Data Protection and Security (GDPR)
Version 1.2
User guide – Data Protection and Security (GDPR)

The GDPR (General Data Protection Regulation) came into effect on 25th May 2018. GDPR enhances and strengthens the rights of individuals in the European Union to control their personal data and also requires organisations, including schools, to review their privacy and data protection measures.

Aladdin has appointed expert data protection guidance to assist and support us in meeting GDPR compliance. Schools using Aladdin can therefore be confident that their data is being stored in a GDPR-compliant environment. In addition, Aladdin includes many built-in data protection and security features to assist schools to meet their GDPR compliance requirements.

This user guide outlines the ways in which Aladdin supports GDPR compliance in your school and will help your school to be sure you are using Aladdin in a GDPR-compliant manner. There is a section detailing how your school should respond to a Subject Access Request (SAR) concerning data stored in Aladdin. There are also guidelines for how your school should respond to a data breach.

To further support data protection in your school, Aladdin have put together a GDPR Information page available within the Aladdin Help section. This information page includes a resource kit containing a number of helpful documents and a sample school data protection self-assessment form. On this page you will also find links to Aladdin’s privacy statements, terms and conditions and data processing agreement.

Whilst every effort has been made to ensure the accuracy of the information / materials contained in this user guide, this document is intended to provide friendly and helpful advice and is not a definitive statement of law. Aladdin is unable to advise schools on their own data protection obligations and we recommend that you should always seek advice from your school’s governing body or obtain specific legal or other professional advice in relation to Irish law for each specific matter.
Table of Contents:

Contents
User guide – Data Protection and Security (GDPR) ......................................................... 2

Table of Contents: ............................................................................................................ 3

Section 1. GDPR – overview and getting started ......................................................... 5
  1.1: What is the GDPR? ................................................................................................. 5
  1.2: What does GDPR mean for schools? .................................................................... 6
  1.3: Is consent required from parents / guardians to store children’s data on Aladdin? .......... 7
  1.4: How Aladdin can help your school comply with GDPR ........................................ 8
  1.5: How can I view my Data Processing Agreement with Aladdin? ............................ 10
  1.6: First steps: guidelines for schools to ensure they are using Aladdin in a GDPR-compliant manner ........................................................................................................... 10
  1.7: Good practice for schools when contacting / emailing Aladdin ............................. 12

Section 2: Protect your data ............................................................................................. 13

Section 2.1: User account security and access rights management ......................... 13
  2.1.1: Who should have System administrator access to Aladdin? ................................. 13
  2.1.2: User account security ......................................................................................... 13
  2.1.3: Resetting / changing passwords ......................................................................... 14

Section 2.2: Access rights audit ..................................................................................... 17
  2.2.1: Check access rights for all staff in your school .................................................. 17
  2.2.2: Remove any staff not currently in the school to former staff list ....................... 17
  2.2.3: Check the teachers assigned to each class ......................................................... 18
  2.2.4: View who has been given resource access to students ........................................ 18

Section 2.3: Keeping data secure when using Aladdin in the school ...................... 21
  2.3.1: Sample “Use of Aladdin DPP Statement” ............................................................. 21
  2.3.2: Automatic logout of Aladdin ................................................................................ 22
  2.3.3: Using the “Remember me” option ...................................................................... 22

Section 2.4: Data classification and document protection within Aladdin .................. 25
  2.4.1: Protecting and securing documents in Aladdin .................................................... 25
  2.4.2: Guidelines for setting protection levels for Aladdin documents ............................. 26
2.4.3: Setting default document protection levels .......................................................... 28

Section 2.5: Printing, downloading, and sharing information from Aladdin .................... 31

2.5.1: Printing .................................................................................................................. 31
2.5.2: Downloading ........................................................................................................ 32
2.5.3: Sharing Information ............................................................................................... 33

Ensuring data protection when texting from Aladdin .................................................... 33
Ensuring data protection when emailing from Aladdin ................................................... 34

Section 2.6: Implementing an acceptable usage policy in your school ......................... 35

Section 3: Keeping data up-to-date in Aladdin ............................................................... 36

3.1: Verifying Student Contact Information .................................................................. 36
3.2: Data Retention ......................................................................................................... 38
3.3: Carrying out an audit of your existing Aladdin documents ..................................... 38
3.4: Deleting documents from Aladdin .......................................................................... 40

Section 4: Aladdin and parental requests ...................................................................... 41

4.1: Subject access requests (SARs) ............................................................................... 41
4.2: Right of erasure ....................................................................................................... 43

Section 5: Responding to a data breach ....................................................................... 44

Section 6: Data Protection Resources for Schools ...................................................... 45

6.1: Schools Data Protection Self-Assessment checklist ............................................... 45
6.2: Sample Data Protection Policy ................................................................................ 45
6.3: Glossary of data protection terms: ......................................................................... 46

Help ................................................................................................................................. 47
Section 1. GDPR – overview and getting started

The GDPR (General Data Protection Regulation) came into effect on the 25th May 2018. GDPR replaced the pre-existing data protection framework under the EU Data Protection Directive.

The GDPR enhances and strengthens the rights of individuals in the European Union to control their personal data and requires organisations, including schools, to review their privacy and data protection measures.

1.1: What is the GDPR?

The GDPR emphasises transparency, security and accountability by data controllers while at the same time standardising and strengthening the fundamental rights and freedoms of European residents to data privacy.

In light of recent rapid technological developments, increased globalisation, and the increasingly complex flows of personal data between countries, the GDPR updated the previous data protection laws and puts in place a single set of data protection rules for all individuals in the EU.

In summary, some of the key principles of GDPR include:

- Personal data must be processed lawfully, fairly and in a transparent manner;
- Personal data can only be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes;
- Personal data must be accurate and, where necessary, kept up to date. In addition, personal data that are inaccurate must be removed or rectified without delay;
- Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Personal data must be kept secure;
- Data breaches must be notified - GDPR requires organizations to report certain data breaches to data protection authorities, and under certain circumstances, to the affected data subjects.

In addition, organisations must be accountable for the personal data they use, and they must be able to demonstrate that they are in compliance with the principles of data protection through documented procedures and practices.
1.2: What does GDPR mean for schools?

The GDPR applies to any organisation, including schools, based in or outside the European Union that engages with residents of the EU. The GDPR enhances and strengthens the rights of individuals in the European Union to control their personal data and requires schools to review their privacy and data protection measures.

Aladdin has engaged expert data protection guidance to assist and support us in meeting GDPR compliance and we are firmly committed to GDPR compliance across our product. We are also committed to helping and supporting our schools to comply with GDPR.

Schools are custodians of large volumes of data about children (and staff) and it is very important that this information is kept secure. In order to get started on GDPR compliance in your school, we suggest a 4-step approach:

1. Identify - what personal data your school collects and where it is stored.
2. Manage - who has access to this data and how is the data used.
3. Secure - ensure that data is secure, protected, and processes are in place to respond to data breaches. (All organisations, including schools, will be obliged to report data breaches to the relevant authorities within 72 hours.)
4. Report - be able to carry out subject access requests.

Schools need to be aware that GDPR does not only apply to information stored in Aladdin, but to ALL information a school collects and stores via paper, in filing cabinets, other software products, information stored on laptops, school servers, etc.
1.3: Is consent required from parents / guardians to store children’s data on Aladdin?

School principals may not need to get consent from parents / guardians to gather and store their children’s data where the data is necessary for administering the education of the children. The school has a statutory basis and a legitimate interest in processing the children’s data and do not need to rely on consent as their legal basis. However, any children's data which is gathered by the school which is additional to that data necessary for administering the education of the child, may require consent. In this case, we would recommend you contact your school governing body for clarity on what they are advising schools on this matter.

Schools are obliged to be transparent and, as such, we would suggest that for future data gathering, the following should be included on the enrolment forms or in your school’s privacy policy:

"We gather and process your child's personal data for the purposes of administering the education of your child. To facilitate this, we will input your child's data into the schools Management Information System, Aladdin. Aladdin is a secure software as a service application which is owned and run by Cloudware Ltd. (T/A Aladdin Schools), from where the data is only processed for the above purpose."

The wording of "administering the education of your child" could be amended by your school should you wish to describe the purpose differently, just so long as the communication provides transparency as to the purpose and the use and storage of the data, that is the important thing.

For parents of children whose data is already on the database, we would recommend schools find a way to publicise the above statement, such as on their website, in their privacy policy, or on a parents' notice board.

For schools using the student transfer feature within Aladdin, schools however need to ensure they have parental consent to transfer the information to another school.
1.4: How Aladdin can help your school comply with GDPR

Although the journey to becoming GDPR compliant may seem challenging, it is reassuring to know that using Aladdin in your school supports and assists GDPR compliance in many key areas.

Secure Cloud-based Data Storage
The security of your data is of the utmost importance to Aladdin and we partner with global industry leaders to ensure this is the case.
We use Google to store your school information in data centres within the EU that are independently audited and certified to international standards. Aladdin has superior data security with extended SSL encryption and this means that even if Aladdin is accessed across an unsecured wireless connection the data is fully protected.

Secure, password protected access to data stored in Aladdin
With Aladdin, access to data is password protected and restricted firmly to those who need to have access to it. For example, users with full administration rights, i.e. the Principal, Secretary and Deputy Principal will see all students, whereas a user with normal access, i.e. a classroom teacher, will only see students in their class, and a resource teacher will see just the students he or she is working with.

Data security and elimination of insecure paper-based records
Using Aladdin in your school eliminates the need for insecure paper records; information in Aladdin is stored securely so there is a reduced need to keep hard copies of personal information. Storing your data in Aladdin is more secure than storing data in hard copy in your school. In the school your data is subject to physical loss and theft as well as unauthorised access from people visiting your school. With Aladdin if your computer fails or is stolen your data is never lost you simply sign in from another device and your data is there as normal.

Ease of access to data
Aladdin makes it easy to find and maintain up-to-date student / parent / class / staff information, Reports and documents are all in one place and are easy to access. It is easy to check, update and edit personal information. Such ease of access to data means that, should it be necessary, your school can quickly and easily respond to a Subject Access Request (SAR).

Keeping student information accurate and up-to-date
Complying with GDPR necessitates that you keep personal information up to date. To help with this Aladdin includes a Verifying Student Contact Information document in the Gallery which you can use at the start of each school year to make sure all your student information is up to date.
**Protection levels on documents**
Aladdin allows you to set protection levels on sensitive student documents. Protection levels include “Normal”, “Protected”, “Admin only”, “Admin only & hidden”, “Principal & selected staff only”, “Principal only”, and “Principal only & hidden”. You can also add password protection to some document types in Aladdin.

**Automatic logout after a period of inactivity**
In order to protect the security of your data, users are automatically logged out of Aladdin after a period of inactivity is detected. This policy is enforced in order to enhance data protection and security when using Aladdin in the classroom, school office, or other public setting.

**Backing up data**
Aladdin takes care of this for you. Aladdin and Google are Data Processors. All the school data is stored exclusively in Google EU Data Centres. Google keep your data safe and secure by using dozens of critical security features.

**Resources**
In addition to the GDPR Information page, Aladdin have put together a resource kit, including a sample Data Protection Policy document and Schools Data Protection Self-Assessment checklist. The Schools Data Protection Self-Assessment checklist is a self-evaluation tool will help your school review its overall level of readiness to comply with the GDPR.

**ePayments**
If you are using Aladdin ePayments your school can collect debit and credit card payments from parents online via Aladdin in a safe and secure way. This module is available as part of the standard Aladdin Start package.

**Aladdin Connect**
Aladdin Connect, the add-on parent portal feature, helps your school’s ability to be GDPR compliant by enabling parents to have secure, logged access to their child's data such as report cards, test results, attendance, etc. Aladdin Connect helps ensure your school's accuracy of parental contact details and eliminates the need for potentially unsecure paper communication, etc.
1.5: How can I view my Data Processing Agreement with Aladdin?

The GDPR requires your school and Aladdin to have a Data Processing Agreement in place. Aladdin and your school already had a Service Level Agreement in place in the form of our existing contract with you, made up of your Order Form, our Terms of Service, and our Privacy Policy. The Data Processing Agreement is a new addition to that entire agreement. You can view your Data Processing Agreement by clicking on the link in the GDPR Information page in the Help section of Aladdin.

1.6: First steps: guidelines for schools to ensure they are using Aladdin in a GDPR-compliant manner

It is reassuring to know that Aladdin is committed to GDPR compliance. However, in order to ensure that your school is using Aladdin in a GDPR-compliant manner, we recommend that you start with the following steps:

**Step 1. Perform an Aladdin access right audit**

- a. Limit admin access rights to only those staff members who absolutely need it.
- b. Ensure no staff member is sharing an Aladdin account.
- c. Update access rights as appropriate and reset passwords for any staff member who may have shared their login details.
- d. Remove any staff not currently in the school to former staff.
- e. Check who is assigned to each class and ensure those who have access to students in a class are as expected.
- f. Use the resource report to view who has been given resource access to students and ensure these are up to date. Remove any access that is not current.
- g. Educate your staff on how important it is to keep their login safe and secure and to never share their account or access their account in an unsafe environment. Ensure they always log out of their account when unneeded, and never leave a computer screen unlocked when unattended. In order to protect the security of your data, users are automatically logged out of Aladdin after a period of inactivity is detected. This policy is enforced in order to enhance data protection and security.

Further detailed information regarding performing an access right audit in Aladdin can be found in Section 2.2: Access rights audit of this user guide.
Step 2. Data Classification & Document Protection within Aladdin

Aladdin has **advanced protection levels** for sensitive documents to help you ensure that only the applicable staff members have logged access to view/edit certain documents. Default protection types can be set via the document settings page to ensure that all documents that may contain sensitive information are by default given the protection level they require.

We would advise all schools to run a check on all documents they currently have on Aladdin and ensure the required protection level is set.

- a. If necessary, it is possible to increase the protection level for sensitive documents and other Aladdin documents containing personal information.
- b. Aladdin gives you the option to add default document protection levels for document types via the document settings page.
- c. Coming soon… an option to run a report to see the protection levels set for all current documents.

Further detailed information about data classification and document protection can be found in Section 2.4: Data classification and document protection within Aladdin of this user guide.

Step 3. Printing, downloading, and sharing information from Aladdin

Aladdin has safeguards for printing and downloading information in the form of automatic watermarks for printouts, and warnings when downloading. For emailing/texting, schools should always ensure their contact information is up to date to ensure communication is sent/received as expected. Schools may also wish to consider using the Aladdin Connect feature which will further enhance a school’s ability to be GDPR compliant.

When viewing attachments in Aladdin, documents may be downloaded during the viewing process. Staff should be vigilant in ensuring they always check and delete any documents downloaded during this process from their downloads folder.

Further detailed information about printing, downloading, and sharing information from Aladdin can be found in Section 2.5: Printing, downloading, and sharing information from Aladdin.
Step 4. Using the sample “use of Aladdin data protection policy” document

In the Gallery there is a document entitled “use of Aladdin Data Protection Policy”. All school staff members should be aware of the school’s Data protection policy particularly in relation to Aladdin. In addition, this information should be included in all schools’ data protection policies.

Further details of this document and instruction of how to access this document can be found in Section 2.3: Keeping data secure when using Aladdin in the classroom / school office.

1.7: Good practice for schools when contacting / emailing Aladdin

Keeping your Aladdin login details secure
The security of your information is of the utmost importance to Aladdin. Aladdin staff do not require and will never ask for a user’s password. You should never email us your Aladdin login details or attempt to give us your login details (password or username and password) over the phone.

We cannot access your Aladdin system without your permission - if you wish us to access your school for troubleshooting purposes, you will need to generate an access code. You should only give out an access code if you have called customer support yourself and you feel access is required to solve the problem you are experiencing. Please note that customer support access can only be generated by an Aladdin administrator in your school and all access is logged.

Emailing personal / confidential data
We would kindly ask that you do not email Aladdin any information (files, screenshots, links, etc.) that may contain personal data. This includes information such as staff signatures, personal student or staff information, such as psychological reports, medical reports / information, allergy information, payment information, etc.

Data import
You can upload information (from Microsoft Word, Excel, and Access files, csv and tab delimited files) into Aladdin using the Data import facility. If you wish us to perform the data import for you, you can upload your information using the assisted data import. Sending us your data this way is 100% secure: your data is encrypted and totally safe. Please do not email us your data or send us any CDs or USB drives as doing so is not secure.
Section 2: Protect your data

GDPR requires that you ensure that your data is secure and protected. Using Aladdin to store your data enables you to take advantage of the in-built safeguards that support you to protect data and maintain high standards of data security in your school.

Section 2.1: User account security and access rights management

2.1.1: Who should have System administrator access to Aladdin?

Access to data in Aladdin is by username and password and each account gives relevant access to their user. Aladdin’s access management options ensure that schools can share with staff only the information that is required of them for their current role. There are several different access levels available in Aladdin, the highest of these being “System administrator”.

Aladdin firmly recommend that Administrator access rights are limited only to those staff members who absolutely need it.

We firmly recommend that System administrator rights are reserved solely for the Principal, Deputy Principal and your school Administrator (Secretary). Adhering firmly to this policy will assist you in maintaining the highest levels of security and data protection when assigning and administering access rights to Aladdin users in your school.

2.1.2: User account security

Aladdin firmly recommend that each staff member has their own username and password to access Aladdin and that user accounts are not shared. Schools, as data controllers, must
ensure that accounts and passwords are not shared and staff take appropriate measures to keep their accounts secure.

If you have shared your Aladdin password, please change your password with immediate effect and do not share this information with any other staff members going forward.

We also advise any staff members in your school who may have communicated their password to any other staff member/other individual previously to also change their password NOT to share these details with anyone else.

2.1.3: Resetting / changing passwords
If you, or another staff member in your school, have shared or otherwise communicated their password, we recommend that the password is changed with immediate effect. An Aladdin administrator can reset a staff member’s password by going to Admin - Staff list and clicking on the name of the staff member whose password you need to change. At the bottom of the staff member’s profile page, you can click the Reset password button.

The temporary password will now appear and you can copy this down.

If you click back into the Staff List you will also be able to see the temporary password in the far-right column. You can place your cursor over the blackened box to see the temporary password.
Give the temporary password to the staff member in question and the staff member can use their existing username and this new temporary password to sign in to Aladdin. If necessary, you can print a password handout sheet by ticking the box beside the staff member’s name and clicking the Create Password handout option.

The staff member will be prompted to change this password to a new password of their choosing, once they sign in. Aladdin will notify users by email when a password reset has occurred (if they have provided an email address).

Dear Melanie Flynn,

This is an automated security message from Aladdin to advise that your password for your Aladdin account in St Robert’s National School has been reset by a system administrator in the school (Bob Fitzpatrick). You should ask them for your new temporary password which you will need to login and reset your password.

If this change has been made by mistake, please contact Bob Fitzpatrick or another system administrator in your school.

Kind regards,
The Aladdin Team

Any user of Aladdin can reset their own Aladdin password by going to the top-right corner of the Aladdin screen and hovering over the circle with your initial on it. Then choose the Email & Password option.
You need to enter your current password and then enter and confirm your new password.

Resetting temporary passwords
When a new user is set up in Aladdin or when a password is reset, a temporary password is allocated to the user. For security reasons, this temporary password will expire if it is not used within a certain time period. If you need to reset this temporary password, you can do so by following the instructions above for resetting a staff member’s password.

Password reset for inactive System administrator accounts
Any Aladdin System administrator accounts (usually Principal, Deputy Principal, and Secretary) that are inactive for more than 90 days will be automatically reset. Users will be sent an email to notify them of the password reset (if they have provided an email address).
Section 2.2: Access rights audit

2.2.1: Check access rights for all staff in your school

It is a good practice to check the access rights for all staff in your school to make sure access rights are up-to-date and as expected. You can check the access rights for all staff by choosing Admin – Staff list and viewing the list of all staff in your school. You will notice that each staff member’s access rights are displayed in the “Access” column.

If necessary, you can click on a staff member’s name to change their access rights.

2.2.2: Remove any staff not currently in the school to former staff list

Aladdin recommend that you check your staff list and ensure that any staff no longer working in your school are promptly moved to the list of former staff members.

When a member of staff leaves the school, Aladdin recommends schools move this member of staff to either a “former staff member” or to a “contact”.

To do this, click on Admin - Staff list and then click on the staff member’s underlined name. At the bottom of this page click on either the Make a former staff member button, or the Move to contacts button.
Once a user has been moved from the main staff list, they will no longer have access to your Aladdin system. In the event that this staff member returns to the school you can move them back into the staff list by clicking on their underlined name to open their staff profile, and then either the 'Move to staff list' or 'Return to staff list' button at the bottom of the page.

2.2.3: Check the teachers assigned to each class
Aladdin recommend that you check who is assigned to each class and ensure that those teachers who have access to students in a class are as expected. You can view this information by going to the School menu and choosing Classes.

In the example above, you can see that John Banks (a former staff member) is still assigned to 1st class. You can rectify this by clicking on the class name and then clicking the Edit button beside the class name.

2.2.4: View who has been given resource access to students
Aladdin suggest that you run the resource report to view who has been given resource access to students and ensure that this information is up-to-date and as expected. You can run the resource report by choosing Admin – Reports and select Resource / support summary.

![Resource / support summary](image.png)

The Resource / Summary report allows you to view either by student or by teacher and you can also view by the type of resource. For example, you can view each resource / support teacher in your school and the students assigned to each teacher.

<table>
<thead>
<tr>
<th>Helena Murray, 5 students</th>
</tr>
</thead>
<tbody>
<tr>
<td>□  James Baker, 3rd Class A, Jane Robinson</td>
</tr>
<tr>
<td>□  Alan Barry, 6th Class A, James Bond</td>
</tr>
<tr>
<td>□  Mary Byrne, Junior Infants, Gillian Fogarty</td>
</tr>
<tr>
<td>□  Saoirse Byrne, 6th Class A, James Bond</td>
</tr>
<tr>
<td>□  Martina Duffy, 6th Class A, James Bond</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Joseph Frank, 4 students</th>
</tr>
</thead>
<tbody>
<tr>
<td>□  Smith Jameson, Senior Infants, Tom Barry</td>
</tr>
<tr>
<td>□  Diamond Leekie, Senior Infants, Tom Barry</td>
</tr>
<tr>
<td>□  Geraldine Murphy, Senior Infants, Tom Barry</td>
</tr>
<tr>
<td>□  Anne Quinn, Senior Infants, Tom Barry</td>
</tr>
</tbody>
</table>

You can check that the report is as you expect and remove any access / allocation that is not current. To remove learning support / resource for a student, you can click on the student’s name. You can then remove the resource by clicking on the Remove option at the end of the line to the right of the student’s name.
It is also possible to Add support from this screen by clicking on the Add support teacher button.
Section 2.3: Keeping data secure when using Aladdin in the school

2.3.1: Sample “Use of Aladdin DPP Statement”
All staff members in your school should be aware of your schools Data protection policy, particularly in relation to Aladdin. To assist you with this, in the Documents Gallery in Aladdin, we have added a document entitled “Use of Aladdin Data Protection Policy Statement”. All staff in your school should be informed of this document and the information in the document should be included in your school’s data protection policy.

You can access the Use of Aladdin DPP Statement document by selecting Modules – Documents and then clicking on the Gallery tab. It is listed under the Data Protection Policy heading. You can click on the document to copy it into your school.

Aladdin regard the security of your data as our most important job. We advise that you educate your staff about the importance of keeping their login safe and secure and to never share their user account or access Aladdin in an unsafe environment. All staff should ensure that they log out of their account when they do not need to access Aladdin.

We also firmly recommend that you only log in to the Aladdin system when in a secure and non-public environment, for example, the school or home of the user and not in a public setting such as an internet café or library for example.

In order to enhance data security when you are using Aladdin in the classroom or in any other public setting we recommend the following:

- If you will be leaving your computer/laptop/device unattended for even a short period of time we strongly recommend that you lock your screen. For example, if you are using Windows press the Win+L key combination on the keyboard (Win is the Windows key and features the Windows logo).

- We strongly recommend that you password protect your computer/laptop/device and store it securely when you are not using it.

- We also recommend that you do not save your Aladdin login details in your browser. If you have already saved your Aladdin login in your browser you can remove it by
following the instructions in our FAQ entitled “How can I remove my saved password from my browser settings?”.

2.3.2: Automatic logout of Aladdin

In order to protect the security of your data you are automatically logged out of Aladdin after a period of inactivity is detected. This policy is enforced in order to enhance data protection and security when using Aladdin in the classroom, school office, or any other setting.

2.3.3: Using the “Remember me” option

On the Aladdin sign in screen, you can tick the Remember me tick box to allow you to stay signed in for longer.

You should not use the “Remember me” option in a classroom or where the computer may be left unattended and unlocked. When you tick the “Remember me” box you will see a warning message letting you know that you should not use this option in a classroom or where the computer/device may be left unattended. The message also informs you that you should always lock your screen when you leave your device.
The “Remember me” option may have been disabled in your school. This is because it is possible for an Aladdin administrator to disable or restrict the “Remember me” option in your school.

An Aladdin administrator can disable or restrict the “Remember me” option by choosing Settings from the Admin menu. Then click on the General tab (on the left-hand side).

On the Communication tab you will notice that there are three options for the Remember me policy – “Allow all staff to use remember me”, “Only admins can use remember me” and “No one can use remember me”.

![www.aladdin.ie says](image-url)
You can select the option you prefer to use in your school, for example, “Only admins can use remember me”, and click Save.
Section 2.4: Data classification and document protection within Aladdin

One of the key principles of GDPR is that personal data should be kept secure. Student documents, by their very nature, contain personal data and as such should be classified as sensitive and given an appropriate protection level in Aladdin.

Aladdin has advanced protection levels for sensitive documents to ensure that only certain staff members have logged access to view / edit certain documents. (Please note that “logged access” means that you can see exactly which Aladdin users have viewed / edited the document.)

It is also possible to set default protection levels for documents to ensure that all documents that may contain sensitive information can be given the protection level they require on an ongoing basis in Aladdin. It is also possible to retroactively change document protection levels of existing documents in your Aladdin system.

We strongly advise all schools to run a check on all documents they currently have on Aladdin and ensure that the required protection level is set. You can find more information about carrying out a document audit in Section 3.3: Carrying out an audit of your existing Aladdin documents of this user guide.

2.4.1: Protecting and securing documents in Aladdin

Aladdin allows you to set protection levels for sensitive student documents. Documents can be given an appropriate protection level. Protected documents require the user to enter their password to gain access to the document.

When a document is protected, any editing / viewing / changes made to the protection level of the document is logged, as shown in the example below:
2.4.2: Guidelines for setting protection levels for Aladdin documents

Aladdin allows you to set protection levels on sensitive student documents. Protection levels include “Normal”, “Protected”, “Admin only”, “Admin only & hidden”, “Principal and selected staff only”, “Principal only”, and “Principal only & hidden”.

Under GDPR, parents / guardians have a legal right to view any information stored against their child regardless of the protection level so please bear this in mind when creating / updating documents.

Protection levels for student documents include:

**Normal**
Anyone with access to this child can view this document. People with access to this child are the classroom teacher, assigned resource / support teachers and users with view all or administration rights.
**Protected**
Protected documents require the user to enter their password to gain access to the document. Any document activity is logged.

**Admin only**
Only administrators with academic access can view the note. Other users see the note title in the note list. Any document activity is logged.

**Admin only & hidden**
As above but other users **do not** see the document in the list. Any document activity is logged.

**Principal and selected staff only**
This is a new protection level allowing **only** the Principal and selected staff to see the document. When you use this option, you will be able to choose individual staff to share the document with. Other users will see the note title in the document list. Please note that even if you include a staff member here, they can only see the document if they have access to the student. The protection level can only be changed on individual documents. Any document activity is logged.

**Principal only**
Only the principal can see the document. Other users see the note title in the document list. Any document activity is logged.

**Principal only & hidden**
As above but other users **do not** see the document in the list. Any document activity is logged.
2.4.3: Setting default document protection levels

Aladdin gives you the option to set default document protection levels for document types within your Aladdin system. When you change a default document protection level, all existing documents of this type can be retroactively changed to the default you have chosen. (Please note that you will see a message when you do this to guard against you inadvertently granting or removing access to the document(s) for some Aladdin users.)

To set default document protection levels for document types, go to Admin – Settings and click on the Documents tab (on the left-hand side). Then, in the Student document types section (on the right-hand side of the screen), for each document type, choose the protection level you require from the Protection (default) drop down.

![Student document types](image)

When you select a default protection level, a tick box will appear in the “Apply New protection to existing documents” column.
You can tick this box to apply the new protection level to all existing documents. If you do not tick this box and click Save then the new protection will apply to all new documents of this type that are created from this point on.

If you do tick the box to apply the new protection level to existing documents, you will see a message letting you know that changing the protection level may affect access to documents for other users of your Aladdin system. This message will differ depending on whether you are raising or lowering the protection level of the document type.
You can click on **OK** if you are happy to go ahead and raise / lower the protection level for the document type. You will then see a tick beside the protection level in the “Apply New Protection to existing documents” column. You can then click **Save** to save your changes.

<table>
<thead>
<tr>
<th></th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>yard incident</td>
<td></td>
</tr>
<tr>
<td>Support File</td>
<td>Admin only</td>
</tr>
<tr>
<td>filled form</td>
<td>Normal</td>
</tr>
</tbody>
</table>

Please note that “Principal and selected staff only” protection level is not available when changing protection levels in bulk. This is because the selected staff may vary from document to document. The protection level on these documents can only be changed on individual documents.
Section 2.5: Printing, downloading, and sharing information from Aladdin

Aladdin has safeguards for printing and downloading information in the form of automatic watermarks for printouts and warnings when downloading attachments.

2.5.1: Printing
When you print a report or a document from Aladdin, a “Printed by…” watermark displaying the name of the Aladdin user who printed the document will appear by default in the top right-hand corner of every page of the document.

![Printed by Bob Fitzpatrick 08/12/2017](image)

The watermark is a useful way of keeping track of who has printed confidential documents and other confidential information from Aladdin. Please note that if you are printing a document that is not confidential, it is possible to remove the watermark before printing. You can do this by clicking the Print button in the top right-hand corner of your Aladdin screen.

Tick the box beside **This page does not contain confidential information, remove the “printed by” watermark** and click OK. The watermark will now be removed from the document.
2.5.2: Downloading

You can add attachments (files) to documents that you create in Aladdin. When you add an attachment, users with access to the document can click on the attachment to open / view it.

When viewing / opening attachments to documents in Aladdin, Aladdin will warn that you that your browser may save the attachments into a download or temporary folder on your computer.

You can check your browser’s settings to find out where to find the location your downloaded files are saved to. Once a file has been downloaded to your computer, other people using the computer / device may be able to access the file unless you delete it from your computer.
Aladdin firmly recommend that staff should be vigilant in ensuring they always check and delete any downloaded documents from their downloads folder.

2.5.3: Sharing Information
When emailing / texting from Aladdin, schools should always ensure their contact information is up-to-date to ensure communication is sent/received as expected.

At the beginning of the school year, many schools send out a sheet to all parents with contact information they currently have for their students. This is so that they can confirm that the information they have is correct, and to allow parents to update them if any information has changed.

To assist you with this, there is a document available in the Gallery entitled “Verifying Student Contact Information”. To access this document, select Modules – Documents, then click on the 'Gallery' tab.

You can find out more about how to copy this document into your school to use for creating mail merge documents etc. in Section 3.1: Verifying Student Contact Information of this user guide.

Please note, schools may also wish to consider using the Aladdin Connect feature which will further enhance a school's ability to be GDPR compliant.

Ensuring data protection when texting from Aladdin
The school should ensure that the purpose for which the phone numbers were originally collected is compatible with the use of the Aladdin texting service. At the time the school collects these numbers (usually on the enrolment form) it needs to inform parents / guardians that the school plans to use the mobile number to issue text messages to notify parents / guardians
about school closures, sports days etc. Alternatively, the school may send a note home to parents to inform them of the planned introduction of a new text messaging service and to request that parents / guardians confirm that their contact information is correct and to provide consent for using their number for same.

In addition to this, where individuals have been informed of the use as outlined above, the school would need to have procedures in place to ensure that the mobile numbers it has are accurate and up-to-date. We would highly recommend a practice to be in place to verify on a regular basis that the mobile number given by a parent / guardian remains valid, e.g. if there is a gap since the last contact with the parent / guardian their number should be verified again, to ensure that texts are only issued to the intended recipient. Normally, schools verify parents’ contact information annually after Christmas (when mobile phones are often changed) or on return to school after the summer holidays. Failure to follow these procedures runs the risk of sending notifications/reminders to the wrong person, either by virtue of a changed mobile phone or because the number held does not relate solely to the account holder.

Finally, we would recommend a practice to be in place where the school sends an annual text message to all parents/guardians that contains the name and contact information of the school, so as to allow anybody who is receiving test messages in error to have a way to identify the school and to contact you to make arrangements to be removed from the list. This can happen for instance when a number is typed incorrectly into the Aladdin system. In this case the school does not realize that a parent is not receiving messages, however a person often completely unrelated to the school with that mobile number receives the messages in error. This gives the individual the opportunity to contact the school to make arrangements to have the number removed, and for the school to make contact with the parent / guardian to request updated information. We recommend that the text of the SMS message to be sent to individuals should contain minimal information and not include any sensitive or medical information.

**Ensuring data protection when emailing from Aladdin**

Your school should ensure that the purpose for which the email addresses were originally collected is compatible with the use of the Aladdin emailing service. At the time the school collects these email addresses (usually on the enrolment form) it needs to inform parents / guardians that the school plans to use the email address(es) to communicate important school information with them, for example, information about school closures, sports days etc. Alternatively, the school may send a note home to parents to inform them of the planned introduction of communication between school and home via email and to request that parents / guardians confirm that their contact information is correct and to provide consent for using their email address for same.

In addition to this, where individuals have been informed of the use as outlined above, the
school would need to have procedures in place to ensure that the email addresses it has are accurate and up-to-date. We would highly recommend a practice to be in place to verify on a regular basis that the email address(es) given by a parent / guardian remain valid, e.g. if there is a gap since the last contact with the parent / guardian their email address should be verified again, to ensure that emails are only issued to the intended recipient. Normally, schools verify parents’ contact information annually, usually on return to school after the summer holidays. Failure to follow these procedures runs the risk of sending school communications to the wrong person, either by virtue of an incorrect email address or, alternatively, the parent failing to receive intended email communications from your school.

Finally, we would recommend a practice to be in place where the school sends an annual email message to all parents / guardians that contains the name and contact information of the school, so as to allow anybody who may be receiving email communications in error to have a way to identify the school and to contact you to make arrangements to have their email address removed from your Aladdin system.

Section 2.6: Implementing an acceptable usage policy in your school

Aladdin firmly recommend that you implement an acceptable usage policy for computer use in your school. Examples of acceptable usage policies can be found on the Department of Education and Skills website.
Section 3: Keeping data up-to-date in Aladdin

Complying with GDPR necessitates that you keep all the personal information your school collects accurate and up-to-date. Aladdin makes it easy to find and update student, parent, class, and staff information and also to update it as necessary.

3.1: Verifying Student Contact Information

To help you with keeping personal information up to date, Aladdin includes a Verifying Student Contact Information document in the Gallery which you can use at the start of each school year to make sure all your student information is up to date. You can download this document by choosing Documents from the Modules menu. Next, click on the Gallery tab and click on the 'Verifying Student Contact Information' under the heading 'Admin'.

Next, press the 'Copy this document into your school's document list' button. At this point you can rename, edit and save the document template to suit your school. This document is a merge template so can be used to run a mail merge. We would recommend you create one of these documents for each student in your school rather than one document per family to ensure all medical information and contact information per child is recorded correctly.
To run a mail merge using the Verifying Student Contact Information template, go to the Student list (or class list) and tick all students you wish to create a document for (we recommend creating a document for each child in your school).

Then from the Actions menu, choose Mail merge and select the Verifying Student Contact Information template.

A document will now be created for each child displaying the existing contact information you have in your Aladdin system for that child. You can either email these documents or print them out and distribute to parents as you prefer.
3.2: Data Retention
The GDPR states that personal data is retained for no longer than is necessary for the purpose or purposes for which it is obtained.

Schools as data controllers need to be clear about the length of time for which data will be kept and the reason why the data are being retained. In addition to this, personal data collected for one purpose cannot be retained once that initial purpose has ceased.

It is recommended that your school has a defined policy on retention periods for all items of personal data collected and stored by your school.

A Records Retention Schedule will assist you to determine how long you should retain personal data and other school data such as Roll books, Garda Vetting forms, and Enrolment applications. There is a Records Retention Schedule available on the Data Protection in Schools website (www.dataprotectionschools.ie), however, we recommend you contact your school's Data Protection Officer for more information/guidance.

Aladdin recommend that you check your school's data retention schedule before deleting any information or document from Aladdin to ensure you are abiding to your data retention schedule. This is particularly true of student documents and other documents in Aladdin containing personal information.

3.3: Carrying out an audit of your existing Aladdin documents
Aladdin recommend that you carry out an audit of all student documents you currently have on Aladdin to check that the appropriate protection level has been set for each document. You can view student profile documents by going to Modules – Documents and clicking on the Student Profile documents tab.

You will notice that the protection level for each student profile document is listed in the “Protection level” column on the right-hand side.
If necessary, it is possible to increase the protection level for sensitive documents and other Aladdin documents containing personal information. To change the protection level for an individual document, simply edit the document and change the document’s protection level.
As previously shown, Aladdin gives you the option to set default document protection levels for document types within your Aladdin system. When you change a default document protection level, all existing documents of this type can be retroactively changed to the default you have chosen. Please note that you will see a message when you do this to guard against you inadvertently granting or removing access to the document(s) for some Aladdin users.

You can find out more about how to set default document protection levels in Section 2.4.3: Setting default document protection levels of this user guide.

3.4: Deleting documents from Aladdin
Before deleting a document in Aladdin, you should refer to your school’s records retention schedule. You should only delete a document in Aladdin if you are sure you wish to remove the document permanently and immediately from your Aladdin system. You will be asked to confirm that you are sure you want to permanently delete the note / document and you should only click OK if you are sure you wish to do so.

When you delete a student document you will not be able to retrieve it under any circumstances. Please note that all student documents, such as behaviour notes, continuum of support documents, first aid reports, etc. are deleted permanently from your Aladdin system and are not recoverable.

School documents, such as policy documents, weekly reports, and cúntais miosúil may be recoverable for up to 48 hours after deletion. Please note that if you have deleted a school document in edit mode (by clicking the Delete option while editing the document) you will not be able to recover it. However, it may be possible to recover school documents that you have deleted from the document list (by ticking the box beside the document name and clicking Delete).

To attempt to recover a school document, choose Documents from the Modules menu and click the Show deleted button.
When you click the **Show deleted** button you will see a list of recently deleted recoverable documents and you can click on the file name to restore it. You can edit and save the document to restore it in your Aladdin system.

**Section 4: Aladdin and parental requests**

Under the GDPR, individuals have expanded **right of access**. Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain confirmation from the school as to whether or not personal data concerning them is being processed, where, and for what purpose. In addition, your school is obliged to provide a copy of the personal data, free of charge, and in an electronic format if requested.

### 4.1: Subject access requests (SARs)  
**Guidelines for schools for responding to a Subject Access Request for personal data stored in Aladdin**

Schools have one month to respond to a Subject Access Request (SAR). Schools using Aladdin have convenient and easy access to all information related to a student, thereby enabling a school to respond quickly and easily to a subject access request.

It is recommended that a school should satisfy itself that the person asking for the information is entitled to receive it and caution should be exercised in releasing information where there is any doubt on the issue of identification. Schools should seek advice where any doubt may arise.

Under Article 15 of the EU Regulation 2016/679, (the GDPR), data subjects, such as school staff, and parents on their own or on their children’s behalf, are entitled to request the following from your school regarding personal data stored in Aladdin:
(a) confirmation as to whether Aladdin processes personal data relating to them;
(b) the purposes of the processing;
(c) the categories of personal data concerned;
(d) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular, recipients in 3rd countries or international organisations;
(e) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(f) the existence of the right to request from your school’s Aladdin system, the rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(g) the right to lodge a complaint with the Data Protection Commissioner;
(h) where the personal data are not collected from the data subject, any available information as to their source;
(i) the existence of automated decision-making, including profiling (as set out in Article 22 (1) and (4)) and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The data subject may also request, and the school will provide a copy, of the personal data undergoing processing.

Where the data subject makes the request by email, and unless otherwise requested by the data subject, the information must be provided by email.
Such requests should be notified to your school’s Data Protection Officer as soon as they are received. Your school’s Data Protection Officer will need to ensure that the data subject requests meet the following formalities:

a. The identity of the data subject is established;
b. The information shall be provided in writing, or by other means, including, where appropriate, by email. When requested by data subject, the information may be provided orally;
c. The information will be sent without delay, and no longer than one calendar month from receipt of the request;
The response will be concise, transparent, intelligible and in an easily accessible form, using clear and plain language; and

The information will be provided free of charge, except where further copies are requested which incurs administrative costs for your school. In such a case a reasonable fee based on the administrative costs may be charged.

Aladdin would recommend first of all contacting the individual parent / data subject to first of all find out what information they are requesting to narrow down the request, i.e. they may just want certain documents. Depending on how your school collects and stores information, you may need to find this information in multiple areas - filing cabinets, other documents/files on computers etc., however for the information within Aladdin, all data relating to the student
should be accessed via their profile page. Print the information required. Ensure you redact any sensitive information regarding other students that may be contained within these files. Aladdin would recommend you black out names of other students etc. and then rescan and email or send photocopies of these printouts to the parent / data subject as the sharing of others’ personal data would be a data breach. If you are requested to provide the information in electronic format, please contact the Aladdin Support Desk for guidance.

4.2: Right of erasure
Guidelines for schools for responding to requests to remove / erase data from Aladdin
Schools are not obliged to remove data from Aladdin if it would present a disproportionate effort to do so. Also, bear in mind that before removing any information from Aladdin it is advisable to refer to your school’s data retention policy. We would strongly advise you to contact your school’s Data Protection Officer / DES / IPPN or other representative body before removing any data from Aladdin.
Section 5: Responding to a data breach

Aladdin regard the protection and security of your information as our first and most important job. Aladdin and Google’s security systems are independently audited to international standards. Aladdin is security scanned daily and Google’s data centre security is independently audited to ISO 27001, ISO 27017 and ISO 27018.

A data breach occurs when personal data has been accessed, altered, lost, or destroyed / deleted without legal basis. The most common reasons for data breach are down to human error - weak or stolen passwords, users being given inappropriate access rights, inadvertent misuse etc.

A parent / teacher / member of the public can make a complaint to the Data Protection Commissioner in the event of a breach or perceived data breach. Schools are obliged to report data breaches to the relevant authorities within 72 hours of detection.

In the event that a staff member or parent is concerned that a data breach may have occurred, for example a computer has been stolen, password hacked or revealed, restricted information emailed to wrong address, or inadvertent misuse by employee, Aladdin would recommend you report this to your school’s Data Protection Officer as soon as possible. Should the data breach involve Aladdin data, Aladdin are available to help in any way we can to assist in emergency account management, provide support, assist investigation etc.
Section 6: Data Protection Resources for Schools

In addition to the features built in to Aladdin to help schools achieve GDPR compliance, Aladdin has created a set of resources including a Schools Data Protection Self-Assessment checklist and a sample Data Protection Policy. You will find this information on the GDPR information page available in the Aladdin Help section.

Please note that schools need to be aware that they need to protect all their data, not just the data that is stored in Aladdin, but also any other systems they may use; paper records, information in filing cabinets etc.

6.1: Schools Data Protection Self-Assessment checklist

Aladdin also provides a sample School Data Protection Self-Assessment checklist, which has been designed by our Data Protection Manager to help our schools obtain a clearer view of their current data protection practices and to review their overall level of readiness to comply with the GDPR. This checklist acts as a starting point to help schools obtain a clearer view of their current data protection practices so that appropriate action, training, and guidance can be implemented in order to help your school to be as compliant as possible.

We hope you find the School Data Protection Self-Assessment checklist a useful starting point for understanding your school’s compliance with data protection obligations. Some questions require a simple Yes / No answer and others require you to supply more detailed information and / or further comments. Not every question will apply to your school and answering “No” to any question does not mean that you are in breach of any data protection legislation or regulation. Many of these questions are inter-linked, and not answering some questions might invalidate the overall response so please take your time to consider and answer each question carefully.

6.2: Sample Data Protection Policy

Aladdin has created a sample data protection policy regarding the use of Aladdin (for inclusion in your school’s Data Protection Policy statement) that schools can adapt and use in their schools. You will find this document in the Documents Gallery. You can download this document, customise it as required, and upload it to your school website.
6.3: Glossary of data protection terms:

**Data Controller:** The individual or the legal person who controls and who is responsible for the keeping and use of personal information on computer or in structured manual files. Schools are Data Controllers of the data stored in Aladdin.

**Data Processor:** The person/entity who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data during the course of his or her employment. Aladdin is a Data Processor of school data stored in Aladdin.

**Data Subject:** The living individual who is the subject of the personal information (data).

**Personal Data:** Means any recorded information, whether stored electronically, on a computer or otherwise, or in paper-based filing systems, that relates to a living individual who can be identified from that data. Personal data can therefore be factual (such as names, addresses, Eircode, dates of birth, bank details, PPSNs, etc.) or can be an opinion (such as a report). Personal data can also include pictures, photographs, videos, audio-tapes or other images of the individual.

**Processing:** Means any activity that involves use of the personal data. It includes collecting, recording or holding/storing the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

**Sensitive Personal Data:** Means personal data which comprises information about a person’s racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings.
Help

The Aladdin Help menu is located on the top right-hand corner of your Aladdin screen. Within the help menu you will find the Manuals and product tutorial videos, Webinars and an FAQ section listing regular questions and answers. To search for an answer to a question you may have, enter a keyword, for example "documents", into the search help box at the top of the Help screen, and press return. You can also view questions per category within the FAQ section by selecting the appropriate name from the dropdown box provided.

For additional information on topics such as ePayments, Money, Report cards, Documents, Groups, Attendance tracking and improvement, managing your intake in Aladdin, creating awards, and so on, please see the relevant user guides stored in the Manuals section of the Help menu.