Digital Transformation and You! - Empowering Schools and Students

(1) Operating Systems
Operating systems know your device and everything on it.

General Tips:
- Use operating systems with lean data usage which respects privacy!
- Configure them such that:
  - no microphone or camera is active
  - no telemetry data is collected and sent
  - no cloud services are used
- Use data-lean anti-virus programs
- Back your data up on hardware connected to the system temporarily for the back-up task, back-up best on DVD (for protection against ransomware)

Digital Self-Defence is the ability to constructively overcome the challenges faced in the complex media landscape.

The measures listed are intended to enable pupils, teachers and students to use digital media responsibly and appropriately. In this way, the opportunities offered by digital transformation are harnessed, while at the same time risks are minimised in order to preserve personal freedom.

One-hundred percent security unfortunately doesn’t exist, but with a clear understanding, anyone can open up new opportunities! Note the reference under (6)!

This compass was created using Linux/DarwinOS and LibreOffice. The research was done through the Firefox browser with the add-ons “NoScript”, “HTTPS Everywhere” and “Privacy Badger”. The content creation was coordinated using gpg-encrypted email.

Special Tips:
- Custom installation
  - available data protection options (e.g. advertising ID, typing behaviour, userapp logging)
  - local accounts (no Microsoft account)
  - third party apps (e.g. browser, email)
  - test installation of telemetry (basic, but cannot be completely disabled)
- Consider deactivation guides for:
  - Cortana, speech recognition, connection and error reporting, cloud services for data storage
  - Check configuration after update!

Digital Self-Defence – Fundamentals – Digital Self-Defence

(2a) Internet Browsers
Browsers know a lot about you and are the “door to the internet”.

Tips for Basic Security:
- When choosing a browser, consider minimal data configuration, expandability, and updateability https://www.mozilla.org/en-US/docs/

- Set the startpage and new tabs to a local site or an empty page (about:blank)
- Block access to location data (WLAN, IP, GPS)
- Do you know about open app downloads through F-Droid?

- Block access to location data (WLAN, IP, GPS)
- Do you know about open app downloads through F-Droid?

- Block access to location data (WLAN, IP, GPS)
- Do you know about open app downloads through F-Droid?

- Block access to location data (WLAN, IP, GPS)
- Do you know about open app downloads through F-Droid?

Watch out! Configure settings as required and be wary of updates, check uncertainties of settings after an update

Unset the environment variable SSLKEYLOGFILE
https://developer.mozilla.org/

- Use the add-on for Firefox: Key Log Format (Nov 19)

(3) Apps
Apps know all the data they have access rights to.

Tips:
- Check app accesses and connections before use e.g. https://www.privacy.gov-au.org/
- Configure apps to be data-lean
- Prefer native apps (need-to-know)
- Block access through app settings on phones (e.g. the microphone, camera, memory)
- Use e.g. Blakada to block trackers

Block access to location data (WLAN, IP, GPS)
- Do you know about open app downloads through F-Droid?

- Block access to location data (WLAN, IP, GPS)
- Do you know about open app downloads through F-Droid?

- Block access to location data (WLAN, IP, GPS)
- Do you know about open app downloads through F-Droid?

- Block access to location data (WLAN, IP, GPS)
- Do you know about open app downloads through F-Droid?

Watch out! Avoid apps with a permanently activated microphone and camera in class, they record you and your surroundings, are disturbed by acoustic noise, or reveal personal messages!

(4) Search Engines
Most search engines also search for you.

Tips:
- Do you know these search engines?
  - lite.quotant.de
  - MetaGer.de
  - YaCy.net
- Take a look https://htmlspec.org/
- Do you know the search queries and active search suggestions you reveal information about yourself (profiling).

Do you know the children’s search engine?
- blinde-kuh.de – Free of analytics for special protection of children (Jun 2016)
- qwantJunior.com (Jul 2016)

Important: Searching directly is recommended, through third-parties there are often personalised results.

Pay attention to updates!

(5) Email
Emails are electronic postcards, which can be read by anyone, unless you do something about it.

Tips:
- Interested in secure email providers? Find information e.g. here: https://secureemail.org/
  - Do you know about extra email programs with encryption (e.g. Thunderbird with Enigmail)? see https://open-std.org/
  - Always display the long email header and check the email addresses
  - Use a data-lean virus-scanner
  - Use only official email for official purposes, no relaying, check incoming mail
  - Recommended: No automatic loading of images and opening of links in the web browser, no HTML emails.
School Website (6)
With your website you assume responsibility for IT security and data protection for yourself and your users.

**Tips:**
- Use native fonts, translation and reading services.
- Specify and adhere to deletion periods for stored data.
- Check for present, unwanted analytical functions of software.
- Use opt-in rather than opt-out.
- Use IP address anonymisation at the meta level.

Test your website at PrivacyScore.org web.koll.datastydd.net, sslabs.com/safest

Research (8)
Social Networks, Chat, Messenger, Navigation Services

Social networks know you, your friends and contacts. Navigation services know your location and destinations. They want your data.

**Tips:**
- Do you know about decentralised, open source based social networks e.g. from the Fediverse?
- Recognise and block access and tracking techniques e.g. by web fonts and APIs, use tools such as (2a), (2b) and (4) i.e. Google Bigbird, webkoll.datastydd.net for recognition and Blockata for prevention.
- Do you know examples for data-dean messengers e.g. Jabber/XMPR, see e.g. Conversational (or IRC clients) (XChat?) see in https://www.jabber.org/, https://xmpri.org/website/admindocs.html or email server networks (chat over email) e.g. https://www.bigbird.de/.
- Activate end-to-end encryption (E2EE)

Internet Gateway/Firewall (9)
The gateway is the door to the internet and the last line of defence for the user’s systems.

**Tips:**
- via DNS you can hide unwanted services, therefore configure and run your own DNS server or one from a provider, no third-party providers, encrypt DNS (DNS over HTTPS).
- Use a separate server (e.g. Windows)
- Configure and use firewalls to filter network traffic.
- Configure and run intrusion prevention systems to help protect against malicious code.
- Check and configure app accesses e.g. with exodus-privacy.eu.org (accesses to smartphone services)

Password (9)
Passwords are an important measure to ensure the digital identity.

**Tips:**
- Use long passwords (at least 10 characters) which include special characters/numbers and avoid common words.
- Use each password for one service/account only.
- Create and memorise a secret sentence and build the password from it using e.g. the first letters and numbers, for example: ‘In Spain in 2018, Jane had a blue swimsuit with 17 stripes and 8 spots.’

Consequences
Privacy-by-Design actively supports sustainability! Reduce energy costs by blocking and code reduction. If Privacy-by-Design is not implemented, there will be direct and significant consequences.


Already in use: Influencing your sovereignty, e.g. not to go to voting https://www.fbi.gov/news/stories/2019/0603/fbi-release-2019-intelligence-

dynamic, personalised pricing.
- profiling.
- Neurmarketing.
- Behaviour-based marketing.
- Algorithmic decision-making.
- People’s creditworthiness.
- Personalised pricing.

“Best suited are the products where the buyer has no idea about a reasonable price.”

Office Applications (10)
Office applications know all the data they process.

**Tips:**
- Do you know any locally installed open source applications? e.g. see in https://www.wikipedia.org/wiki/List_of_free_and_open-source_office_software_packages
- LibreOffice
- GIMP
- Use local native spelling and translation support.

Check privacy conditions of cloud-based applications with subscription models (e.g. Office 365) and Microsoft Office.

“...When you shop, your data may be the most valuable thing for sale...”
https://www.wired.com/story/mac-app-store-publishers-security-

...“...The regulatory authorities may well intervene...”
https://www.zdnet.com/article/regulatory-authorities-will-intervene-in-cloud-sector/...“...My sister always gets ten times the number of points, so why don’t I?...”

Note
The links given are deliberately printed in small print and should be looked up digitally.