you decide...

Thoughts and facts about protecting your personal data for 13-17 year olds

This brochure has been published by The Data Inspectorate in cooperation with
the Norwegian Centre for ICT in Education and the Norwegian Board of Technology.
First edition January 2007, revised 2011.

ISBN 978-978-82-997509-0-5

First print run: 52 000
Second print run: 51 000
Third print run: 68 000
Fourth print run: 60 000
Fifth print run: 80 000
Sixth print run: 80 000

Editor in chief: Ove Skåra, The Data Inspectorate
Project manager: Karoline Tømte, Norwegian Centre for ICT in Education
Journalist: Inger Lise Welhaven and the editorial team
Concept/production: Gambit Hill & Knowlton
Design: Haugvar Kommunikasjon & Design
Photography: Håvar Haug/Bård Ek
Illustrations: Åsne Flyen
Printing: BK Grafisk

For more information, go to www.dubestemmer.no

The Data Inspectorate
P.O. Box 8177 Dep
NO-0034 Oslo, Norway
Tel.: (+47) 22 39 69 00
www.datatilsynet.no

Norwegian Centre for ICT in Education
P.O. Box 530
NO-9256 Tromsø, Norway
Tel.: (+47) 854 19 000
www.iktsenteret.no

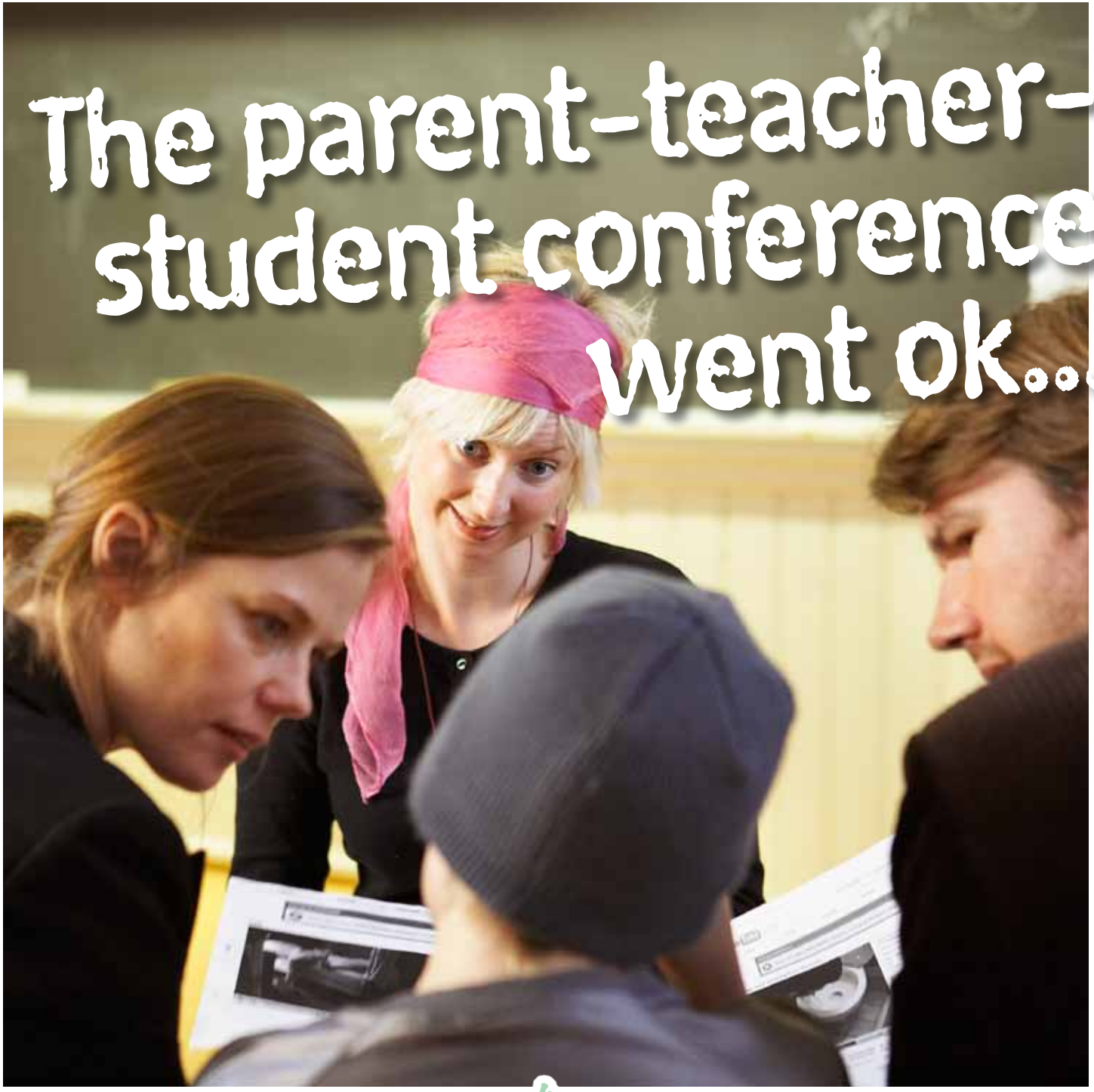
Norwegian Board of Technology
P.O. Box 522 Sentrum
NO-0105 Oslo, Norway
Tel.: (+47) 23 31 83 00
www.teknologiradet.no

YOUR CHOICE

This brochure underlines the importance of protecting your personal data. It shows you how your personal details can be used and abused by others, and how you can protect this information.

You'll already be familiar with much of the content, but other bits will likely be completely new to you. We hope this brochure will help with discussions – and perhaps introduce you to new concepts. Our goal is to help you make the right choices.

You decide.


The parent-teacher-student conference went ok...

... but all hell broke loose when the teacher googled my work!

You don't show up to the parent-teacher-student conference and admit to taking your essays straight from the Internet. And you're not likely to raise your hand in class and tell people what websites you've been on lately. If you have a secret to tell your friend, you're hardly going to advertise it on flyers in the cafeteria.

There are some things you'd rather keep to yourself ...

But then you might not be as anonymous as you think.

BANG! The door slams shut. Alone at last. You sit down in your chair. Turn on the computer and get out your mobile. Chatting with friends and surfing online. Left to your own devices, away from annoying parents and nosy younger siblings. And if they really must come in, they will have to knock first. You rule the roost in your room.

"PROTECTING PERSONAL DATA MEANS THERE ARE BOUNDARIES AND RULES FOR HOW OTHER PEOPLE CAN USE INFORMATION ABOUT YOU."

You are entitled to be left in peace

We all have things we don't want to share with other people. Not because they are illegal or because we need to keep them hidden necessarily, but simply because it's our own private business. This is why you are the one who should normally decide what other people find out about you and what information you choose to keep to yourself.

Your choices

You alone decide what you want to share and who you want to share it with. Very few people will want to circulate embarrassing pictures of themselves and risk their boyfriend or girlfriend, teachers and parents finding them just a few seconds later. No one likes it when other people snoop around their private things, whether it be their bedside cabinet or on their computer.

Your boundaries

The need to have your own personal space, which others respect and don't barge into, varies from person to person. Different groups of friends also have different views on what is private. What's more, attitudes about what is private have changed. Things that your parents may only ever have done behind closed doors are perhaps things that you wouldn't think twice about showing everyone.

Sometimes we need to be anonymous. We should be able to feel secure in the knowledge that no one else is able to know everything about us, or see everything that we do. This is why you can go to the school nurse without others finding out what you talked about. You should also be able to go to the bathroom without being recorded on camera.

You have the right to shut the door and decide for yourself who you invite in.

WHAT DO YOU THINK?

Where do the boundaries lie for what your parents should have the right to know about you? Should they be able to see what you keep in your bedside cabinet? Should they be able to see your bank statements to check how you are using your debit card? Is it ok that they go onto your computer and check which websites you've visited? Is it ok that your parents use services on their mobile phone to check where you are?

How old should you be before your parents are no longer able to demand access to information about everything you do? Should there be different limits for the examples listed above, and if so, how should these be defined?

TASK:

Attitudes about what is private and what is appropriate for public consumption have changed.

Find examples of situations shown on TV, online, in newspapers and magazines that you think could not have been shown 20 years ago, because they would have been considered 'private'. Show how the boundaries have changed. Where do you think the boundaries should lie today?

Find more tasks and watch videos on protecting personal data and the right to privacy at www.dubestemmer.no

The Personal Data Act

The Personal Data Act is intended to ensure that information about you is used in a way that is respectful of you. The purpose of this Act is to protect people from having their right to privacy violated through the processing of personal data.

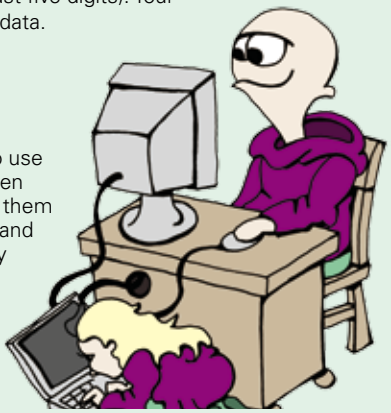
Personal data

An item of personal data is an item of data that can be linked to an individual person. For example, this means that a name, age, address and telephone number are items of personal data if they can only be linked to you. Images that can be identified as a certain person are also a form of personal data, even if no name is attached to the image.

Your national identity number consists of your date of birth (the first six digits) and your personal number (the last five digits). Your national identity number is an item of personal data.

Consent

Other people are generally not permitted to use your personal data unless you have first given your consent, i.e. you have agreed to allow them to do so. Your consent should be voluntary and given willingly, and can be withdrawn at any time.



This is the general rule, but there are exceptions. For example, in a number of contexts, central and local government authorities are allowed to record and use your personal data without your consent.

The general rule is that once you have turned 15, you can agree to the collection and use of your personal data. If you are younger than this, anyone who wants to use your personal data must generally obtain your parents' consent. If sensitive personal data is involved (such as criminal acts, health, sexuality, etc.), your parents' consent is often required until you reach 18.

Information and access

- If you give out your personal data, you have the right to know who is collecting this data, what it will be used for, whether it will be transferred to other people and if so, who will have access to it.
- You have the right to know what data other people hold about you, what the information is going to be used for and how they have obtained the information.
- You can request that incorrect or incomplete information be corrected.
- Data that is no longer required for the original purpose should be deleted.

THAT'S LIFE!

Contact details end up in the wrong hands

A teenage girl gave out her name, age, e-mail address and telephone number when she was looking for penpals on the Internet. The information was misused and she received some very unpleasant messages from people she didn't know, including older men. She found it very difficult to get the information removed once she had lost control over it, and it took no less than two years before she got help removing what she had put on the Internet.

Source: NRK

Monitoring her daughter's spending

One mother explains that she puts her daughter's allowance into a bank account using a debit card rather than giving her cash. She regularly goes through her daughter's bank statements online, giving her a complete overview of when and where her daughter has spent her allowance.

Source: The Data Inspectorate

SCHOOL CAN BE BORING – sometimes. It can be very tempting to duck behind the screen and find something more fun. But even if you're sitting in a corner and no one is looking over your shoulder, there are a lot of people who can see what you're doing.

"PERSONAL DATA PROTECTION IS BASIC PROTECTION OF THE PRIVATE LIFE OF THE INDIVIDUAL"

Not as anonymous as you might think

Personal data is a currency which is becoming more and more valuable, and one of the fastest-growing data types on the Internet. Most young people circulate information and images of themselves and other people on blogs and social networking sites. There are also many official sources of public data, such as tax registers and telephone directories. The tools for searching and combining information online are also constantly improving.

Take control

Creating a profile on a social networking site is easy, but many people don't realise that personal privacy settings are often set so that everyone can gain access to their profile. For example, you should remember that if you have not actively changed your user settings, people other than your friends will probably be able to see your photographs and read your profile.

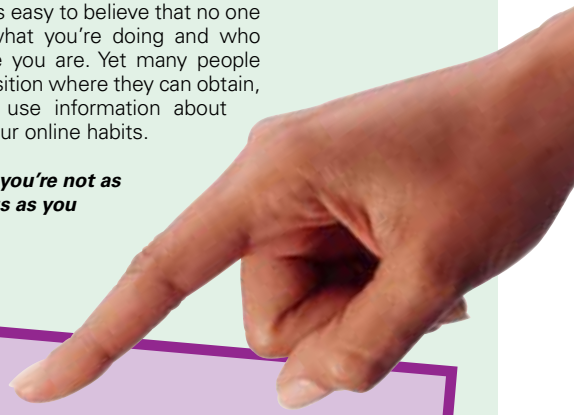
Some social networking sites alter their personal privacy settings regularly, without informing their users. This means that information you thought was hidden, can suddenly become accessible for everyone. It is therefore important that you check your personal privacy settings at regular intervals.

It can also be a good idea to remember that profiles on some social networking sites are linked to the search engine Google. This means that everyone who searches for your name will be able to see all or part of your profile depending on your personal privacy settings.

Something that is not always obvious with some social networking sites is what information about you different applications have access to. Every time you or your friends add an external application such as a game, the developers of the game can obtain information about you.

Sitting on your own behind a screen, it is easy to believe that no one can see what you're doing and who and where you are. Yet many people are in a position where they can obtain, store and use information about you and your online habits.

So maybe you're not as anonymous as you think...?



WHAT DO YOU THINK?

What's the problem with having a profile on a social networking site? Have you checked out your personal privacy settings to see who can view your profile and who has access to your information? Do you know who owns the images you upload and who, if anyone, can use them?

TASKS:

Talk with other people in your class. Help each other figure out how you can:

- delete the history file in your browser
- delete all temporary files ("temporary Internet files")
- alter the privacy settings in your browser
- alter the privacy settings on a social networking site you are a member of

Choose two applications. Try to find out what sort of information about you or your contacts they have access to. What do you think they need this information for?

Find more tasks and watch videos on anonymity and social networking sites at www.dubestemmer.no

Like an open diary

Other people are able to see which websites you've visited, either by checking the history file or temporary files for text, images and e-mails. These files are not automatically deleted when you close the browser. You should remember this, especially if you share a computer with other people.

How can they know who I am?

Every time you go online, you are assigned an IP address. This address is unique to each piece of equipment (computer, mobile, printer) and is like a telephone number. The Internet service provider records when you are connected and which IP address you have been assigned. The websites also record the IP addresses that visit them. If the police want to investigate who has visited a website, they can check the website's logs and then ask the Internet service providers for a list of who was using the IP addresses at a particular time.

Many websites are interested in knowing who visits them, so they save a small file (called a cookie) on your computer. Each time you visit the website, it checks whether your computer has such a cookie file, and records the information contained in it, for example the user name and password used to log in to the website. You can refuse to allow websites to store information files by changing your privacy settings in your browser. However, this could prevent some websites from working properly. You must decide what is more important to you: your privacy or accessibility.

Who should be able to see what?

It is important that you check your privacy settings for the social networking sites you are a member of carefully. Here are some tips for what to look for:

- Who has access to your information? Do you have an open or a closed profile?
- Have you made lists of friends, so that you have more control over who can see what?
- Can search engines such as Google see your profile?
- Do the developers of applications have access to information about you?
- Do you know what your friends can share about you? Could they tag images of you, for example?

THAT'S LIFE!

Video making threats intended as a joke

A school in Eastern Norway was closed immediately when a video which made threats was discovered on YouTube. The video warns, in English, that a massacre will be carried out at the school, and makes death threats against six teachers. After the Norwegian National Criminal Investigation Service traced a 15-year old pupil at the school, he admitted to both making and uploading the video. In court, the boy said how shocked he was when he realised the magnitude of what he had done. He had only intended it as a joke.

Source: Aftenposten

You share valuable information with more people than you think

Many people use the 550,000+ games and tests that are available on Facebook, but not everyone knows that they also give out valuable information about themselves and their friends. Many of the most popular games collect, store and share your personal data with other people. They will also continue to store information about you and your friends even if you delete your Facebook account.

Source: Norwegian Consumer Ombudsman


It was just a joke...

... but suddenly I had pressed "Enter"!!

You don't give out photos of your girlfriend to men you don't know.

If you film everything that happens at the end-of-year party, you don't show the film on a big screen at the local shopping centre.

Probably not...

You decide what other people should know.

IF YOU HAVE A BLOG, PROFILE etc. online, you are the editor for these pages. Information that is published is made available to large or small groups of people, depending on the settings you choose. As editor, you have a responsibility. A responsibility for what information you can and can't circulate about others, but also a responsibility as regards what you should and should not publish. What seems ok to you, might not be ok for others.

You are your own editor

We all need to be noticed. Some people sign up for reality TV shows. Others create a blog or a profile on a social networking site where they post images and information about themselves.

A big responsibility

All newspapers have an editor who is responsible for everything the newspaper prints or posts online, both text and images. Deliberate lies, slander, illegal images and racism can do great harm and lead to fines or imprisonment. The press has also drawn up a set of ethical guidelines for journalists and editors to follow, called "The Code of Ethics of the Norwegian Press".

Just like a newspaper editor is responsible for their newspaper, you are responsible for everything you post online. So you need to think about what you post as far as your own personal information goes, not to mention information about others. The same applies to images. It is equally important to be able to take responsibility for what you post on blogs and other websites. What may be a joke to you at the time, may seem harmful to others.

Too late to go back

It can be fun to post information and images of yourself or other people. Sitting in front of your computer at home, it may seem innocent and not in the slightest bit dangerous, and it is easy to shift the boundaries between what is private and what you choose to share with others.

Sometimes it can be almost impossible to delete information and images that have been posted on the Internet. Other people may have downloaded the information and posted it on other websites, or copies may have been stored by search engines.

Think before you press "Enter".

WHAT DO YOU THINK?

Have you ever regretted posting something on the Internet about yourself or others, and if so, why did you regret it?

Why do you think some people decide to post images of themselves on social networking sites? Is it ok that there are different boundaries as regards what and how much you want to post?

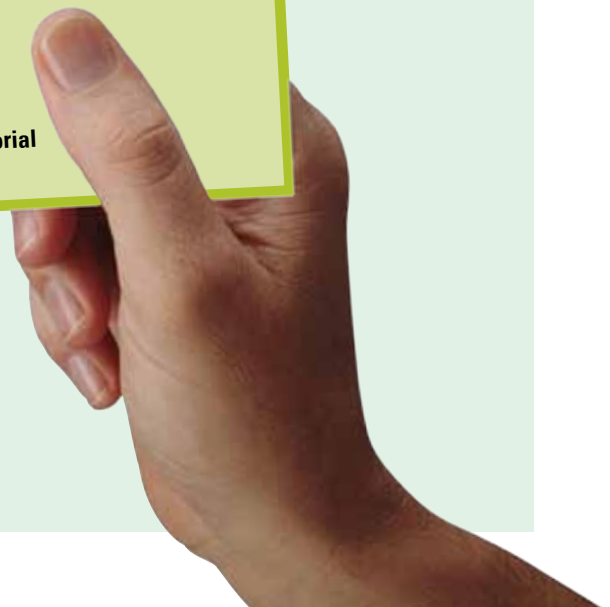
TASKS:

Type your name or user name in a search engine.

- What do you find?
- Do you feel it gives an accurate picture of who you are? Why/why not?

Find "The Code of Ethics of the Norwegian Press". Create your own code of ethics with guidelines concerning what you post online.

Find more tasks and watch videos on editorial responsibility at www.dubestemmer.no



A real YES!

Every time you upload images of one or more identifiable people online, you must ask their permission first, and receive a real YES in response. But a yes given at one point in time won't always hold true. If someone who said yes changes their mind at a later date, you are obliged to help remove the image.

Rules for the use of images:

The rules distinguish between two types of images. Those which focus on people and those which focus on activities. If one or more people are the main point of focus, you must always get the consent of everyone who can be identified, either directly or indirectly, in the images before they are published. This also applies to group images, such as class photographs. If the people in the image are under 15, their parents or guardians must also consent to the publication.

If it is the actual situation or activity that is in focus and the people in the image are less important, the images can be published without consent if they are not harmful for the people in the image. Examples of this are images from a public parade or concert. The images must also not seem harmful given the context in which they are being published.

Get rid of it!

This is how you delete unwanted information about yourself online:

1. **Talk to the person who published it**
   Do you know who posted the unwanted information about you? Contact the person concerned and ask them to delete the information.
2. **Talk to the Internet service provider**
   If you do not know who posted the information, or they will not listen to you, you can contact the website (the domain) on which the information has been published. To find out who owns a Norwegian domain, go to the Norwegian WHOIS database at www.norid.no.
3. **Contact organizations or public authorities**
   Slettmeg.no has an overview of organizations that can help you.
4. **Contact the police**
   If you think the information is so extreme that it should be removed immediately, you should contact your local police station. Report the situation!

THAT'S LIFE!

Fights caught on video

There's a full-blooded fight going on in the school playground. Two students are letting each other have it, egged on by other students. More people gradually join the throng. Many people are holding their mobile phones up in the air. The clash is being filmed. The videos are uploaded onto YouTube.

Every day hundreds of thousands of new video clips are uploaded onto YouTube. Several show Norwegian students involved in fights. YouTube receives over 250 million hits a month and videos like these are watched by thousands of viewers.

In many contexts, it is illegal to upload videos onto the Internet without the consent of those involved.

Source: Dagbladet

Photographs of graduating students end up on a porn site

Photographs of a number of graduating girls have been posted on a pornographic website. The girls are for example depicted topless during their graduation celebrations. Some of them are drunk and having sex. Many of the images give the impression that those being photographed have no idea they are having their photograph taken. And those who have turned up naked probably did not imagine that the images might end up on a porn site. The images have probably found their way to the website via people's blogs, Facebook, mobile phones or the like. Some of the images were also taken in context with typical graduation activities, such as skiing naked through a town centre.

Source: NRK

HAVE YOU HEARD ABOUT MARIA IN THE OTHER CLASS?

Check out what she did at the party last weekend! Pass it on; Have you heard about Maria in the other class? She was out of her tree; check what she did at the party last weekend!

Just think a little about ...

Rumours can spread like wildfire via the Internet and text messaging. It is quite possible that Maria filmed herself drunk at a party and sent the video to her best friends, but who is responsible for the fact that the video has now been spread far and wide? Is it ok to pass on a video that puts someone in a bad light? Who posted the first unpleasant comment? Maybe the video of Maria was intended as an innocent prank that has now got completely out of control?

Impossible to stop

Once a rumor has been started, it isn't easy to stop. Once a video has been sent from your mobile, there's no "Undo" button. Threats, slander, false allegations or breaches of a person's right to privacy are actually punishable by law.

The Internet and mobile phones are making the world smaller and social networks bigger. We now have communication opportunities that previous generations could never have imagined. But they also give us unprecedented opportunities to hurt each other. Research has shown that bullying online and via mobile phone is a significant problem among young Norwegians.

Students tease the teacher until he explodes in anger in the classroom. Someone films everything on their mobile and uploads it onto the Internet. The guy who's drunk the most at the party is persuaded to strip in front of the camera. The next day, the whole world can see the images. A former friend "steals" Emma's identity and sends an unpleasant message to her friends, using Emma's number as the sender.

WHAT DO YOU THINK?

Some people claim that the Internet and mobile phones have made it easier to bully other people. What do you think?

Think back to messages and images you have sent or passed on. Could some of these have harmed other people and if so, how?

What have you done or said on the Internet that you would never have done in real life?

Has anyone uploaded information about you onto the Internet? If so, did you like what you saw? Did they ask your permission first?

TASKS:

Get together into groups and come up with some rules for how you want people to act towards each other. Focus on the Internet and mobile phones in particular.

Find examples in the media of mobile phones or the Internet being used as an arena for bullying. What was done about it?

Find more tasks and watch videos on digital bullying at www.dubestemmer.no

Think for yourself

When you're sitting in front of your computer or holding your mobile phone in your hand, you're the one who decides what you want to share with the rest of the world. You are responsible for thinking it over before you send or forward information and allegations about other people.

If you wouldn't dare say it to their face, you shouldn't say it online either.

Digital bullying

Bullying is when one or, more usually, several people perform negative actions against another person over time. Bullying can cause long-term harm to the person concerned.

The Municipal Mediation Services

The Municipal Mediation Services are seeing a rise in the number of cases where children or adolescents are threatened or bullied on the Internet. According to the police, many cases of violence start in this way.

The Municipal Mediation Services receive and consider cases involving digital bullying from the police, schools, school nurses, parents and others. The Municipal Mediation Services will be happy to tell you whether a case involving bullying is something that they can consider.

The Municipal Mediation Services can arrange information meetings for parents and teachers.

THAT'S LIFE!

Punished for online bullying

After calling another girl "a whore" in an online chat room, a 17-year old girl in Eastern Norway was convicted of disturbing the peace of another. The court considered that the message could be classed as public harassment and bullying and should therefore not be protected under the right to "freedom of expression". The girl was ordered to pay a fine of NOK 4500. "We always find out who is behind this kind of harassment. People think they are anonymous online, but you always leave behind electronic tracks," said the owner of the website.

Source: digi.no

"I can't take any more"

Last summer, me and my friends partied a bit, like most teenagers. We had a really good time and met new people. We took photos and posted them on a webpage. We had a password and everything! Nothing could go wrong. But when school started again, a lot of people heard it was a "party site", and people became more and more eager to get the password. Then something terrible happened with the website where we had uploaded the images. Suddenly everyone could see the "owner's" pages. The nightmare started when the people we knew told their parents. In the end, one mother contacted the school and explained everything. We had to talk to teachers and counselors. My parents were also contacted, but fortunately they thought it was just part of being a teenager. It was worse seeing the other students. They knew something, all of them did. When I started school a year ago, I had a great time. But now I dread going to school every single day. I have learned a valuable lesson – I won't ever post something on a website, whether it's images or anything else. Now I feel like I have a video camera following me. Regards, anon.

Source: Aftenposten, reader submission in the comment section Si ;D (abridged)

Harassment of the teacher

A teacher at a secondary school had a serious argument with one of his students. Several months later, the student got his revenge by creating a website in the teacher's name, full of gross invasions of privacy. For example, photos of the teacher were uploaded along with false allegations and gross harassment. A chat page was also set up where other pupils could write comments and statements about the teacher. The website was reported and deleted, but the teacher found the whole episode extremely unpleasant.

Source: The Data Inspectorate


I had to check in
then of course ...

... but I hadn't thought about the consequences!

You don't leave your unlocked diary lying around on your desk if you want to make sure no one will read it.

And if you download films illegally from the Internet, you don't send a letter to the film company afterwards, saying "I've stolen a couple of films from you".

Or...?

Who actually knows what you're doing?

YOU UPDATE YOUR STATUS on Facebook, check in your position, write an e-mail to a friend, pay for a packet of gum with your card, swipe your monthly electronic bus pass and smile at the CCTV camera at school.

"EVERYONE HAS THE RIGHT TO EXPECT HIS PRIVATE LIFE AND FAMILY LIFE, HIS HOME AND HIS CORRESPONDENCE TO BE RESPECTED."

From the European Convention on Human Rights

Who knows what about you?

Even before your first lesson has started, many people have recorded what you have been doing and where you have been. Over the course of a day, we give out enormous quantities of information about ourselves, both consciously and subconsciously. The sharp rise in interest among commercial organizations in using this information means that it is important that clear boundaries are established as regards how freely information about you can be used.

Nothing but positive?

Camera surveillance can help to prevent and clear up crimes such as vandalism, violence and theft. If a CCTV camera is installed at your school to reduce vandalism at night, it is ok that the same camera is used to catch furtive smokers during the daytime?

Is it ok for your parents to install a tracking program on your phone, so that they know where you are and who you are in contact with at all times?

The more digitalised our everyday lives become and the more information that is stored about us, the more important it will be that we know what is being stored about us and how the information is being used. Our personal data is the currency of the future and will only become more and more valuable for many organizations. We give out small pieces of information in many different contexts and to many different organizations and people. What happens when the information is combined and used for something other than what we had intended?

WHAT DO YOU THINK?

Do you behave differently if you know that a camera is watching you? Is it ok if someone can see everything you're doing, all the time?

Who should be allowed to know what you are doing on the computer you are using at school? Teachers? Classmates? Parents? What should they be able to check and how should they be allowed to use this information? If your school discovers that bullying is going on via the school network, should the teacher be able to check what has been done and who is behind it?

TASKS:

What rules apply to the use of computer equipment at your school? Is there a difference between the use of private equipment and the use of the school's equipment?

Find out whether your school has rules about the teacher's right to know about your use of digital equipment at your school. What do you think the teacher and the school should and shouldn't be allowed to check? Draw up some suggestions for rules.

Find more tasks and watch videos on surveillance and anonymity at www.dubestemmer.no

Take responsibility

Each and every one of us is responsible for protecting our own information whenever we can. You don't leave your bike in the town centre without locking it first and you don't go on holiday without locking your front door. In the same way, it is important to protect your information by using good passwords which you keep to yourself. Always.

Remember, your personal data is valuable currency. Take control!

No surveillance during school hours

Many schools have installed CCTV cameras in an attempt to combat vandalism, etc. but this raises important issues as regards privacy. Children and young people have a right to have their private lives respected, just like adult employees. The school playground has similarities with an employee's break room, and students can generally not choose whether or not they want to be there. Children and young people are more vulnerable than adults and are not able to establish boundaries as regards what they should do. It is therefore particularly important that the school handles this issue appropriately. There are examples where camera surveillance during school hours has even been used to catch furtive smokers, to see who is rooting around in the cafeteria or to identify students who leave the school premises.

The Data Inspectorate therefore normally orders schools to stop any surveillance of the students during school hours. Students and employees at the school must of course also be informed about any surveillance that is taking place both during and outside school hours. Concealed surveillance is never permitted.

Take control over your private information

Mobile phones, tablets and computers contain a lot of private information about you and your contacts. Once an unauthorised person gains access to your personal data, they can steal your identity. It is therefore vital that you protect your equipment. You could for example do this by using a:

- device lock. This is a screen lock with a password, pattern or PIN code.
- PIN code. This is required every time your phone or tablet is restarted.
- tracking program. There are programs that can locate phones, delete the content remotely or activate an alarm.

Remember, always check what kind of information the applications that you install will have access to. Back up your content regularly. Never leave your phone or computer unattended without activating the device lock!

What is the school allowed to check?

As a general rule, schools are not allowed to monitor Internet use by its students using the computer system's logging function. The aim of the log is to ensure that the computer system is used appropriately. But the log can also be used to identify unwanted activity on the Internet, providing the student's identity is not revealed. In such cases, the school can use the information in the log to send out warnings that the Internet activity must cease. The school can also consider closing off access to the websites concerned.

The school can demand access to e-mail if it suspects that it contains information on criminal offences, or if there is reason to believe that a student is using e-mail to harass someone or to distribute spam or viruses. The school should establish clear guidelines for the use of its computer equipment. It can be a good idea to involve students in this process. But remember: the school is not allowed to access the private computers of students even if they are using the school network.

THAT'S LIFE!

Hidden camera in smoke detector

A baker's shop in Oslo was ordered to pay a fine by the Data Inspectorate after secretly monitoring its employees. The camera was disguised as a smoke detector and was installed in a room where the employees could withdraw to do office work and private chores. The employees believed they were not being monitored while they were in this room. "This is gross negligence," says Bjørn Erik Thon, Director of the Data Inspectorate.

Source: VG

Got the sack after surveillance

A binman was fired after the management checked the log from the GPS that was fitted in his bin lorry. It was alleged that the driver took excessively long breaks and claimed too much overtime. The Data Inspectorate, the Norwegian Data Protection Tribunal (Personvernnemda) and the court of appeal concluded that the company's use of information from the GPS system in this case was illegal. The employees had to be told about the use of personal data in this way in advance.

Source: NRK

Jealous ex-boyfriend took revenge

A love-struck 16-year old girl shared everything with her boyfriend – intimate pictures of herself, user names, passwords and other personal information. When the relationship was over, he took revenge by logging in to her Facebook profile and blog, and uploading the revealing images of her there. He also changed the passwords to her accounts, so that the girl couldn't remove the images.

Source: slettmeg.no

YOU DECIDE WHO YOU CALL AND WHEN. YOUR TELECOM PROVIDER WILL RECORD IT.

You decide where you use your debit card and what you use it for. The bank records it. You decide which search terms you use in Google. The search engine records it. You decide what to buy online. The website stores the information. Over the course of a normal day, you leave many tracks behind you. Many people may be interested in them.

Do you know who's following you?

11 September 2001: terrorists flew into the World Trade Center in New York. After the attack, stricter security controls, including new passports, more wiretapping, the tracing of mobile phones and the monitoring of Internet traffic were introduced to prevent further attacks and other criminal activities.

Use and abuse

The increased fear of terrorism and other serious crime has meant that the boundary for what we are willing to accept in terms of monitoring and surveillance is shifting. Developments in technology mean that this is actually possible. Most people consider using someone's electronic tracks to fight crime as a positive thing, but is it right that we are all more or less treated as suspects in the event that we do something wrong sometime in the future?

Never before has it been possible to gather so much information about each and every one of us. It can also be tempting to use this information for purposes other than what it was collected for. Electronic tracks can be used for purposes we don't like, such as commercial enterprises that use electronic tracks for marketing and sales.

Good intentions

There are a lot of people who collect information about you so that they can offer good services. For example, you are registered in the public health and school databases so that you can receive good public services. The police and the judicial system need to be able to collect information and check electronic tracks in order to investigate crimes and convict criminals, saving lives and maintaining law and order in society.

It is important to establish clear rules on who has the right to collect information about others, how this information is to be used, what it can be used for and how long it can be stored. Information that is collected for one purpose should not automatically be used in other contexts.

More and more of what we do is recorded. Surveillance cameras are watching us in more and more places. Someone is watching us and collecting information about us even when we're not doing anything wrong. Some people don't like this idea, even if they know their hands are clean.

Can surveillance always be justified?

WHAT DO YOU THINK?

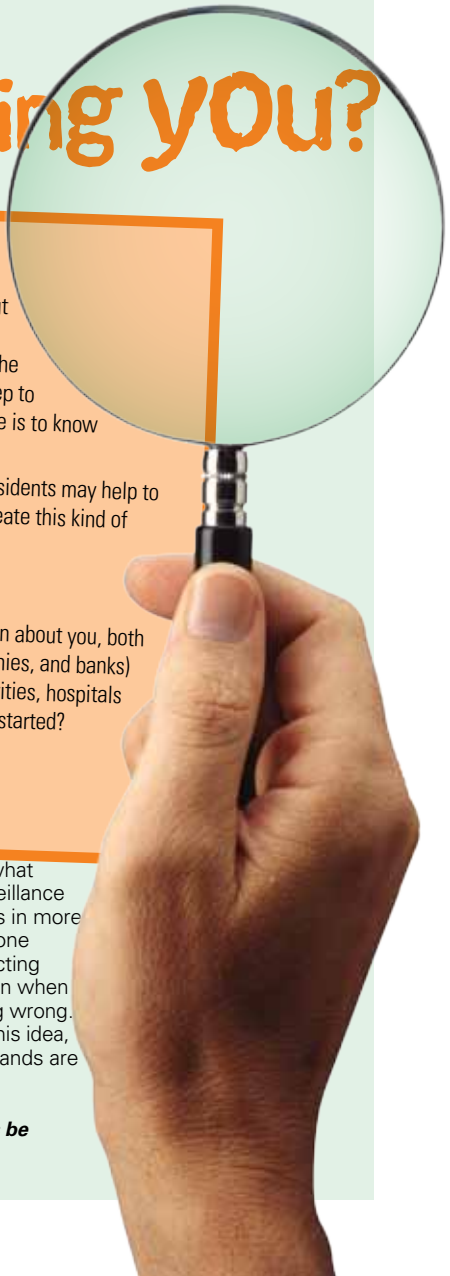
There are many people who want to get hold of information about you and your online habits and interests. Work out what information you give out about yourself on different websites. Draw up a list of the information you think it is ok to share and what you would rather keep to yourself. Is it ok that commercial organizations know everything there is to know about you? Why/why not?

DNA testing of all newborn babies and a DNA database of all residents may help to solve crimes in the future. Do you think it would be a good idea to create this kind of database? What kind of problems might this cause?

TASK:

Make a list of the organizations you think have collected information about you, both commercial organizations (such as Internet providers, telecom companies, and banks) and public organizations (such as central and local government authorities, hospitals and schools). Is the list longer than you thought it might be when you started?

Find more tasks and watch videos on digital tracking at www.dubestemmer.no



THEY'RE WATCHING YOU!

Your medical records are secure, right?

In order for the health service to work, medical information has to be stored on every single patient in medical records. At the same time, patients must also be secure in the knowledge that the information they give will be taken care of and will not be made available to unauthorised people. The consequences of patients withholding information they feel is particularly private because they are afraid that the information could end up in the wrong hands could be serious.

On a number of occasions, it has become apparent that medical records at Norwegian hospitals are not sufficiently secure and that far too many people can gain access to the information they contain. At one hospital, a head of department read the medical records of several of his subordinates without any authorisation. At another hospital, the chef had access to all the medical records in order to check who had allergies. This shows how important it is that hospitals keep medical records securely and know who has access to what.

Everything is recorded

To combat crime, the EU has established a Data Retention Directive. The regulatory framework means that information about who people speak to by telephone, how long the calls last and when the calls take place is to be archived for up to two years. This also applies to information about who individuals send e-mails to and receive e-mails from, and when they are connected to the Internet. Information on where you are when you are communicating is also stored. It is up to each individual country to decide how long the information is to be archived. In Norway, the Parliament decided that the regulations should apply from 2012, and that the information should be retained for six months.

You are being recorded

Many people are interested in your personal information and you are recorded on a daily basis. More and more organizations are collating information about you. The police can use the information to uncover crimes, while criminals do it to commit identity theft or other crimes. Commercial organizations need your information to make money. Nothing is free – you pay with your personal information. And remember that you have the right to demand access to information that has been recorded about you. You also have the right to have incorrect information corrected or deleted.

World of Warcraft

In the online game "World of Warcraft", the operator of the game can "see" whether you are using a code-breaking program while you play. If you cheat, they can expel you from the game.

Tailored advertisements

Social networking sites, search engines and other websites store information about your searches and online habits. They also store information that they obtain through messages you send and receive. For example, Google uses software that scans your e-mail and searches for words that reveal what you're interested in. This information is used to tailor the advert you see in your browser. You will therefore see different adverts to your friends. Your personal data is very valuable and commercial organizations will often pay to get hold of it.

With dad in tow

A teenage girl went on a skiing trip with her friends and without her parents. Her father subscribed to a mobile phone-based service which enabled him to sit at home at his computer and keep an eye on where she was. He didn't see anything wrong with this kind of monitoring. His daughter said she thought it was ok too, although she was a little sceptical that her father could trace her at all times. The Ombudsman for Children in Norway, Reidar Hjermann, was extremely sceptical about this. In his opinion: "A system where parents can check where their children are at any time is an obvious violation of the child's private life".

Source: NRK Dagsrevyen

To protect personal data, there are rules concerning how other people can use information about you. We hope you now have a better understanding that will help you decide what information you should give out to other people, and who you should give it to.

Although there will inevitably be situations where you don't always have complete control, we hope that you nevertheless feel a bit more secure. Because in most situations, it really is **YOU WHO DECIDES!**

TO THE TEACHER

Some rules – like using common sense and showing consideration for others – apply both online and in real life. In other areas, there may be characteristics associated with digital media which mean you need to know a bit more and reflect a little.

Tips for use

This booklet is intended for use as a basis for discussion and reflection. For some classes, it will be better to use 'You decide' in small bites in individual lessons over a longer period of time, while for others, it will be better to work intensively on the issue over a project week.

You can go through issue by issue from folder to folder, or you can select an issue that is particularly relevant for your class. Some issues are also ideal subjects for discussion as a group, while other issues are better suited to a discussion between students and their parents or guardians.

At www.dubestemmer.no, you will find videos, MORE issues and tasks. The videos are ideal as a basis for discussion.

At some schools, a year group has been given the task of teaching younger pupils about 'You decide' issues. This often works well because the older students learn by doing the teaching themselves, and also act as role models for the younger pupils.

'You decide' can be used during parents' evenings. Many of the tasks and videos are just as well-suited to adults as they are to young people. Aware and committed parents are important in creating good online sense at home.

You should note that some of this material may be unpleasant to certain pupils. We are aware of cases where pupils have found sensitive and personal information about themselves, which they did not know existed. The teacher must therefore to some extent assess whether the tasks are suitable for the students concerned.


www.dubestemmer.no