks related to content we share, contacts we enable, privacy risks, reputation/PR, financial/economic, legal/political, other)	**Risk to whom** (Girl Effect, Girls, Partners)	**Severity of consequences** (if this happens) (1=low- 2=medium- 3= high)
Main activity 1	**Content:** (What is the risk of harmful or inappropriate content being shared or accessed?)			1
	Contact: (What are the contact risks to consider? e.g, contact with staff, partners, strangers, other girls (or other children or youth), or potential physical risk in participating or traveling to an event or activity)?			3
	Privacy: (Are there any risks related to data, media/use of photos or stories, or other types of privacy?			3
	Reputation: (What potential reputation risk might girls, children and/or youth face by participating? What are the reputation risks that the organization might face? What about partner organizations?)			
	Financial/Economic: (Does participation put any type of financial burden on girls/children or youth or require their families to provide financial resources? Does this place children and youth or the organization or partners in any type of risk? Is there a risk that girls / children or youth people would place themselves at risk in order to come up with funds to participate? Or that they receive some type of financial benefit that creates conflict in the family or community?)			
	Legal / Political: (What is the environment in which we are working? Does the activity create any potential legal or political risks to girls/children/youth, the organization, or its partners?)			
	Other: What contextual risks are there in a particular country that the team should be aware of and mitigate?			
Main activity 2	**[...]**			

RISK ASSESSMENT FORM FOR ONLINE/OFFLINE ACTIVITIES (2/2)

Safeguarding Goals:
- Promote a safe and trusted environment;
- Prevent exposure to risk or harm;
- Protect children and young people who experience or report abuse.

Project Name:

Likelihood of it happening? (1=low- 2=medium- 3= high)	**Risk ranking** (1=low; between 1 and 2=medium; over 2=high	**What are your migitation strategies?**	**Risk level after mitigation?** (1= low, 2=medium, 3=high) - if it's still high, the activity should be halted until risk can be brought down to an acceptable level)	**Next steps to take: What steps need to be taken to bring risk down to acceptable levels or to ensure that risk does not increase?**	**Who is responsible? By when?**
1	1	We will xxxx in order to xxxx	1		
1	2	We will xxxx in order to xxxx	2		
1	2	We cannot reduce this risk because...			