EPB0056

# Written evidence submitted by Socrates Software Ltd

## Summary of common fears/problems with tech in prisons and how they are mitigated

| Fear/problem | Mitigation |
|---|---|
| Unrestricted internet access | Providing multiple layers of security, both at the device and network level, to ensure that access is provided only to authorised content.<br><br>This can be through a combination of access controls on the device/network, firewalls, and through the use of secure proxy services. Using an end-to-end solution where the end-user device/software securely accesses controlled, authorised content increases security over simple 'whitelisting' approaches. |
| Access to social media sites (Facebook etc.) | Through the use of restricted content delivery from the network, network access controls, firewall rules and web proxies where appropriate, all access to social media sites can be effectively prevented, whereby the only content accessible is via a closed system, or a closed system with only authorised sites allowed. The use of special security software on devices can also help by making it impossible to access any kind of unrestricted browsing activity. |
| Access to witnesses & victims | All communication with the public / families etc. should pass through appropriate security controls, subject to the risk level assessed. This can include requiring pre-authorisation of contact with family members before messages/calls can be initiated. |
| Accessing illegal material | Along with appropriate network security, devices should be locked down such that they can only access authorised networks/access points, to prevent them being used with public networks or other unauthorised access points that may be present. |
| Communication with gang members outside | In addition to requiring communications to be pre-authorised, messages or calls should be recorded and/or monitored; this can include requiring messages to be reviewed by staff before they are sent, flagging messages for review when certain keywords are found, or using systems to monitor which prisoners are communicating with who, for intelligence gathering purposes. |
| Communication with prisoners in other prisons | Systems can be set up to automatically detect and flag messages that appear to have been relayed from one prisoner to another in a different prison, by checking inbound messages against previous outbound messages. By using systems and software which has been designed specifically for prisons, the use of potentially vulnerable websites or web services that could allow prisoners to leave messages to be ready by others, can be avoided. |
| Passing secret messages to other prisoners | Using secure, locked down devices with software/applications that have been designed for prisons can help ensure that data stored on the device is secure and tied to a particular user profile. Allocating each prisoner with their own secure account and ensuring that device software restricts access to this account and its data, ensures that content, data and messages created by one prisoner cannot be accessed by another, even if they have physical access to the same device. In cases where collaboration is desirable and prisoners need to communicate with each other, this can be achieved through messaging services which include appropriate security controls and auditing. |
| Taking photos/recording video with devices | Ensuring the use of appropriate device management software that has been designed specifically for the security requirements of prisons means that access to cameras and video recording can be either completely deactivated, or restricted to certain access requirements. This may include allowing the camera to be used for certain applications, and ensuring that any images are securely stored such that an prisoner cannot access them / post them online. |
| Reconfiguring devices to bypass security | Specialist device management systems can be used that securely lock down a device to a chosen configuration, preventing prisoner access to settings and configuration. In addition, where these systems have been specifically designed for use in prisons, they can include features such as tamper detection, prevent connection of external peripherals (e.g. USB), restrict access to external storage (e.g. SD cards) and prevent the ability for devices to be factory reset. |

| | |
|---|---|
| Accessing Wi-Fi access points via illicit devices | Appropriate network security can be used to prevent illicit devices from connecting to Wi-Fi access points. Combining this with appropriate server software which will only deliver authorised content to recognised devices means that even if an illicit device were to bypass network security restrictions, it cannot gain access to any content or services. Some specialist Wi-Fi access points can also provide information about illicit devices which are attempting to make connections, providing valuable intelligence to track down their location. |
| Accessing internal networks | Networks and access points can be configured such that staff networks and prisoner networks are kept completely separate; this prevents any chance of prisoner devices being able to access staff systems. Device-level and network-level controls such as device lockdown software (restricting to specific networks), client certificates, certificate pinning and firewalls can provide further security. |
| Devices being broken/smashed/used as a weapon | Ruggedised cases can be provided to protect devices from accidental / everyday damage. Generally, the more valuable the device is to an prisoner in terms of providing useful content/services and facilities such as the ability to message their family, the more care that will be taken and less instances of deliberate damage. |
| Tech will replace staff (corrections officers or teachers) | Prison staff and teachers can sometimes be anxious that tech is being introduced to replace some or all of their role. This can be mitigated by including staff stakeholders in the planning process and ensuring that what is being delivered via the tech will help improve the lives of staff as well as prisoners. For prison staff this can include providing ways of reducing labour intensive tasks, improving communication between staff and prisoners, automating requests / paper processes. For teachers, implementing content that provides a blended learning approach should enhance classroom time by allowing prisoners to study topics in their own time, reinforcing classroom-led study and freeing up time in the classroom to tackle questions and gaps in understanding. In addition, teachers can be provided with a valuable tool to track progress and understanding, and provide additional study materials to learners including assignments, revision, past papers or background reading material. |
| Prisoners will become violent/frustrated during outages | By choosing appropriate systems that have been designed for use in prisons, where connectivity can be challenging, incidences of outages can be avoided, whereby the system continues to operate offline, even if connectivity is lost for a period of time. Allowing prisoners to continue to use the content they have downloaded to their device even whilst offline will eliminate or reduce levels of frustration. |

**Summary of ‘best case’ solution functionality (applicable globally)**

- Devices which are as close as possible to the actual devices prisoners are likely to use and encounter after release, to help improve digital skills
- A combined offering of offline and online materials, by providing a curated collection of downloadable content that prisoners can download to their device and use offline, along with online content that may include approved websites which may either be external or intranet sites within the local environment
- Use of specialist device lockdown and management software, designed specifically for prisons (off the shelf solutions are generally not secure enough)
- Use of devices with sufficient capacity to support learning and offline materials
- Solution that works both offline and online so that it can continue to be used without connectivity
- Flexible solution that allows working in partnership with national and local providers to deliver appropriate content
- Ability to support and deliver interventions/programmes
- Work with employers/industries to deliver vocational learning
- Ability to support the use of 3rd party apps
- Supports blended learning, allowing self-guided study
- Provides the ability for devices to be purchased / taken into community on release and converted into a ‘standard’ device
- Allows prisoners to take their certificates, CV, etc. into the community
- Provides continued support after release through a community app to be used on user’s own smart device
- Can support staff functions as well as prisoner functions
- Option to provide specialised devices containing content or apps specifically for visitors, healthcare, etc.
- Customisable to needs of specific facilities / regions
- Allows programme providers to supply digital content to prisoners
- Can integrate with offender management systems
- Can improve prison efficiency with automated forms, requests, etc.
- Use of secure devices and systems that have been specifically designed for use in corrections
- Appropriate level of penetration testing of devices and systems, with associated documentation and risk assessments
- System can be easily updated remotely to support additional functionality or content over time

- Secure messaging services that allow prisoners to communicate with family and friends, maintaining family ties and their external support network; whilst providing appropriate security controls for prison staff to be able to monitor/block communications where required.
- Ability for prisoners to make voice and/or video calls from a device
- Option for facilities to take a managed service offering, whereby device hardware is delivered pre-configured, ready-to-use, requires no on-site infrastructure (beyond Wi-Fi connectivity), and replacement hardware is swapped out as and when required.
- Device management service, where service provider manages device configuration, upgrades, content and configuration changes remotely on behalf of the facility.
- Reduction in prison administration/overheads by automating common processes/workflow, replacing paper requests, or by providing ability to enter case notes on the go via staff devices.