

Impero Product Privacy Notice

Table of Contents

Who are we and what do we do?	1
How this Privacy Notice applies to you	2
Who is responsible for the personal data which Impero processes?.....	2
What personal data do we process?	2
Our Products.....	3
How Impero obtains this information:	4
Why do we need to process this data?.....	4
Security of personal data.....	5
Where we store and process customer data?.....	6
How long does the Impero Group keep customer personal data for?.....	6
Applicable laws.....	6
Cookies.....	6
Your rights.....	6
How to contact us	7
Notification of changes	7

Who are we and what do we do?

The Impero Group is a group of subsidiary companies of Impala Bidco and forms part of the Impero and Netop companies as defined in our Company Structure available at www.imperosoftware.com/policies-terms (referred to herein as “Impero”, “us”, “we”, “ours”).

Impero provides various Services and Products as outlined below, to organisations across the globe which may involve the collection, use, sharing, or other processing of personal data. Our Services provide organisations (our “Customers”) with a secure and user-friendly way to monitor and manage the internal working of computer devices and how those devices are used by individuals operating under the control of the Customer (“Users”) and various individuals affiliated with a Customer (“Subjects”). Some of our Services also offer the ability to store, review, flag and analyse concerns pertaining to a Subject’s physical and mental wellbeing that is observed away from a computer device, or indicated by the Subject’s device usage. These Services are frequently used by Customers to support Subjects who are children or youth in their care. Some of Impero’s Services provide a contextual background and an ability to link concerns to device usage so that Customers can comply with their legal obligations, where those exist, of safeguarding Subjects who are children or young adults.

PUBLIC

We respect and value the privacy of our Users and their Subjects and will only collect and use personal data in ways that are described within this Notice, in a way that is consistent with our obligations and their rights under the law.

How this Privacy Notice applies to you

This Product Privacy Notice provides information on how we collect, use, share and otherwise process the personal data of Users and Subjects while they are using our Services.

This Privacy Notice applies to you if you are identified as a User or a Subject to our Services. This may include where your organisation is our Customer and has purchased one of our products to safeguard, monitor or otherwise support you.

If you are a User and would like to know more about how we process your personal data when contacting us or during a purchasing of a product or service, please visit our Website Privacy Policy at www.imperosoftware.com/policies-terms

Who is responsible for the personal data which Impero processes?

When providing our Services, Impero acts as data processor on behalf of its Customers. Customers are responsible for providing appropriate privacy notices to Users and Subjects whose data they provide to us, explaining how their personal data will be processed and their rights in relation to it. Customers who provide an Impero entity with sensitive categories of personal data need to comply with additional requirements under the local data protection laws of the territory in which they reside.

When you use an Impero Service provided by your organisation, Impero's processing of your personal data in connection with that Service is governed by a contract between Impero and your organisation. Impero processes your personal data to provide the Service to your organisation and you; we act on our Customers' instructions in relation to the processing of personal data.

We will comply with legal obligations in each territory where we provide services which are applicable directly to processors, including implementing appropriate technical and organisational measures to ensure the security of the personal data.

When processing personal data, Impero takes appropriate legal advice to ensure compliance with all applicable laws. Impero is ISO27001 certified, which is a globally recognised information security certification requiring robust security practices.

What personal data do we process?

Our Customers have choices when it comes to the technology they use and the data they share. When a Customer is asked to provide personal data for Users or Subjects, they can decline. Our products require some personal data to operate and provide the service. If a Customer chooses not to provide data required to operate and provide them with a Service, they cannot use that service. Likewise, where we need to collect personal data by law, or to enter into or carry out a contract with a Customer, and they do not provide the data, we will not be able to enter into the contract; or if this relates to an existing service the Customer, User or Subjects are using, we may have to suspend or cancel it. We will notify the Customer who in turn should notify Users and Subjects if this is the case at the time.

PUBLIC

Where providing the data is optional, and a User or Subject chooses not to share personal data, features like personalisation that use the data will not work. In some instances, a Customer will have legal obligations which require that certain data is processed. The data we collect depends on the context of interactions with Impero and the choices Customers and Users make, the products, services and features used, location, and applicable law.

The information collected by Impero varies by Service and by Customer, based on the specific implementation and selected usage. Each Impero Service may collect common information about devices, Users and Subjects. The type of information collected on Users and Subjects may include (Services Data):

- Name and contact data
- Subscription and licensing data related to their account
- Device and usage data. Data about their device and the product and features being used, including information about hardware and software, how our products perform as well as device settings.
- Location data. Preferred language. Location can also be inferred from IP address.

Depending on a Customer's choice of Product and type of integration, we may process the following special categories of information about Subjects on behalf of our Customers (Special Category Data):

- Personal data revealing racial or ethnic origin
- Data concerning health
- Data concerning a person's sex life
- Data concerning a person's sexual orientation
- Personal data revealing political opinions
- Personal data showing religious or philosophical beliefs

For certain products, our Customers use this additional demographic data to better support the Subjects in their care. Subjects are often children and young people. Schools and educational establishments in particular have a legal obligation to safeguard and monitor their students. Some of our products use this special category data to provide contextualised information, facilitating this legal obligation.

Our Products

- **Impero Connect:** allows organisations to remotely access and control computer devices across a network and/or across the internet. This can be cloud-based or hosted. Impero Connect processes Services Data, content of screen or display, and individual entered text (chat).
- **Netop LiveGuide:** a live chat tool for websites that provides text, audio and video communication between individuals. Netop LiveGuide processes Services Data and individual entered text (chat).
- **Impero Wellbeing:** software to capture, record and identify signs of harmful online behaviour. Users can highlight and prioritise Subjects of concern. This requires the processing of Services Data, contents of screen or display, as well as some Special Category Data which may be processed as part of screen captures which document device usage.
- **Impero Webcheck:** robust internet filtering which analyses content in real-time to ensure Subjects are protected online. This is a solution powered by our partner, Netsweeper. This requires the processing of Services Data as well as some Special Category Data. You can view Netsweeper's Privacy Notice at www.netsweeper.com/privacy-policy.

PUBLIC

- **Impero Classroom:** software which makes it easy to monitor and manage student activity on classroom devices. This requires the processing of Services Data, contents of screen or display, and individual entered text (chat).
- **Education Pro:** combines learner wellbeing and device management to enhance digital learning, support IT administration, manage classroom device usage, and monitor safeguarding issues effectively. Education Pro offers a range of hosting options and built-in cross-platform technology. This requires the processing of Services Data, contents of screen or display, and individual entered text (chat). Special Category Data may be processed as part of screen captures documenting device usage, and user entered data providing demographic information on individuals.
- **Edlink:** The EdLink software is a third party solution which collects information around the location of the device and any applications used as part of the normal use of the solution. The purpose of this data is to recover lost devices and perform control & monitoring functions on the target devices. This is powered by Mobile Guardian, their privacy policy can be found here: <https://www.mobileguardian.com/privacy-policy/>.
- **Impero Backdrop:** a school safety solution, allows schools to record, manage and track student mental health and safety concerns at any time. This requires the processing of Services Data. Special Category Data may be processed when a Customer has linked to an organization's Management or Student Information System (MIS or SIS), or when a User enters such data manually. This information allows us to contextually provide safeguarding services.
- **Netop Vision** (including Netop Vision Pro, Netop Vision 365, Netop Vision for Chromebooks): software which makes it easy to monitor and manage student activity on classroom devices. This requires the processing of Services Data, contents of screen or display, and individual entered text (chat).

How Impero obtains this information:

As outlined above, we process data on behalf of our Customers in order for us to be able to provide our Products and Services to them. Depending on the Product, data may be captured directly from a device registered with a Service. Customers and Users add data to our systems manually or may authorise the linking of another system such as a Management Information System (MIS), Student Information System (SIS), or other registration system to feed data into our systems automatically.

Our systems can be utilised without Special Category Data. It is up to our Customers to decide what personal data is processed by choosing which data to enter manually and what their preferred method of integration is.

Why do we need to process this data?

We rely on a variety of legal reasons and permissions (sometimes called "legal bases") to process data, including with your consent (where you are a User), a balancing of legitimate interests, necessity to enter into and perform contracts, and compliance with legal obligations, for a variety of purposes described below.

We use personal data to:

- **Provide our products**, which includes updating, securing, and troubleshooting, as well as providing support. It also includes sharing data, when it is required to provide the service or carry out the transactions our Customers request and supporting our Customers in fulfilling their legal obligations. The data we process allows us to provide our Customers with a rich

PUBLIC

and interactive experience. For example, our Wellbeing Product will process personal data obtained from a school's MIS system and link this with any newly logged concerns. This allows some of our Customers to fulfil their legal obligations and safeguard children in their care.

- **Managing your account.** This includes troubleshooting, any patchwork and bug fixes.
- **Improve and develop our products.** We use data to continually improve our products, including adding new features or capabilities. For example, we use error reports to improve security features, usage data to determine what new features to prioritise.
- **Personalise our products and make recommendations.**
- **Legal compliance.** We process data to comply with law. For example, we use the age of our customers to ensure we meet our obligations to protect children's privacy. We also process contact information and credentials to help customers exercise their data protection rights.

When you use an Impero Product with an account provided by an organisation you are affiliated with, such as your work or school account, that organisation can:

- Control and administer the Impero Product and Product account, including controlling privacy-related settings of the Product or Product account.
- Access and process your data, including the interaction data, diagnostic data, and the contents of your communications and files associated with your Impero Product and Product accounts.

Where your organisation provides you with access to Impero Products, your use of the Impero Products is subject to your organisation's policies. You should direct your privacy inquiries, including any requests to exercise your data protection rights, to your organisation's administrator.

Security of personal data

Impero is committed to protecting the security of personal data. We use a variety of security technologies and procedures to help protect personal data from unauthorised access, use or disclosure. For example, we store personal data on computer systems that have limited access and are in controlled facilities. We never transmit personal information, and in the rare occasion we would need to do so, this is encrypted.

We enter into contractual agreements with all Customers and any service providers which include robust data protection and security measures. These include Data Processing Agreements and the incorporation of Standard Contractual Clauses.

Only a selected number of Impero's staff have access to view data about Users or Subjects held in our Services. Access is granted on a need-to-know basis solely as necessary in relation to providing Services for the relevant Customer. All staff with access to personal data undergo background screening before they can access personal data. Every access or attempt to personal data is logged and actively monitored.

We may from time to time outsource development, but under no circumstances are outsourced developers able to access personal data.

Where we store and process customer data?

If your organisation has chosen an on-premise Product, all personal data is hosted on your organisation's servers, we do not have access to these.

For our cloud and hosted Products, the storage location is typically the Customer's region or the closest possible instance if the law allows us to do so. For example, data from UK based Customers, their Users and Subjects is kept in the UK, and data for US based Customers, their Users and Subjects is kept within the US.

We use third parties, currently Microsoft Azure and Amazon Web Services, as our standard hosting providers. We maintain hosting instances in a variety of countries. For a full list of the countries where hosting instances are available please contact the Impero sales team .

How long does the Impero Group keep customer personal data for?

Impero retains personal data for as long as necessary to provide the products and fulfil the transactions you have requested, and for other legitimate purposes such as complying with our and our Customers' legal obligations, resolving disputes, and enforcing our agreements. Because these needs can vary for different data types, the context of our interactions with you or your use of Products, actual retention periods can vary significantly. After termination of a Customer's contract with us, all of their Customer, User and Subject personal data is destroyed. Customers are provided the option of retrieving their data from our systems before it is destroyed.

Applicable laws

By default, Impero complies with the privacy laws of England and Wales regarding the collection, use, and retention of personal information. In addition, we comply with the laws of the European Union (the GDPR) which form the basis of many worldwide data protection laws, and we strive to take legal advice before selling into a new territory to ensure we comply with locally applicable data protection laws.

Cookies

Our Services may use cookies. Cookies allow Impero to recognise your device and store some information about your preferences or past actions. This helps us to provide you with a good user experience when you browse our website and also allows us to improve our site. For detailed information on the cookies we use and the purposes for which we use them see our Cookies Policy available at www.imperosoftware.com/policies-terms.

Your rights

In certain circumstances, where we are controller, you may have certain rights relating to your personal data, subject to local data protection laws. We may direct you to the controller of your personal data where we are not the data controller. Depending on the applicable laws these rights may include the right to:

- Access your personal data held by us
- Know more about how we processed your personal data
- Rectify inaccurate personal data and, taking into account the purpose of processing the personal data, ensure it is complete

PUBLIC

- Erase or delete your personal data (also referred to as the right to be forgotten), to the extent permitted by applicable data protection laws
- Restrict our processing of your personal data, to the extent permitted by law
- Transfer your personal data to another controller, to the extent possible (right to data portability);
- Object to any processing of your personal data. Where we process your personal data for direct marketing purposes or share it with third parties for their own direct marketing purposes, you can exercise your right to object at any time to such processing without having to provide any specific reason for such objection
- Opt out of certain disclosures of your personal data to third parties
- If you're under the age of 16, opt-in to certain disclosures of your personal data to third parties
- Not be discriminated against for exercising your rights described above
- Not be subject to a decision based solely on automated processing, including profiling, which produces legal effects ("Automated Decision-Making"). Automated Decision-Making currently does not take place on our websites or in our services and
- Withdraw your consent at any time (to the extent we base processing on consent), without affecting the lawfulness of the processing based on such consent before its withdrawal.

If your data has been submitted to us by or on behalf of an Impero Customer and you wish to exercise any rights you may have under applicable data protection laws, please inquire with them directly. If you wish to make your request directly to us, please provide us the name of the Impero Customer who submitted your data to us. We will refer your request to that Customer, and will support them as needed in responding to your request within a reasonable timeframe.

How to contact us

The Impero Group has appointed a Data Protection Officer. You can send any questions or requests regarding Impero's use of your personal data to dpo@imperoftware.com.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

Notification of changes

We reserve the right to amend or vary this document from time to time to reflect evolving legal, regulatory, or business practices. When we update our privacy policy, we will take appropriate measures to inform you, consistent with the significance of the changes we make (which, for minor changes, may include posting the revised statement to our site with immediate effect). Please check this page periodically for changes. We will obtain the appropriate consent to any material changes if and where this is required by applicable data protection laws.

Last revision: 16 March 2022

Responsible: Jenny Kyurkchieva, Data Protection Officer