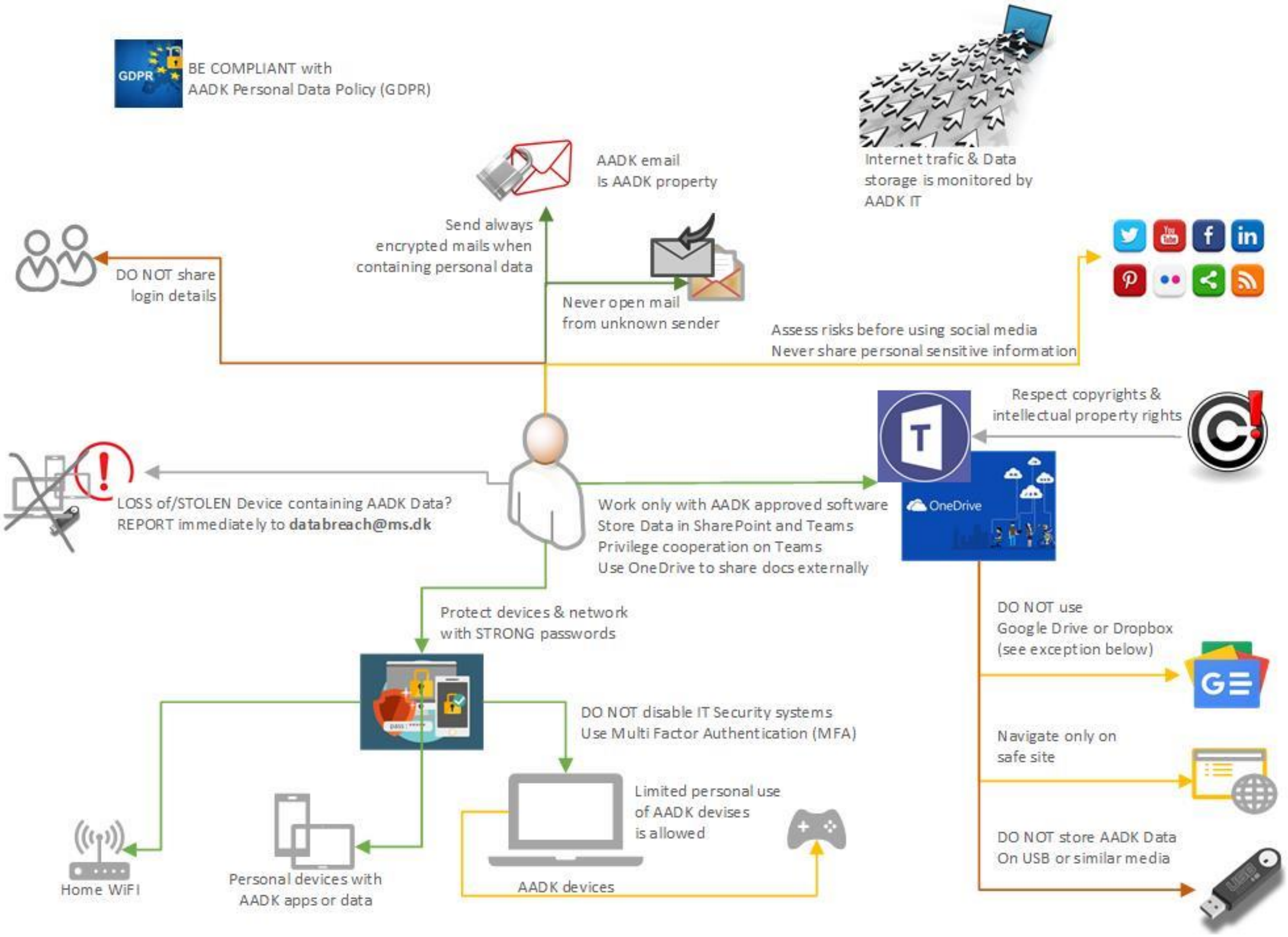
Staff IT Security Policy

This section is part of AADK general IT Security Policy and describes the policies that AADK employees are expected to follow when using the IT systems.

IT Security – staff compliance at glance



These policies are mandatory, and any violation may lead to disciplinary sanction.

1. Users ID and device

- All user accounts are considered strictly personal and logon details may not be shared with anyone, no matter the reason or context.
- Passwords on AADK devices must be changed every 90 days.
- All mobile devices must be protected with a password and encrypted storage, to protect lost devices from leaking AADK data. Log on AADK devices and apps must be confirmed with Multi Factor Authentication (MFA). This also applies for BYOD devices that are given access to AADK data, such as private smartphones and tablets that connect to a users' AADK mailbox and apps.
  This is enforced using a mobile device policy in Office365 Exchange (see section 8 for details).
- All stolen or lost laptops must be reported to the email 'databreach@ms.dk' and AADK Service Desk immediately. The Service Desk will take steps to render the device inoperable and protect AADK data.

- Any software not provided nor pre-installed on AADK device must be approved by AADK Service Desk prior to installation. After obtaining approval, users can elevate their privileges to perform software installation themselves. Games, pirated software or other software downloaded from the Internet is not allowed.

2. Usage and cooperation

- Users are not allowed to tamper with or disable IT security systems such as antivirus systems and software updates.
- All users are expected to have read, understand and follow the published GDPR guidelines on inSight i.e. *AADK Personal Data Policy*, in all aspects of their work.
- Users are committed to participating in trainings related to IT security and Data protection, to determine what ‘sensitive information’ is, and are expected to comply with AADK IT Security Policy and guidelines on sensitive information.
  It is explicitly forbidden to share sensitive information on social media of any kind; and it is a requirement to encrypt such information when communicating them out of ActionAid
  Employees are responsible for deleting any personal data from the storages they are responsible for (Outlook, folders on Teams and SharePoint and such) when they do not need them anymore; they are committed to reviewing stored personal data once a year and apply deletion in accordance with *AADK Personal Data Policy*.
- Users must not use AADK or AA e-mail or any other organisations’ communication means to represent, give opinion, or otherwise make statements to external parties on behalf of AADK or AA, unless it is part of own job/role description or appropriately authorised to do so.
- Social media and communication apps are for most of AADK employees essential in their work. While AADK acknowledges this need, users must assess and mitigate risks before using such media, and never share personal sensitive information on non-safe media. AADK will share on intranet (Teams and SharePoint) recommendations of communication apps on an on-going basis.
- Limited personal use of AADK computers is allowed, and such use is governed by the *Code of Conduct* published on AADK intranet. It is strictly forbidden to navigate on sites, upload, download or store any data that violate international, national, or local laws and regulations. Users are expected not to use for personal use resource-heavy means like streaming, international call and such that could choke up our limited technical capacities (e.g., storage or bandwidth).
- The AADK corporate email is AADK property, and users are encouraged to **not** use AADK emails for private use. So is file storage: all files and folders are AADK property; if users need to store confidential business files, they may use the Personal Documents on their OneDrive; there, they are also allowed to create a Private folder to store private files that do not conflict with AA Code of Conduct.
- Users are not allowed to create rules or scripts to automatically forward e-mails located on the internal AADK and AAI system to external e-mail services like yahoo or g-mail.
- AADK users must respect any copyright and intellectual property rights.

3. Data storage

- AADK data may only be saved on the systems provided and managed by AADK IT.
  Microsoft Teams and AADK SharePoint are the preferred cooperation platforms across the federation and within AADK.AADK employees may invite external users within Teams to cooperate on projects; if external users have or obtain access to personal information, they should commit to AADK confidentiality clause.
- It is normally forbidden to store any AADK-related data on cloud storage services such as Dropbox, Google Drive, Amazon drive, or any other service not provided by AADK IT. However, if some of our partners propose a safe solution (e.g. professional Google space) to share or store AADK data, and such sharing is required to cooperate with these partners, AADK employees may use these communication and storage means under condition of *AADK Personal Data Policy* incl. having a confidentiality clause and deleting data after use.

- It is not allowed to store AADK data on USB devices, unless these are handed out by the AADK Service Desk, clearly marked with AADK name, used for temporary transfer of data, and cleaned afterward.
- It is not allowed to insert/use USB sticks obtained (or found) elsewhere into AADK computers.

4. Monitoring and IT/Management access to data

- Internet traffic and usage will be monitored to detect and counter threats from potential sites or IP-addresses that are identified as high-risk addresses (e.g. non-secure download, forbidden addresses, fish or spam sender and such).
- AADK storages are regularly screened to identify personal data that need to be deleted; screening includes mails and files in Outlook and SharePoint.
- AADK management reserves the right to access a user’s corporate mails and files as well as browsers and traffic history when deemed necessary in case of long-term absence or when the employee is no longer under AADK employment. The decision to apply this access right rests with the Head of PSD.
  AADK Management and the Compliance Manager reserve the rights to access user’s corporate mails and files as well as browsers and traffic history or any other data, or to seize user’s AADK devices, if needed for an administrative investigation. The decision to apply these rights rests with the Operations Director.

If a user is in doubt about any of the above provisions, the AADK Service Desk will provide specific guidance upon request.