itslearning & GDPR

A summary of what data we process, your rights as a customer and how data protection is built into our development processes.

Introduction

Terms used in this document:

In general, the terms and concepts used in this document have the same content and meaning as those found in the General Data Protection Regulation (GDPR).

- *Data controller* – the itslearning customer, meaning typically a school, university, district or municipality.
- *Data processor* – itslearning
- *Data subject* – a natural person, in this context an itslearning user

itslearning as a Data Processor

For the cloud services we provide to our customers and their end users, itslearning is what both existing and new EU regulation define as a Data Processor. As a Data Processor we do not decide the purpose or lawfulness of the processing, we merely process data on our customers' behalf. The GDPR regulations force stricter requirements upon all processors of data. We will fully comply with these requirements for all of our services, including itslearning.

Itslearning does not independently obtain user data to our services. User data can either be submitted to the platform by customers' representatives, through an integration with a third-party system, or in some cases by the users themselves. Most commonly, personal data in itslearning comes from student information systems under the control of our customers. We only import data from third-party systems on the instruction from our customers.

Further details on role and responsibilities of the Data Controller and Data Processor can be found in the DPA (Data Processor Agreement). This, and more information about itslearning and GDPR can be found on our website (https://itslearning.com/global/gdpr).

Details of personal data being processed

Which data is collected and how it is processed in itslearning, depends on how our customers use our system. This document contains a general description. The DPA can be updated to contain a specific description for each customer if needed.

Data subjects

In itslearning, data subjects fall into one of four groups:

1. Staff (teachers, administrators, assistants…)
2. Students
3. Parents
4. External people given access by the customer (examiners, …)

Collection and processing of data

itslearning as Data Processor is processing personal data received via the itslearning platform, on the hosted service for the customer and applications from partners and on the website

(http://www.itslearning.com). Processing is done on behalf of the Data Controller for the following purposes:

- Providing the Services in accordance with existing agreements
- Providing basic and technical support related to the Services in accordance with the Data Processor Agreement and the Service Subscription Agreement
- Maintenance, ensure security, analyse or evaluate how well the service works

The duration of processing is the term in the Subscription Agreement plus the period from the expiry of the term until deletion of all Customer Data by Data Processor in accordance with the term.

Categories of personal data

The information that may be submitted to itslearning about a data subject (depending on how a customer has chosen to configure and implement the service) falls into several categories, these are given below with some examples of each:

Category	Examples
Personal information (contact information)	- User name - Email - Phone number - Contact details of parents or guardians - IP-addresses - Activity logs
Communication	- Messages (IM / Old messages) - Discussion (could also be considered a student response or course material) - Bulletins + comments
Course material (produced by user in context of teaching)	- Assignment - Test - Note - Uploaded document
Assessments (given by teacher to student)	- Assessments (grades, descriptive feedback) - Attendance comments - Behaviour comments
Calendar entries	- Events
Student responses	- Answer to assignment (including uploaded files) - Test attempt - Crossword answer
Internal logic	- Last used selection in dropdowns some places - Personal settings: language, simplified tree structure, accessibility ++ - Cookies

How to satisfy the right of the data subject

Roles and responsibilities

All requests should go from the data subject to the Data Controller, who in turn may or may not use our functionality or ask itslearning for help to exercise the right for the itslearning platform. **Each individual request needs consideration and processing before action is taken.** The rights of the data subject are described in Chapter 3 of GDPR (https://gdpr-info.eu/chapter-3/). These rights are not absolute, and should be processed in the context of both GDPR and local regulations.

Please note that according to GDPR there are exceptions to exercising the rights of the data subject when the data is considered necessary…

- … to exercise right of freedom of expression and information of other data subjects
- … to comply with legal obligations or the performance of a task carried out in public interest
- … for archiving, historical or statistical purposes

Under GDPR, the data subject rights are between him and the Data Controller. Any data subject requests from end users to itslearning will be handed over to the customer. itslearning will cooperate in good faith with customers to ensure they can exercise the rights of the data subjects in a prompt manner.

In addition to administrative and other functionality already available in the itslearning system, the itslearning DPO and our service team are available to help our customers as Data Controllers satisfy the right of the data subject.

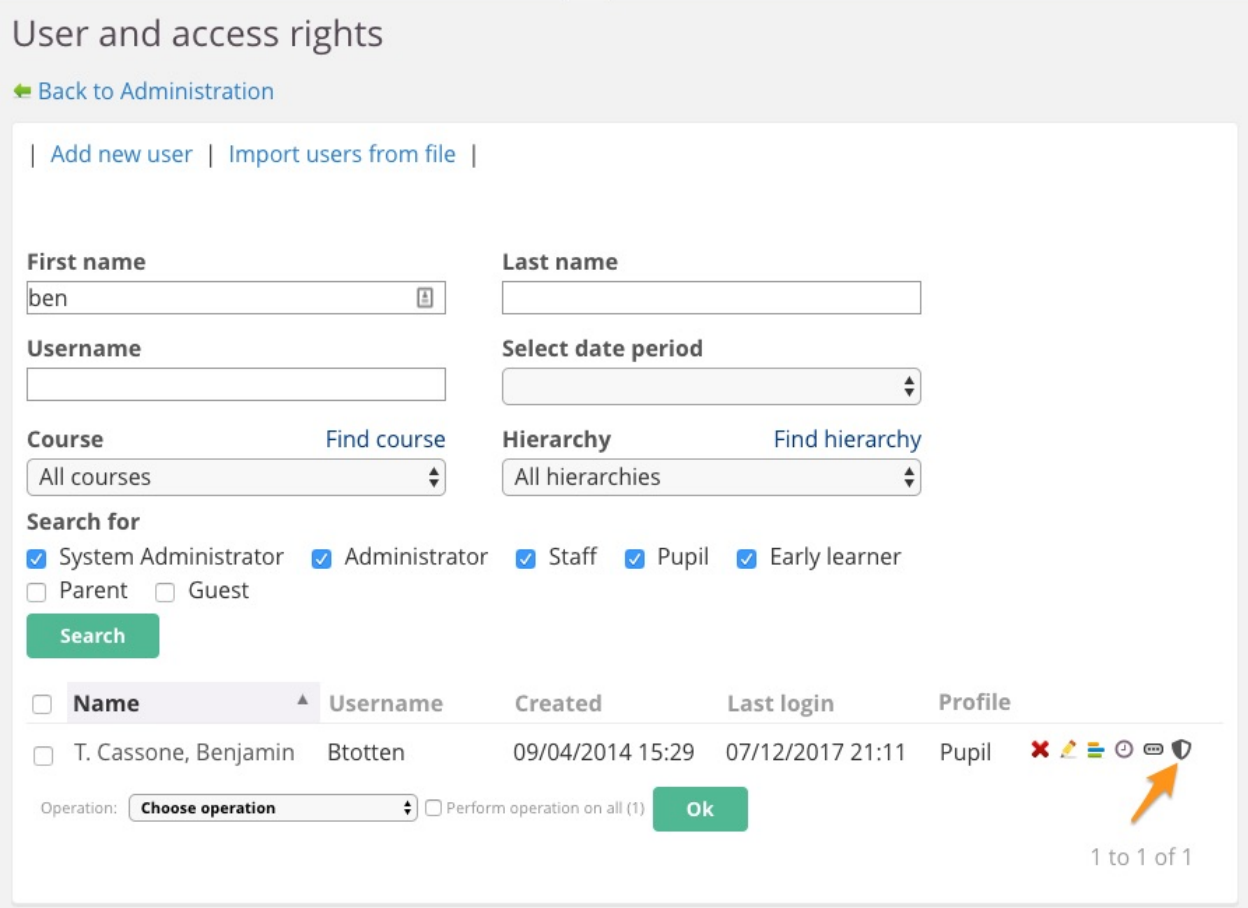
Below is a description of how some of the rights can be exercised with the help of itslearning functionality.

Performing actions to satisfy the rights of the data subject

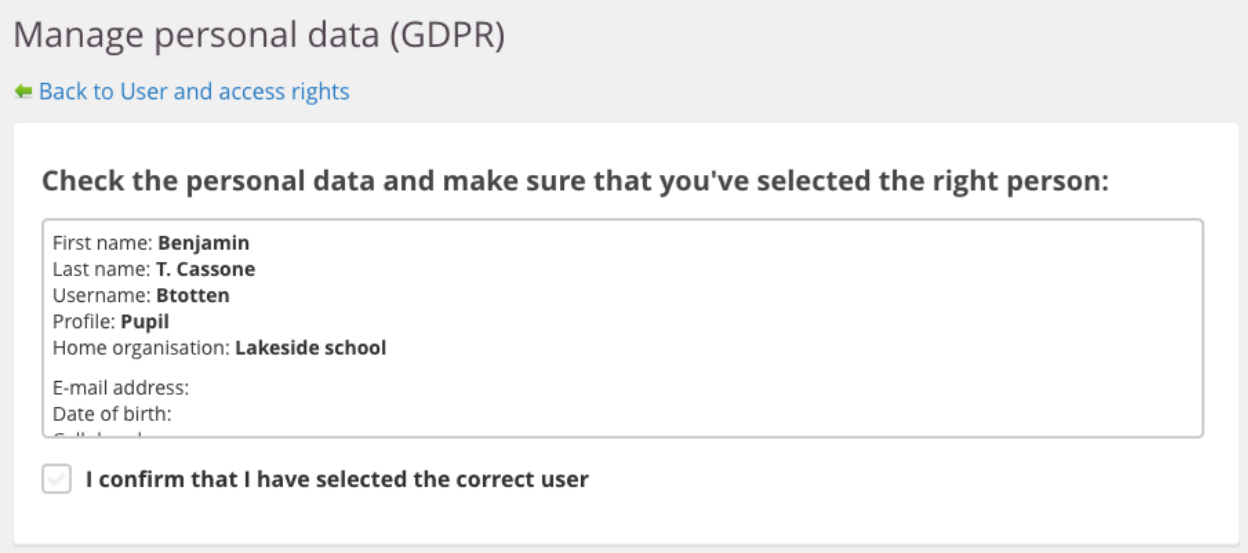
When a request from a data subject is received and accepted by the Data Controller, they should contact itslearning support.

To help our customers satisfy the rights of the data subject, we have added a “GDPR tool” to assist administrators perform the necessary actions. This tool will be enabled after the initial contact with support. The tool will then be available to the system administrator. The actions available will help with giving access to what data are stored related to a data subject, edit his or her information, restrict or delete data. Details for each action can be found below.

To access the GDPR assistance tool, the administrator should go to Admin -> Users and access rights, search for the data subject in question, and click the shield icon to the right, as indicated in the screenshot below:



Clicking the icon will first ask for confirmation that the correct user is selected (in case there are multiple users with the same name):



After confirming that it is in fact the correct user, options will be available to help with the next steps.

Each of these actions will require the administrator to enter a reason for performing the action, which will be logged.

In general, this tool is “instant” meaning the actions performed will be processed without delay. Some actions might however take some time to complete. This is to ensure that performance of the system is maintained should the request include extensive amounts of data.

The right to access and data portability

The data subject has the right to obtain information from the Data Controller about what personal data are processed, how and why. In some cases, the data subject may also have a right to transmit those data to another Data Controller. This is described in the DPA, and categories of data can also be found on page 2 of this document for easy reference.

More details about these rights can be found in Article 15 (https://gdpr-info.eu/art-15-gdpr/) and Article 20 of GDPR (https://gdpr-info.eu/art-20-gdpr/).

To access the specific information stored in itslearning related to a data subject, the administrator should access the GDPR tool and select PREVIEW/DOWNLOAD. This will create a file in xml format with all information stored related to the data subject. Please note that generating this file might take some time, depending on the amount of information stored in each case. The file will be available for download once it is generated.

Data in the “Internal logic” category will not be included.

The right to rectification

Should there be inaccurate, incomplete or erroneous personal data concerning a data subject, he or she has the right to have the Data Controller rectify it.

More details about this right can be found in Article 16 of GDPR (https://gdpr-info.eu/art-16-gdpr/).

In many cases the user can correct information himself in the itslearning interface. In other cases, and most commonly, information about a person like name, email address and so on should be edited in the external student information system and synchronised with itslearning. Other types of data can be corrected by teachers or administrators in the itslearning system. We have included a link to more help on rectification in the GDPR tool.

The right to restriction of processing

More details about this right can be found in Article 18 of GDPR (https://gdpr-info.eu/art-18-gdpr/).

Restriction will be performed as a “soft delete” when the administrator selects RESTRICT in the GDPR tool. The effect will be the same as if the user was moved to the trash can in itslearning. All information about a user will be removed from UI, but not irreversibly erased.

This might in some cases mean that the user name is anonymised while content is kept available (pseudonymisation). The table below outlines how this is handled in the different categories of personal data:

Category	Effect of RESTRICT
Personal information (contact information)	Not visible
Communication	Anonymised
Course material (produced by user in context of teaching)	Anonymised, unless the material exists so that it is only available to the data subject in question
Assessments (given by teacher to student)	Still visible and not anonymous if the teacher is restricted, as the assessments are still of value and affecting the rights of the student.
Calendar entries	Personal events are no longer visible, shared events are anonymised
Student responses	Not visible
Internal logic	Never visible

Restriction is reversible and can be performed by restoring the data subject (user) from the trash can. When restriction of processing is lifted, the Data Controller is obligated to inform the data subject.

The right to erasure ("right to be forgotten")

In almost all cases, deleting a user and his related data, will be done because the purpose for processing his data is no longer valid. Most commonly this is because a student left school, a teacher changed jobs, or because the customer has terminated the contract with itslearning. In these cases, we recommend that the normal flow for deleting users is used. Move the user(s) to the trash can or mark them as deleted in the external system. Complete the process by emptying the trash can, after which the user(s) and their data will be permanently deleted from itslearning.

Deleting information related to a specific data subject request based on his right to erasure as defined in GDPR, can be done by accessing the GDPR tool and select DELETE. More details about this right can be found in Article 17 of GDPR (https://gdpr-info.eu/art-17-gdpr/). This will completely erase any information related to the data subject from the itslearning platform, with some exceptions mentioned in "Roles and responsibilities" above.

As an example, this will include assessments given by a teacher to a student. If the teacher is deleted, these data will still remain in the system to retain the rights of the student.

Please note that this action is not reversible.

Category	Effect of DELETE
Personal information (contact information)	Permanently deleted
Communication	Permanently deleted when all affected users are deleted. For example, a group conversation in the message system is deleted when all participants of that conversation are deleted. Bulletins and discussions are deleted when the course they belong to is deleted.
Course material (produced by user in context of teaching)	Anonymised, unless the material exists so that it is only available to the data subject in question (in which case it is permanently deleted)
Assessments (given by teacher to student)	NOT removed if the teacher is deleted, as the assessments are still of value and affecting the rights of the student.
Calendar entries	Permanently deleted if personal, anonymised if shared
Student responses	Permanently deleted
Internal logic	Permanently deleted

Data Protection – in every step of our product development process

itslearning's product development process embraces a number of industry-leading frameworks, including a close adherence to developing software that includes data protection by design and by default. This includes the adoption of a set of standardized principles, and the use of a checklist to ensure at each stage of our development process data protection is considered and included as necessary.

Basic requirements for any software handling personal data

- **Lawful, fairly and transparent:** All personal data is processed lawfully, fairly and in a transparent manner in relation to the data subject
- **Ensure purpose limitation**: The software must only collect personal data for specified, explicit and legitimate purposes.
- **Ensure data minimisation**: The software must only process personal data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Ensure accuracy:** The software must ensure that all personal data is accurate and up-to-date. Incorrect data must be deleted or rectified.
- **Ensure storage limitation**: The software must ensure that it is not possible to identify the data subject for longer than is strictly necessary for the purposes for which the personal data are processed.
- **Ensure integrity and confidentiality:** The software must ensure appropriate security of the personal data.

Key concerns for establishing Data Protection and Information Security

As itslearning works on developing software, there are a number of steps and questions related to data protection and information security that we consider. These reflections include considering:

- Define the processing to be done, and establish an overview of the personal data: Will personal data be processed by the software?
- If the software is working as intended **without** identifiable data, no identifying data must be collected.
- Data protection can be designed in using pseudonymisation techniques in the software.
- The software must only use personal data as planned.
- Personal data must be available to those authorised to use it when necessary.
- The software must be developed with default settings that protect the rights of data subjects and safeguards privacy.
- When personal data is collected from **persons other than** the data subject, **information** must be provided concerning which categories, e.g. information about assessments, of personal data are being processed
- To ensure security of processing of personal data, it is necessary to:
    - ensure **confidentiality**. Personal data must be secured against unauthorised disclosure or access.
    - ensure **integrity**. Personal data must be secured against accidental and unlawful destruction, loss, or alteration.
    - ensure **accessibility**. Personal data must be available to authorised personnel who require it for their work.
    - ensure **resilience**. Resilience means that software that is processing personal data must be able to resist e.g. vulnerabilities, attacks, and accidents.

Use of Sub Processors

When using (sub) processors, we ensure that we have a Data Protection Agreement with the processor. We also require that:

- The controller must only use processors who provide adequate guarantees that they will implement measures ensuring compliance with the data protection regulation and ensure the protection of the rights of the data subject.
- The controller must ensure that any suppliers and subcontractors fulfil all requirements by entering into processing contracts.

Principles for Data Protection and Privacy by Design and Default

The 7 principles below are created by the Information & Privacy Commissioner of Ontario. We have embedded them in our software development process, from the way we work through the ideation phase, through to how software developers work with the requirements, up to the release of new software to the itslearning platform.

1. Proactive, not Reactive
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality
5. End-to-end Security
6. Visibility and Transparency
7. Respect for User Privacy

Data protection by Design and by Default for new products/features in itslearning

We have a checklist to help teams understand and comply with the requirement of data protection by design and by default in article 25 of the General Data Protection Regulation. The checklist is inspired by a similar checklist developed by The Norwegian Data Protection Authority.

The core elements of the checklist describe what considerations are taken by the people involved in each step of our product development process:

Innovate

The product owners are responsible for designing, writing requirements and specifications for a new or changed feature so that:

- The purpose and lawfulness for processing personal data is defined
- Security and privacy is ensured through Design and by Default
- Our data-protection principles are followed
- New / existing sub-processors are identified, and there is a valid DPA.

Build

The software architects, developers and test engineers are responsible for designing, coding and testing new and changed features so that:

- All processing of personal data is aligned with the defined purpose and lawfulness
- The feature meets data-protection principles
- Fulfils the data-protection principles
- They write secure code by implementing the requirements for data protection and security according to official itslearning coding standards

Deliver

The integration consultants are responsible for ensuring that:

- Any processing through integrations meets the purpose and lawfulness of the feature
- The integration design fulfils the data-protection principles
- Fulfils the data-protection principles
- Write secure code by implementing the requirements for data protection and security

Support/maintenance

The operation engineers are responsible for considering the following for new services:

- The processing in the new service is aligned with the defined purpose and lawfulness
- The design of the new service fulfils the data-protection principles
- Fulfills the data-protection principles
- Follow the company policy regarding Incident Management

Passing data to 3rd party providers

The itslearning LMS is highly flexible, and can be extended with tools, content and additional services. This can be done by our customers, our end users and third parties acting on behalf of both itslearning and our customers. The purpose of such extensions is always to offer more tools, capabilities and options for our users. Examples of such extensions can be:

- Assessment tools, for example assignment tools or digital test tools tailored for specific curriculum or teaching methods
- Teaching and learning activities, such as interactive study materials
- Open Educational Resources (OER) and licensed content provided by publishers
- Third party applications for mobile devices

In some cases, these extensions will require some personal data to be transferred from itslearning in order to provide value to our users, for example:

- Show the name of the user as part the application
- Give a teacher a list of students and their group affiliation when assessing an activity
- Suggesting additional tools or materials based on achievements

For itslearning, it is of the highest importance that our customers and end users feel secure that their data is protected, and only used according to the specified requests and needs of our customers. As such, itslearning takes strong measurements in order to protect all personal data, and only expose this data to the extent that our customers need.

Below is a short description of the different ways itslearning can be extended, and how we enforce protection of this data in accordance with our customers needs.

itslearning extensions, the Developer Program and the App Library

The itslearning *development program* is a platform, architecture and framework which allows third parties to extend itslearning by creating their own applications, plugins or modules ("Extensions"). These extensions can then be made available directly to end users by the administrators, or end users can browse for applications which have been made available to them in the itslearning *app library*. The *app library* may contain extensions developed by itslearning, by the customer, or by

approved third parties who offer free or licensed tools to a customer. These extensions can access some personal data, and may be given extended access to personal data by a customer. You can read more about this on itslearning's public developer portal.

In order to enforce protection of personal data, the following restrictions are in place for the developer portal:

- Only extensions provided by itslearning or itslearning´s sub-processors are made available in the app library to all customers, globally or in a specific market
- Extensions created directly by a customer may be made freely available for that customer´s end users
- Extensions made by approved third parties who are *not* sub-processors of itslearning, can offer licensed (free or paid) extensions to selected customers, but will require a separate Data Processing Agreement. ("DPA") with the customer before the extension can be made available in the app library. The customer will be informed that personal data may be transferred to third parties.
- Additionally, it is possible for a customer to completely disable the app library upon request

Short story: itslearning will will not transfer personal data to third parties through extensions, unless this is authorised by the customer.

LTI Tools

The LTI standard ("Learning Tools Interoperability") is a way to easily connect learning applications and tools with itslearning, in a secure and standard manner. Using LTI, customers and users can gain access to a wide range of content and tools provided by any third party. The standard is maintained by the IMS Global Learning Consortium. You can read more about it here. Depending on the way it is set up, LTI tools *may* have access to a user's personal data when used together with itslearning.

in itslearning, LTI is used to provide tools and content in different ways, including:

- Educational resources made available through the itslearning library by publishers or other third party providers
- Educational resources setup directly by the customer
- Ad-hoc resources made available to a class, directly by the class teacher

Educational resources made available in the library to all users by itslearning or itslearning's sub-processors are covered through your agreement with itslearning. A customer may import additional resources, but a separate data processing agreement must be made between the customer and the third party when this is done.

The option for *class teachers* to add ad-hoc LTIs is managed through permissions defined by the customer. By default, teachers are not able to add their own LTI tools to a course, but can be given permissions for his by the customer. The customer can also decide if these tools should expose any personal data to the tool provider.

Short story: itslearning will not transfer personal data to third parties through LTI, unless this is authorised by the customer.

APIs

itslearning also offers Application Programming Interfaces ("APIs") which can give third parties access to personal data. These APIs are closed for third parties, and access to these will not be given to third

parties except upon written instructions from a customer. In short, itslearning will not transfer personal data through our APIs, unless this is authorised by the customer.