idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

Resource Booklet

Data Protection for Children

7-10 years

Foreword

Dear Educators,

It is my pleasure to welcome you to this Resource Booklet, prepared to accompany the educational video and to support you in understanding key data protection terminology. This material is intended to prepare you with the necessary tools to stimulate meaningful classroom discussions and to confidently guide conversations on data protection.

The central message of this awareness campaign is the importance of protecting one's personal data, particularly among younger generations. While the campaign was developed to mark European Data Protection Day, it should be regarded as a living initiative, aimed at raising continuous awareness of the risks and potential harms that the online environment may present to children.

Although children of a young age should ideally not be in possession of mobile devices, nor have access to social media platforms or applications that are not age-appropriate, we have taken a considered and informed decision to develop this educational video. This reflects the reality that many young children are already accessing the internet and are therefore exposed to online risks.

Children deserve and merit special protection. This material represents the first in a series of resources that we plan to roll out over the coming months and years, with the objective of placing children at the centre of our awareness and educational strategies.

Educators are among the key pillars supporting children during their formative years. We recognise and deeply appreciate the dedication, commitment, and daily effort you invest in preparing our future generations for the world they will soon face.

Thank you for your invaluable work, and do keep up your excellent efforts.

Ian Deguara

Information and Data Protection Commissioner

Educator's Guide

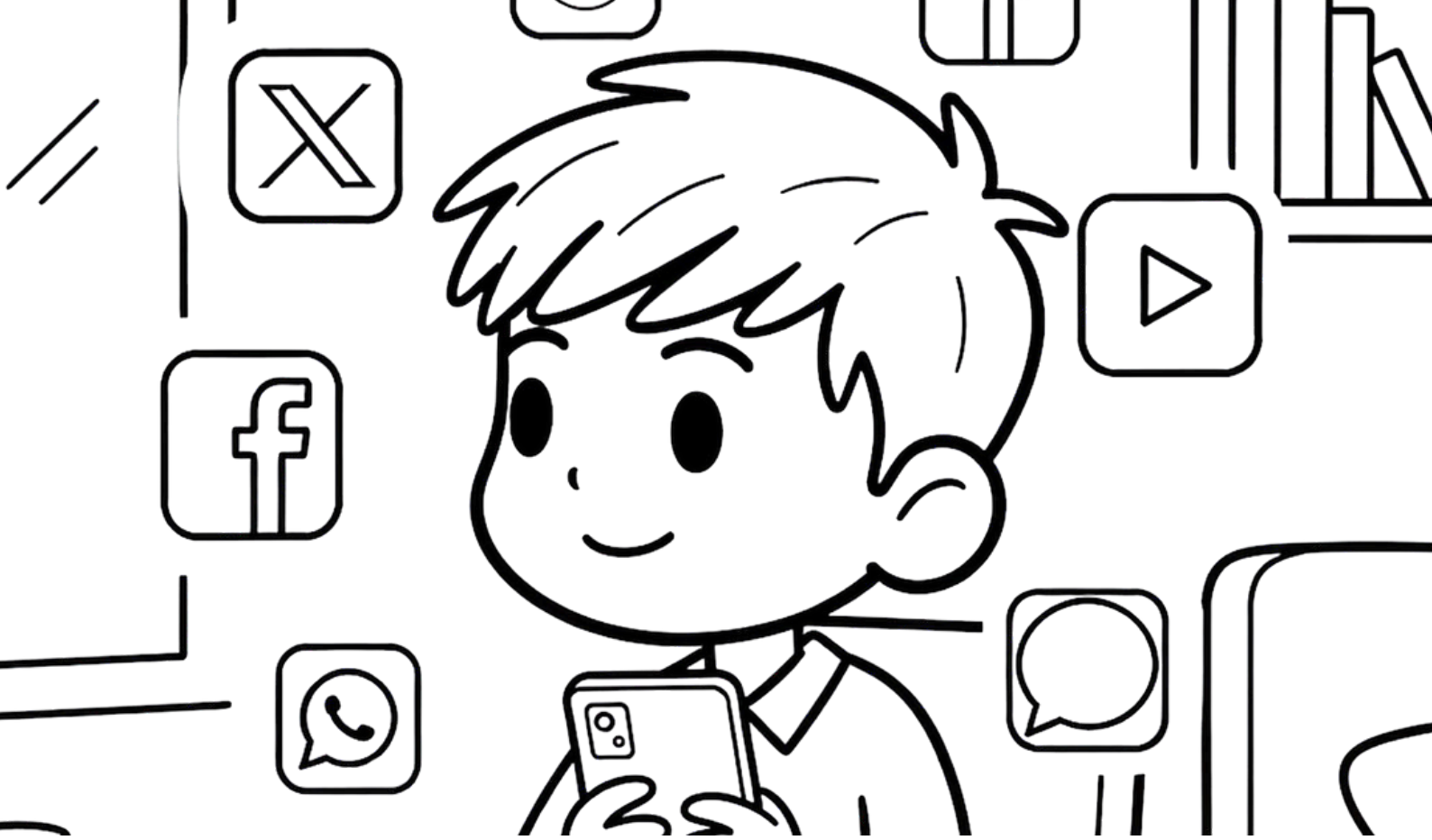
idpc
INFORMATION AND DATA PROTECTION COMMISSIONER

This section equips educators with the knowledge they need before introducing the topic of data protection to students. It breaks down the key concepts of the General Data Protection Regulation and the Data Protection Act into simple, practical explanations that connect directly to the scenarios shown in the campaign video. The aim is to build educators' confidence so they can guide classroom discussions, answer students' questions and reinforce safe, informed online behaviour.

idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

01 Understanding Data Protection



1.1 What do we mean by Data Protection?

Data protection is a fundamental human right that ensures every person (including children) can control their personal information. It is about keeping personal data safe and ensuring that it is used responsibly, fairly and only for legitimate purposes. For children, data protection is especially important because they may not recognise the risks of sharing data online, such as manipulation, tracking, bullying or unwanted exposure.

Under the EU's General Data Protection Regulation (GDPR) and Malta's Data Protection Act (Chapter 586 of the Laws of Malta), organisations must handle children's data with extra care. These rules exist to protect young people from misuse of their information, whether in school settings, apps, games, websites or social media. Data protection empowers children to make informed choices and helps adults support them in understanding what happens to their data.

1.2 What is Personal Data?

Personal data is any information that identifies a person, either directly or indirectly. For children, this can include:

- **Name, age, gender**
- **Photos, selfies or videos**
- **Home address or school name**
- **Location data**
- **Email addresses, usernames or account IDs**
- **Hobbies, interests, habits or online behaviour**

Sometimes a single piece of information is enough to identify someone and other times small pieces come together to create a clear picture of who a child is.

Understanding the value of personal data helps educators explain why companies, apps and websites often ask children for information. Data shapes the content children see online, such as targeted advertisements or personalised suggestions.

Personal data shared online is difficult to control and personal data like photos can be copied, forwarded, saved or even edited using AI tools. When children understand this, they are more likely to think before sharing!

1.3 What is Processing?

Processing refers to any action performed on personal data. This includes collecting, storing, analysing, sharing, deleting, tracking or posting data online. Every time a child uses an app, website or digital device, their personal data is being processed in some way.

Understanding processing helps educators explain that personal data does not simply *'sit'* somewhere, but rather it is constantly moving, being used and often shared.

1.4 What is General Data Protection Regulation?

The General Data Protection Regulation (GDPR) is the main EU law that sets rules on how personal data must be handled. It requires organisations to be transparent, responsible and secure when using personal information. Before the GDPR, children were not mentioned specifically in European data protection laws. The GDPR changed this by recognising that children need special protection because they may be less aware of the consequences of sharing their data. It also grants both adults and children strong rights that help them understand and control how their personal data is used.

The GDPR applies to everything from school systems and educational platforms to apps, games and websites used by children. The Maltese Data Protection Act (Chapter 586 of the Laws of Malta) aligns national law with the GDPR and sets out the powers of the Information and Data Protection Commissioner (IDPC).

1.5 Key Data Protection Rights under the GDPR

The GDPR grants important data protection rights to all individuals, including children and these rights apply equally in both online and offline situations. For educators, understanding these core rights helps them confidently address students' questions and guide them through everyday scenarios similar to those shown in the campaign video. In this section, we focus on five key rights that are most relevant to children: the right to be informed, the right of access, the right to rectification, the right to erasure and the right to object. Each of these rights is explained below, along with practical examples that show how they support children in taking control of their personal information.

1.5.1 The Right to be Informed

The right to be informed ensures that individuals understand how their personal data is collected, used, stored and shared. Organisations must explain this clearly and in simple language, especially when the information relates to children. This right exists so children are not left guessing about what an app, website, service provider or digital platform does with their data. It also helps them understand whether sharing their information is necessary or optional and what the consequences might be.

Examples

- Before an app accesses a camera or microphone, it must explain why it needs this data.
- An app tells children whether their location will be tracked, how often and for what purpose.

This right helps children pause and ask: *"Do I understand what I'm sharing?"*

1.5.2 The Right of Access

Children and their parents have the right to see what personal data an organisation holds about them and to request a copy. For children, it supports transparency, helping them see what digital footprint they have created and how companies or platforms might be using it.

Examples

- A child wants to know what information a gaming platform has on their account (game history, messages, purchases, profile data).
- If a child was involved in an incident in a playground covered by cameras, they (or their parent) may request a copy of footage showing them.

This right helps children pause and ask: *"What information is being kept about me?"*

1.5.3 The Right to Rectification

The right to rectification ensures that personal data must be correct and up to date. If information is inaccurate or incomplete, individuals can ask for it to be changed. For children, this right is crucial because incorrect information (such as a wrong age, outdated contact details or an inaccurate profile) can affect the ads they see or the content recommended to them.

Examples

- A child notices a mistake in their date of birth on an online account and requests that it be corrected.
- A medical form contains outdated allergy information and needs updating.

This right helps children pause and ask: *"Is the information about me correct or should something be updated?"*

1.5.4 The Right to Erasure

The right to erasure allows individuals to request the deletion of their personal data when it is no longer needed, when they withdraw consent, or when the data has been used unfairly. This right is especially meaningful for children, who may share information without understanding the long-term consequences. It helps ensure that information does not stay online forever and that children can regain control over data they regret sharing.

Examples

- A child wants photos removed from a website.
- A child asks a website to remove a profile created when they were younger.

This right helps children pause and ask: *"Is this information still needed or should I ask for it to be deleted?"*

1.5.5 The Right to Object

The right to object allows individuals to say "*no*" to certain uses of their personal data. When someone objects, the organisation must stop using the data unless it has a very strong and legitimate reason to continue. For children, this right is key because it allows them to challenge unwanted profiling, targeted advertising, or unnecessary data collection that makes them uncomfortable or puts them at risk.

Examples

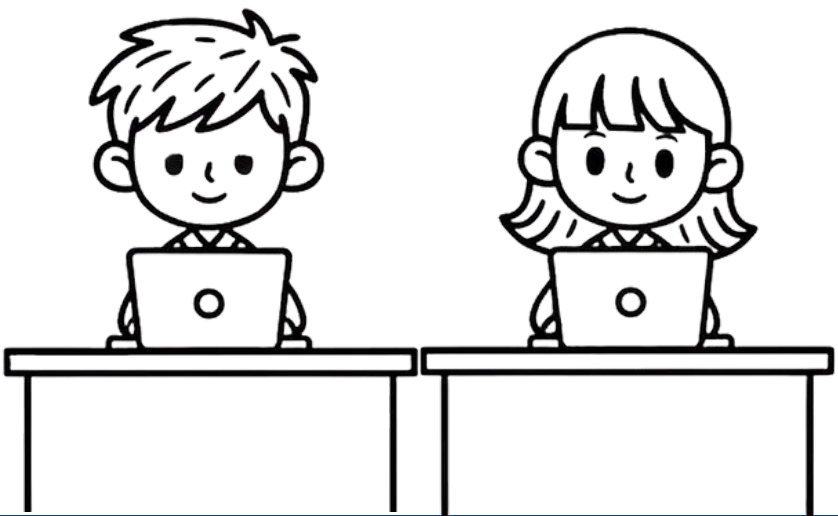
- A child objects to their data being used for personalised advertising.
- A youth tells an app they do not want their activity tracked for behavioural analysis.

This right helps children pause and ask: *"Do I feel comfortable with how my data is being used or should I say no?"*

1.6 What Is the role of the Information and Data Protection Commissioner?

The Information and Data Protection Commissioner (IDPC) is Malta's independent authority responsible for ensuring that data protection laws are respected and applied correctly. The Commissioner works to protect individuals' rights by promoting awareness and understanding of data protection, including the risks, rules and safeguards that apply whenever personal data is processed. This educational role is particularly important for children, who may not always recognise how their information is collected or used.

The IDPC also investigates complaints from individuals who believe their data protection rights have been breached and it has the power to require organisations to change their practices or take corrective measures when they fail to comply with the law. Considering that many digital services operate across borders, the IDPC collaborates with other European data protection authorities to ensure that people, including minors, receive consistent protection regardless of where the organisation processing their data is based. Through these responsibilities, the IDPC helps create a safer and more accountable environment for the handling of personal data in Malta.



Step-by-Step Teaching Plan

idpc
INFORMATION AND DATA PROTECTION COMMISSIONER

This section equips educators with practical tools to confidently deliver data protection lessons using the campaign video as the starting point. The plan mirrors the flow of the earlier educator-preparation material, ensuring educators can link concepts smoothly from explanation to practice.

This teaching plan translates the key data protection concepts into classroom-ready steps. It ensures educators feel prepared and confident when guiding students through discussions about personal data, online behaviour and their rights under the GDPR.

By following the plan, educators will:

- introduce data protection in a simple and relatable way;
- connect learning to the video's scenarios;
- build students' understanding step by step; and
- reinforce safe and responsible behaviour online and offline.

idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

02

What is Personal Data?

Lesson 1

Learning Outcomes

By the end of this lesson, students will be able to:

- Explain what personal data means using their own words.
- Identify personal data shown in the campaign video (selfie, age, location, hobbies, password).
- Understand why personal information is valuable and why it needs protection.
- Make safer decisions about what they choose to share online

Teaching Notes

This lesson is designed to support you as an educator and to make your delivery as smooth and comfortable as possible. The entire lesson is fully centred on the campaign video, so there is no need to divide it into parts. Simply allow students to enjoy the story first and trust that the discussion and activities that follow will naturally guide them to the key learning points.

The key idea to communicate is that personal information has value and deserves protection.

Lesson Plan 1

01 Watch the Full Campaign Video

Play the entire video from start to finish without stopping.

02 First Reactions Discussion

Ask open questions:

- *"What was the video about?"*
- *"What happened to Gianni?"*
- *"Did anything surprise you?"*

03 Guided Discussion: What Information Was Shared?

Replay key moments briefly if needed, then ask:

- *"What did Gianni almost share at the start?"* (Selfie)
- *"What did the quiz ask him?"* (Age, hobbies, town)
- *"What did the app track?"* (Location)
- *"What did his friend ask for?"* (Password)

Write answers on the board. Explain that all of these are personal data because they tell others something about a real person.

04 Educator Explanation: What Is Personal Data?

Explain clearly:
Personal data is any information that can identify a person or tell us something about who they are, where they are or what they do.

Link directly to the video:

- A photo is personal data.
- A password is personal data.
- A location on a map is personal data.
- Certain answers in a quiz are personal data.

Explain why it is valuable:
Personal data can be used to contact you, track you, advertise to you or pretend to be you. That is why it must be protected!

05 *'Where Does My Data Belong?'*

This activity helps students clearly understand what counts as personal data, what does not and where personal data is commonly used: Me, School and Gaming Apps or Websites. The activity is fully linked to the situations shown in the video.

Classroom Setup:
On the whiteboard, draw four large boxes and label them clearly:

- ME (information about me as a person)
- SCHOOL
- GAMING APPS or WEBSITES
- NOT PERSONAL DATA

06 How to Run the Activity

A Explain the Rules Clearly

Tell students they will see many different words. Their job is to decide:

- Is it personal data or not?
- If it is personal data, where is it mostly used: Me, School, or Gaming/Websites?

B Start with Guided Practice

Begin with 2–3 example words together as a class and talk through the thinking out loud so students understand how to decide.

Then, students will choose one word, say out loud where they think it belongs and place it under the correct box on the board.

After each word is placed, ask:

- *"Do we all agree?"*
- *"Why does it belong there?" (Encourage them to think about multiple categories: e.g., "my age" may go to school, apps and websites)*

As words appear, link them to Gianni:

- Photo → selfie scene
- Password → gaming scene
- Location → map scene
- Age, town, hobbies → quiz scene

C Final Reflection as a Group

Once all words are placed, ask:

- *"Which box has the most words?"*
- *"Which type of personal data do children share most?"*
- *"Which of these caused problems for Gianni?"*

End with this clear message:
Just because information seems normal to share, that does not mean it is safe to share everywhere.

ME
(Personal Data About Me)

- Full Name
- Date of Birth
- Nationality
- Email Address
- Home Address
- Contact Number
- Guardian's Full Name
- Selfie
- Health Condition
- Fingerprint
- Voice Recording

SCHOOL
(Personal Data Used at School)

- Full Name
- Date of Birth
- Nationality
- Email Address
- School Email Address
- Parent Contact Information
- Student ID Number
- Class Photo
- Allergies
- Behavioural records
- Academic records

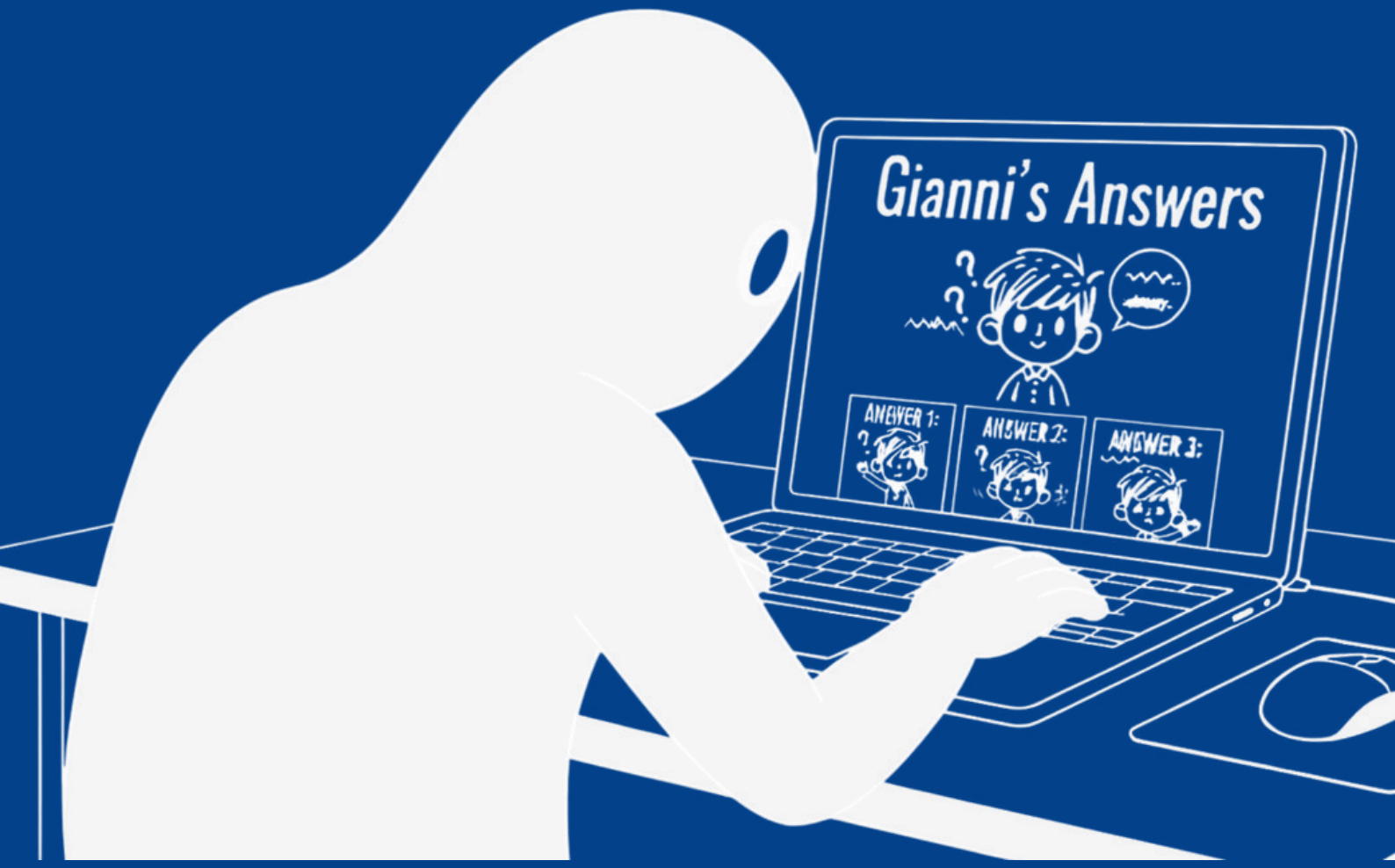
GAMING APPS / WEBSITES
(Personal Data Used Online)

- Full Name
- Date of Birth
- Nationality
- Email Address
- Log in Credentials
- Phone Number
- Password
- Profile Picture
- Payment information
- Precise Location Data

NOT PERSONAL DATA *(General Information)*

- Backpack colours
- Type of shoes I wear
- My pet's species
- Colour of my backpack
- School Logo
- Number of students in class
- School uniform colours
- Opening hours
- Game Level Reached
- Game Difficulty
- In-Game Points

idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER



03

Who Can See My Photo?

Lesson 2

This activity helps students understand that different people can see what we post online, even when we do not expect it. It connects directly to Gianni's selfie scene and shows students that once something is shared, it may reach intended, unwanted and even completely unknown audiences. The activity also introduces the idea that some audience control is possible through privacy settings and smart choices, but not all sharing can ever be fully controlled.

idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

Learning Outcomes

By the end of this lesson, students will be able to:

- Explain how digital content spreads rapidly and permanently online
- Articulate why it is important to pause and reflect before sharing photos or messages
- Apply the 'think before you share' principle to real-world situations
- Understand the difference between intended, unwanted and unknown audiences.
- Learn that once something is shared online, it may reach many more people than planned.
- Recognise that audience control is possible, but never perfect.

Teaching Notes

Emphasise that students should relate the activity to Gianni's experience in the video. You may wish to gently remind students that:

- Wanting to share things online is normal.
- Problems usually happen not because of bad intentions, but because information travels further than expected.

The goal is not to stop sharing completely, but to share more wisely and safely.

Lesson Plan 2

01 Reconnect to the Campaign Video

Remind students of the opening scene where Gianni takes a selfie and is about to send it. Ask:

- *"Who do you think will see this photo?"*
- *"Who do you think Gianni wanted to see the photo?"*
- *"What might happen once it is sent?"*
- *"Who do you think actually ended up seeing it?"*

02 Social Media Apps & Age Awareness

Before introducing the audience boxes, help students recognise where sharing usually happens. Show printed logos of well-known apps commonly associated with sharing, messaging and gaming. For example: WhatsApp, TikTok, YouTube, Instagram, Snapchat, Roblox, Facebook etc.

Ask students gently:

- *"Do you recognise any of these?"*
- *"What do people usually do on these apps?"* (chat, post photos, watch videos, play games)
- *"Do you think these apps are made for children or for adults too?"*

Then introduce the idea of age limits:

- Explain that many apps have an age requirement, often 13+, because sharing personal data online can carry risks.
- Emphasise that these rules exist to protect children, not to punish them.

You may say:

- *"Some apps ask users to be a certain age because sharing information online can sometimes be risky. These rules help protect children while they grow and learn".*
- *"No matter which app we use, once we post something, it can move between different groups of people. Now we are going to look at who those people might be".*

03 How Social Media Apps Share Posts

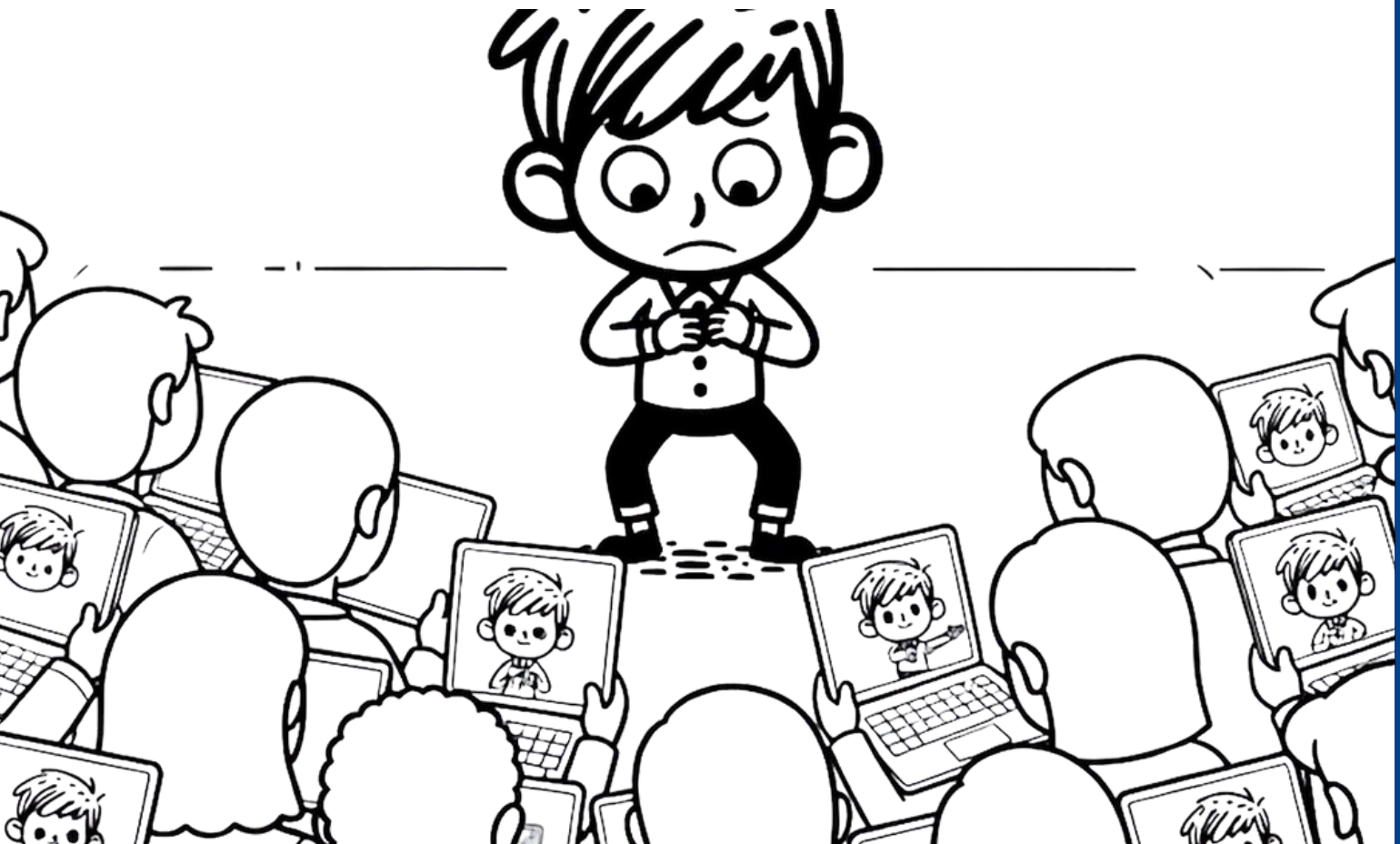
When we post a photo, video, or message on an app, such app shows that post to other people depending on the settings (friends, groups, or the public). Once something is shared, other people can copy it, screenshot it, or share it again.

04 Class Demonstration

Draw a stick figure for Gianni in the centre and three friends around him. Explain that Gianni sends the photo to three friends and each friend shares it with three more people. Continue to show the exponential spread visually. Ask:

- *"Can Gianni still control who sees it?"*
- *"What could happen if someone he doesn't know sees it?"*

"This is how quickly sharing can grow — even when we only send something to one or two people".



05 Draw the Three Audience Boxes

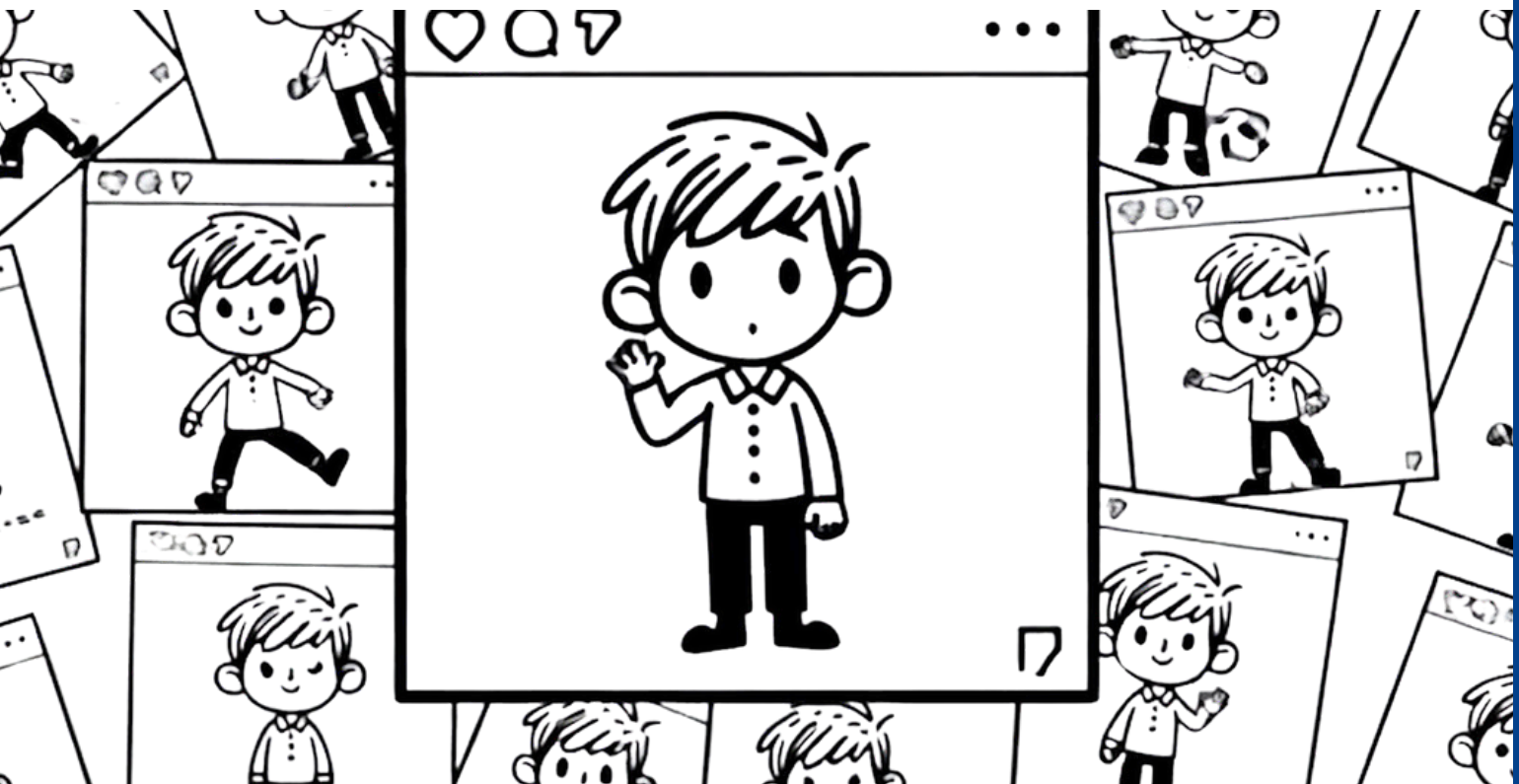
On the whiteboard, draw three large boxes and label them clearly:

INTENDED AUDIENCE	UNWANTED AUDIENCE	UNKNOWNAUDIENCE
The people you want to see your post	People you did not want, but who end up seeing it	The people you want to see your post

Explain each box slowly and clearly using simple examples:

INTENDED AUDIENCE	UNWANTED AUDIENCE	UNKNOWNAUDIENCE
parents, family members, close friends	classmates you don't get along with, bullies, school staff	strangers, fake accounts, people in other countries

Explain that Gianni's photo moved through all three boxes.



06 Main Sorting Activity: "Who Could See This?"

Read out the following sharing situations one at a time. After each one, students decide together: *Which box does this audience belong in?*

You write the example under the box they choose.

Example situations:

INTENDED AUDIENCE	• You post a TikTok about studying tips for your classmates • You share a family photo on Facebook for your relatives and close friends • You send a funny Snapchat filter photo to your best friends only. • Sending a video of a school play to your grandparents.
UNWANTED AUDIENCE	• A classmate you don't like sees your Instagram story because a friend reposted it • Strangers see your Facebook post because a friend shared it without you knowing) • You share your Minecraft username publicly and someone from school you don't like finds you online. • Educator sees your Snapchat where you complained about homework.
	• Random TikTok users around the world watch your video on the *"For You Page"*. • You post a public Snapchat story and people you don't know watch it. • Someone seeing your Snap after your friend accidentally shares it outside your group. • People on the internet seeing a TikTok you posted with a trending hashtag.

07 Controlling Your Audience

Explain that sometimes we can choose who sees our posts, but once someone else shares it, that control becomes weaker.

Discuss simple control tools:

- Private (only people you approve can see your posts, so it is safer because strangers can't see your content) vs public accounts (anyone can see what you post, so it is considered to be riskier because anyone, including unknown people, can view, comment or share your content)
- Not accepting strangers (avoid adding strangers and remember that some strangers may pretend to be someone you know.
- Think before you share and ask yourself:
  - Who is my intended audience?
  - Could anyone unwanted see this?
  - Could strangers or unknown people see it?

Ask students to finish this sentence:
"Before I send something online, I should think about _____".

Reinforce the key message: ***Once something is shared, it can reach far beyond who we planned. Choosing the right audience is part of protecting our personal data.***

idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

04

Your Digital Keys

Lesson 3

Learning Outcomes

By the end of this lesson, students will be able to:

- Explain why passwords must remain private using the house key analogy.
- Describe at least three risks of sharing passwords, even with trusted friends.
- Understand that passwords should only be shared with parents or guardians, when necessary.
- Recognise the difference between weak and strong passwords.
- Apply basic rules for creating secure passwords.
- Identify common password-related tricks and unsafe requests.

Teaching Notes

This lesson uses a strong real-life comparison *(house key = password)* to help children understand digital safety in a concrete way. Wanting to share things online is normal. Some students may already have shared a password or may share devices with family members. It is important to:

- Focus on learning safer habits going forward
- Emphasise that password rules are about protection, not mistrust

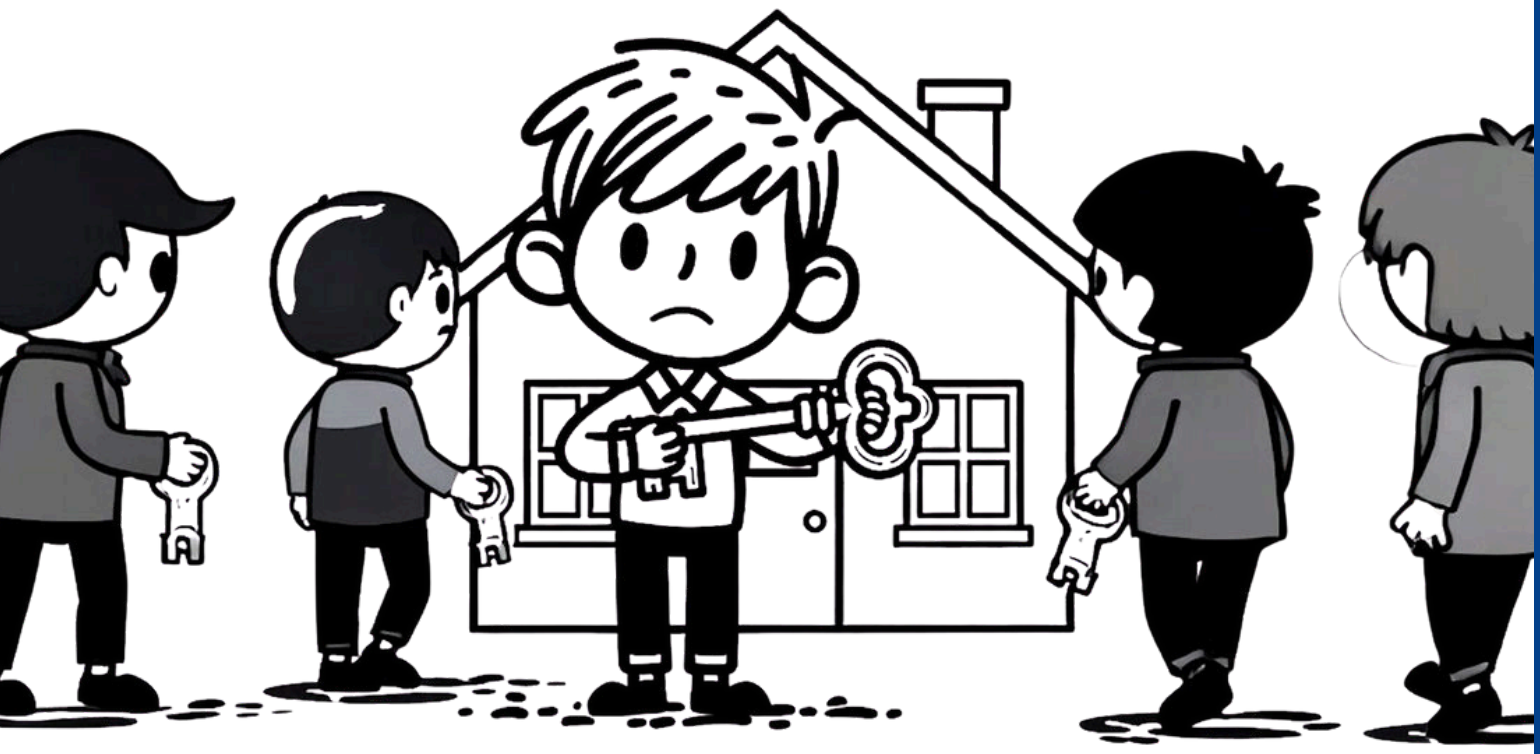
Lesson Plan 3

01 The House Key Analogy

Begin the lesson by showing the students a real key or a large drawing of a key on the board. Explain that this key opens a house door and ask the class who they think should be allowed to have a copy of such a key. As students respond, write their answers on the board and gently guide the discussion by asking why certain people should or should not be trusted with the key.

Typical responses might include:

- Parents/guardians (YES)
- Brothers/sisters (MAYBE)
- Best friend (MAYBE/Risky)
- Someone you just met (NO)
- Put a photo of it online (DEFINITELY NOT)



For each response, ask *'why'* or *'why not?'*,
to encourage students to think about the
risks involved if the key was lost or copied by the wrong person.

- **Parents/guardians:** Trusted, responsible, live with you
- **Best friend:** Might be trustworthy BUT could accidentally lose it, someone else might find it, creates risk
- **Stranger:** Dangerous as they could rob your house
- **Online:** Anyone could see it and make a copy

Once the discussion is established, guide the students toward the connection between a house key and a password. Draw a clear comparison chart on the board and explain that:

HOUSE KEY	PASSWORD
Opens your front door	Opens your accounts
Protects your home	Protects your games, messages, photos, personal information
If stolen, strangers can get in	If shared, others can access your personal information
You wouldn't give it to just anyone	You shouldn't share it with anyone

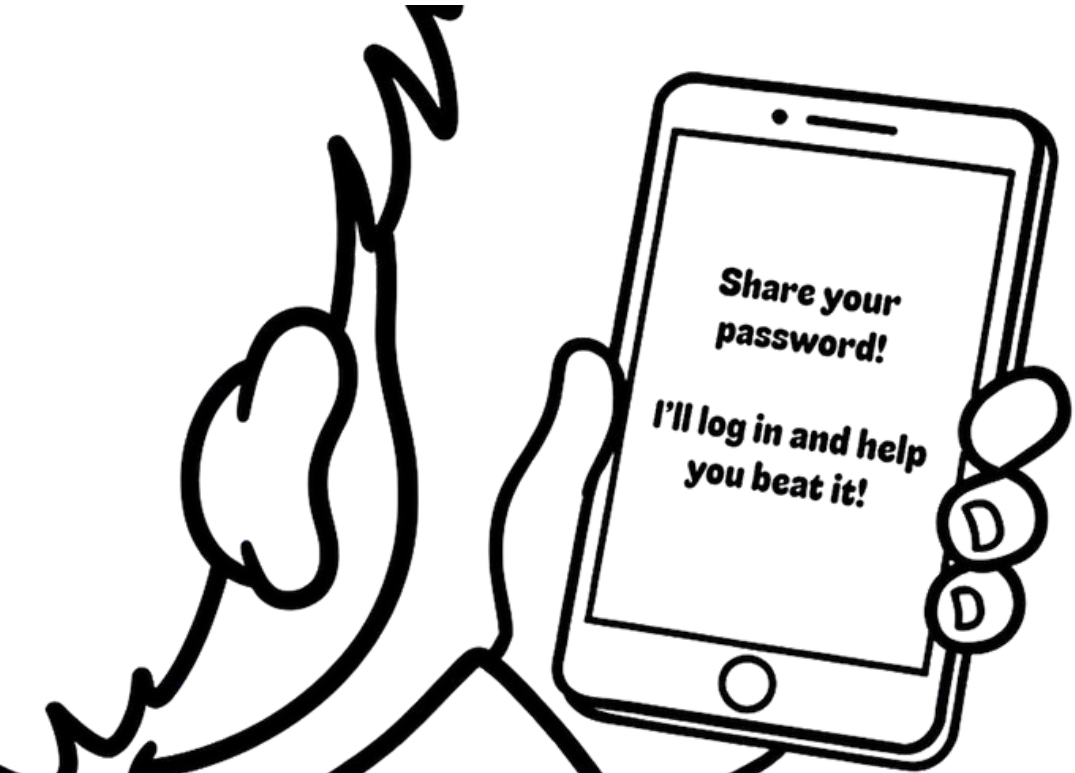
You may say:
"Passwords are digital keys. They protect your accounts just like house keys protect your home. Let's think about what could happen if Gianni had shared that password with his friend in the video".

02 Reconnect to the Campaign Video

- *"What could his friend accidentally do with Gianni's password?"* (Change settings, see private messages, accidentally share it, change password)
- *"What if someone else saw the password on Gianni's device?"* (They could access Gianni's account too)
- *"Even though he is Gianni's friend and would never do anything bad on purpose, could something still go wrong?"* (Yes - accidents happen, devices can get lost or you may not remain friends)

03 Golden Safety Rule

- NEVER SHARE PASSWORDS, NOT EVEN WITH FRIENDS YOU TRUST
- Explain that this rule is not because we don't trust our friends. It is because we cannot control what happens after.



04 Rules for Creating Strong Passwords

Sometimes people use passwords that are really easy to guess, because they are easy to remember. Ask the children to come up with examples of what these might be.

For example: 1234567, birthdays, the word *'password',* pet names or family names.

Point out that we describe these as weak passwords.

Today we have been learning about why Super Strong Passwords are important. Have you used any of these passwords before?

password	**123456**
too simple	too simple
Gianni2812	**ilovepizza**
has personal information (name and birthday)	needs numbers, symbols and some capital letters

These are weak passwords. Strong Passwords are important. You don't want someone else to work it out! Here are some rules that we can use to create a Super Strong Password:

Think of a phrase that is easy to remember.

my cat is called Garfield

Using the phrase, write down the first letter of each word.

mcicg

Capitalise some of them

McIcG

Add one or two numbers and symbols that you will remember

1McIcG

Learn it!

idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

05

Does This App Really Need It?

Lesson 4

Learning Outcomes

By the end of this lesson, students will be able to:

- Explain why apps ask for personal information and permissions
- Identify which app permissions are necessary and which are not
- Understand that "*free*" apps often collect personal data as payment
- Recognise how personal data is used to create targeted advertisements
- Apply the *'pause and ask'* principle before granting app permissions

Teaching Notes

This lesson focuses on two key scenes from the video: the location tracking scene and the quiz scene. Both illustrate how apps collect personal data, often without children realising the consequences. The goal is to help students understand that every time they click "*allow*" or answer a question, they are sharing valuable information about themselves.

- Focus on learning safer habits going forward
- Emphasise that password rules are about protection, not mistrust

Lesson Plan 4

01 Reconnect to the Campaign Video

Remind students of two specific scenes:

- **The Location Map:** *"What happened when Gianni clicked 'allow' for location?", "What did the map show?", "Who do you think could see where Gianni was?"*
- **The Quiz:** *"What questions did the quiz ask Gianni?", "What happened after Gianni answered them?", "How did the app know what ads to show him?"*

02 Why Apps Want Your Data

Explain that apps are often described as *'free'* because you don't pay money to download them. But they're not really free, instead of money, you pay with your personal data!

Companies collect information about you so they can:

- Show you advertisements for things you might want to buy
- Sell your information to other companies
- Track your behaviour and habits
- Predict what you'll do next

Connect back to Gianni:

- The quiz collected his age, location and interests
- The app used this to show him specific ads for Minecraft toys, art supplies and games in his town

This is called *'targeted advertising'* and it happens because the app knows personal information about him!

03 Does This App Really Need It?

This activity helps students critically evaluate app permission requests and decide whether the information is truly necessary for the app to function.

Classroom Setup:
On the whiteboard, draw three columns:

APP TYPE

PERMISSION REQUESTED

DOES IT REALLY NEED IT?

A How to Run the Activity (Step-by-Step for Educators)

Explain the Task
Tell students they will look at different types of apps and the permissions these apps might ask for.

Their job is to decide: *Does this app really need this information to work properly?*

B Introduce the Apps

APP TYPE	PERMISSION REQUESTED	IMPORTANT QUESTIONS	DOES IT REALLY NEED IT?
Weather App	Your location	Does a weather app need to know where you are to show you the weather?	YES (It needs your location to show accurate local weather)
Snapchat	Access to your camera and microphone	Does Snapchat need your camera and microphone?	YES (Snapchat is designed for taking photos, videos and recording voice messages, so it needs camera and microphone access to work properly) BUT also discuss: *"Does Snapchat need to know your exact location all the time?"* Answer: NO (You can use Snapchat without sharing your location. The location feature is optional for filters and Snap Map, but the app works fine without it)

APP TYPE	PERMISSION REQUESTED	IMPORTANT QUESTIONS	DOES IT REALLY NEED IT?
Roblox	Access to your microphone	Does Roblox need your microphone?	MAYBE (If you want to use voice chat to talk to other players, yes. But you can play most Roblox games perfectly well using just text chat, so microphone access is optional) Important discussion point: *"Who might hear you if you turn on the microphone in Roblox?"* Answer: Other players, including people you don't know. That's why it's important to think carefully before turning on voice chat.

APP TYPE	PERMISSION REQUESTED	IMPORTANT QUESTIONS	DOES IT REALLY NEED IT?
Minecraft	Access to your microphone	Does Minecraft need your microphone?	MAYBE (If you're playing with friends and want to talk while playing on multiplayer servers with voice chat, yes. But most Minecraft gameplay doesn't require a microphone at all, you can build, explore and play without it) Additional question: *"What about Minecraft asking for your location?"* Answer: NO (Minecraft doesn't need to know where you are in the real world to let you play in the game world)
Flashlight App	Access to your contacts	Does a flashlight need to see your contacts to turn on the light?	NO (This is suspicious and unnecessary. A flashlight app should only need access to your phone's flashlight/torch feature)

APP TYPE	PERMISSION REQUESTED	IMPORTANT QUESTIONS	DOES IT REALLY NEED IT?
Navigation App	Your location	Does a map app need to know where you are?	YES (It needs your location to give you directions)
TikTok	Access to your camera, microphone and contacts	Does TikTok need these?	Camera and microphone: YES (To create videos) Contacts: NO (TikTok works fine without access to your contacts. This is used to suggest people you might know, but it's not necessary for the app to function)

C Special Focus Discussion: Microphones in Apps

After presenting the scenarios, have a specific discussion about microphones since this is mentioned in several popular apps children use.

Ask students:

- *"When you allow an app to use your microphone, what can it do?"*
- *"Who might be able to hear you?"*
- *"What could the app do with this data?"*
- *"Would you click 'allow' or 'deny'?"*
- *"Can you still use the app if you say 'no' to some permissions?"*

When you give an app permission to use your microphone, it can:

- Record your voice
- Listen to conversations (in some cases, even when you're not actively using the app)
- Share your voice recordings with other users
- Keep recordings of what you said

D Teach the '*Pause and Ask*' Rule

Before clicking '*allow*', always ask:

- Does this app really need this information to work?
- What could happen if I share this?
- Can I use the app without sharing this?

Important Reminder for Students:
Just because an app CAN ask for permission doesn't mean you HAVE to say yes. Many apps work perfectly well even if you say *'no'* to some permissions. You're in control!

idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

06

Your Data Protection Rights

Lesson 5

Learning Outcomes

By the end of this lesson, students will be able to:

- Explain what rights are and why they matter
- Understand that children have the same data protection rights as adults
- Apply these rights to real situations similar to those in the video
- Know how to ask for help when their rights are not respected
- Recognise that data protection rights exist to keep them safe and in control

Teaching Notes

This lesson introduces the concept of rights in a way that is accessible and empowering for children. Rather than overwhelming students with legal terminology, the focus is on helping them understand that they have control over their personal information and that laws exist to protect them.

The lesson connects directly to all the scenarios in the video, showing students how their rights apply in real situations they can relate to.

Lesson Plan 5

01 Introduction: What Are Rights?

Begin with a discussion about rights in general before introducing data protection rights specifically.

Start with the question: Has anyone heard the word *'rights'* before? What do you think it means?

Simple Explanation: Rights are special protections that belong to every person. They help make sure we're treated fairly and kept safe. Just like you have the right to go to school, the right to play and the right to be treated with kindness, you also have rights about your personal information.

Examples of Everyday Rights Children Understand:

- The right to be listened to
- The right to feel safe
- The right to education

Explain: *Today we're going to learn about five special rights that protect your personal data, both online and in the real world. These rights belong to you, just like they belong to adults. This means that even though you're children, the law protects you in exactly the same way.*

02 Reconnect to the Campaign Video

Briefly remind students of each situation Gianni faced:

- The selfie that could spread everywhere
- The password his friend wanted
- The app tracking his location
- The quiz collecting his information

Ask: *"In each of these situations, did Gianni have any control? Could he do anything to protect himself?"*

Explain: *The answer is **YES**. Gianni has rights that help him control his personal data. Let's learn what they are. These are actual laws that protect you!*

03 The Five Rights Every Child Has

Introduce each right one at a time by creating a large chart on the board with these columns:

Right to be Informed

What it means

You have the right to know how your personal data is being used. Apps, websites and companies must explain clearly what they will do with your information. They can't keep it a secret!

Real-World Examples

- Before an app uses your camera, it should tell you why
- Before a quiz collects your age and location, it should explain what it will do with that information
- Before a game track your location, it should say who can see it
- Before Snapchat uses your microphone, it should explain that other people will hear your voice messages
- Before Roblox asks for voice chat, it should tell you that other players (including strangers) might hear you

Connect to Gianni

- The quiz should have told Gianni that his answers would be used to show him targeted ads for toys and games
- When Gianni clicked *'allow'* the app should have explained in simple words what would happen next

What Gianni could do

- Read the app's explanation before clicking *'allow'*
- If he doesn't understand, ask a parent or educator
- Choose not to use apps that don't explain clearly

PAUSE AND THINK QUESTION

"Do I understand what this app or website will do with my information?"

Apps must explain what they do with your data in a way you can understand.

Right of Access

What it means

You have the right to see what information a company or app has collected about you. You can ask: *"What do you know about me?"* and they must show you!

Real-World Examples

- You can ask a gaming platform like Roblox or Minecraft to show you what information is saved in your account
- You can ask a website what data they've collected about you
- Your parents can help you request this information if the app makes it difficult

Connect to Gianni

- Gianni could ask: *"What information did you collect about me?"*

What Gianni could do

- Write to the company (with a parent's help) and ask for a copy of his data
- Check his account settings to see what information is stored

PAUSE AND THINK QUESTION

"What information is being kept about me?"

You can ask to see what data apps and websites have about you.

Right to Rectification

What it means

You have the right to fix information about you if it's wrong. If an app or website has incorrect information, you can ask them to change it. They must fix it!

Real-World Examples

- If a website shows the wrong age for you, you can ask them to correct it (this matters because wrong ages can mean you see wrong content or ads)
- If your name is spelled wrong in an app, you have the right to fix it
- If an online profile has outdated information, you can update it

Connect to Gianni

- If the gaming app had the wrong date of birth for Gianni, he could request it be updated
- Wrong information can lead to wrong advertisements or wrong content being shown

What Gianni could do

- Go into his account settings and update wrong information
- Contact the app or website (with help from a parent) to fix errors
- Check regularly that his information is still correct

PAUSE AND THINK QUESTION

"Is the information about me correct or should something be updated?"

If information about you is wrong, you can ask for it to be fixed.

Right to Erasure

What it means

You have the right to ask for your personal data to be deleted. If you don't want a company to keep your information anymore, you can ask them to erase it. This is sometimes called 'the right to be forgotten'.

Real-World Examples

- You can ask an app to delete your account and all your data
- You can ask Roblox, Minecraft or Snapchat to delete your profile and everything they know about you

Connect to Gianni

- Gianni could ask the gaming app to delete his gaming account
- Gianni could request that the location app erase his tracking history
- Gianni could ask the quiz app to delete all the answers he gave

What Gianni could do

- Delete his account if he stops using an app
- Contact the company and request full deletion

PAUSE AND THINK QUESTION

"Is this information still needed or should I ask for it to be deleted?"

You can ask apps and websites to delete your personal data.

This right is very powerful but remember: once something is shared widely online (like Gianni's selfie could have been), it's very hard to get it back completely. Other people might have already copied it, screenshotted it or shared it. That's why thinking before you share is so important! The right to erasure works best when you catch things early.

Right to Object

What it means

You have the right to say '*NO*' to certain uses of your personal data. If you don't like how your information is being used, you can object and ask them to stop. You don't always have to just accept it!

Real-World Examples

- You can say 'no' to apps using your data for advertising
- You can object to your information being shared with other companies
- You can refuse to let apps track your behaviour and habits
- You can say 'no' to apps selling your information
- You can object to targeted ads based on your personal data

Connect to Gianni

- Gianni could object to the quiz using his answers to send him targeted ads for Minecraft toys and art supplies
- Gianni could say "no" to the location app sharing his movements with other companies
- Gianni could object to apps creating a profile about his gaming habits and selling that information

What Gianni could do

- Choose apps that don't track and sell information

PAUSE AND THINK QUESTION

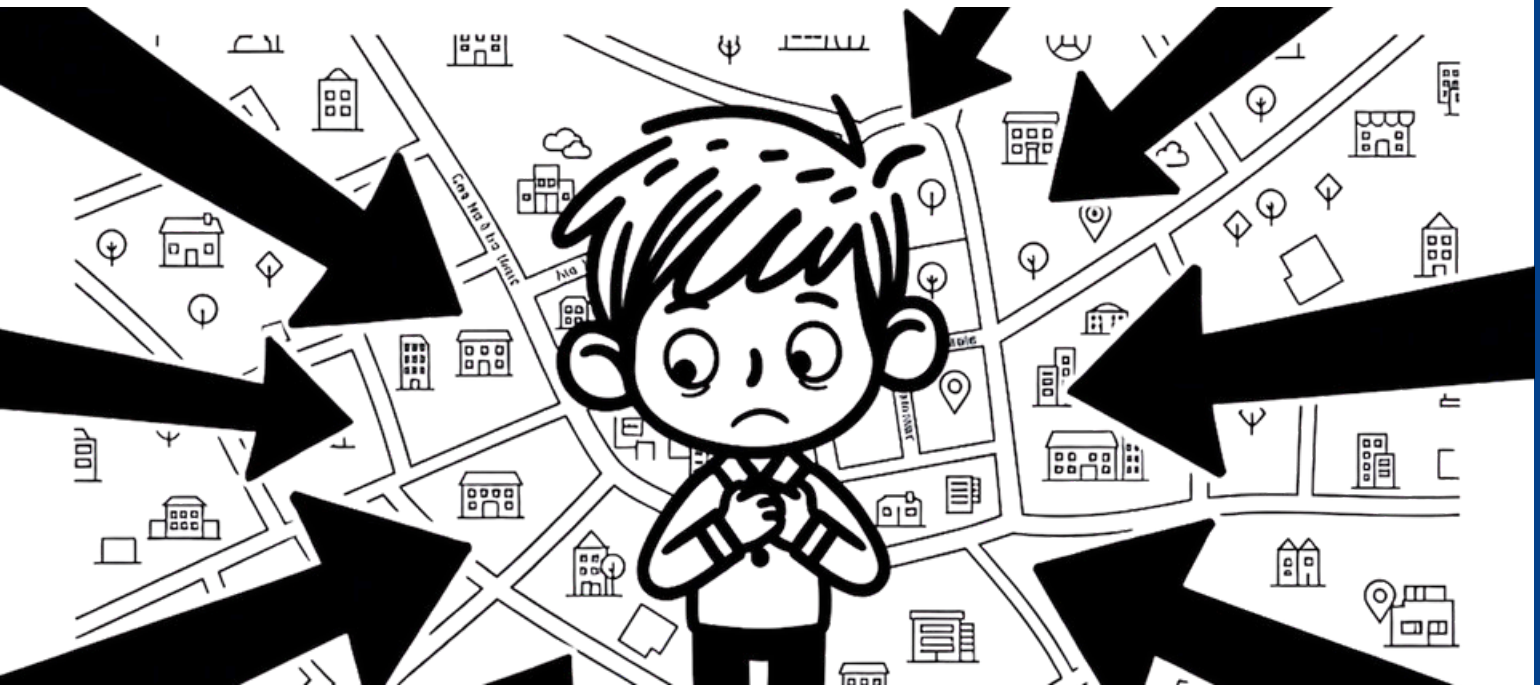
"Do I feel comfortable with how my data is being used or should I say no?"

You have the power to say NO to certain uses of your personal data.

04 Rights Detectives

Students solve cases by identifying which right to use.

CASE #1	*Maya signed up for an app, but she has no idea what information they collected about her. She's worried! Which right can help Maya?*	**RIGHT OF ACCESS** *(She can ask to see what data they have)*
CASE #2	*Tom's gaming app thinks he's 13, but he's only 9. Now he's seeing content for teenagers! Which right can help Tom?*	**RIGHT TO RECTIFICATION** (He can ask them to fix his age)
CASE #3	*Sofia keeps getting advertisements for toys she doesn't want. The app is using her search history to show her ads. She doesn't like it! Which right can help Sofia?*	**RIGHT TO OBJECT** (She can say NO to personalised advertising)



CASE #4	*Jake used to play a game two years ago. He doesn't play anymore, but the app still has his email, photos and date of birth. Which right can help Jake?*	**RIGHT TO ERASURE** (He can ask them to delete everything)
CASE #5	*Emma downloaded an app that started tracking her location, but it never explained why or who could see it. Which right was broken?*	**RIGHT TO BE INFORMED** (The app should have explained clearly before tracking her)

05 Follow-Up Activity (Optional)

Give each student a blank A4 sheet and ask them to draw a picture, symbol or short slogan that represents one of the four rights they learned about: the right to be informed, the right of access, the right to rectification or the right to erasure. They may also include a short slogan such as *"Tell Me First!"*, *"Let Me See My Data!"*, *"Fix My Info!"* or *"Delete It, Please!"*

Create a display area titled *"Our Data Protection Rights Cloud"* and hang all drawings together.

Contact Information

Phone +356 2328 7100
Website www.idpc.org.mt
Email idpc.info@idpc.org.mt

Address 2, Airways House
High Street
Sliema, SLM 1549