

AWIGE.ORG (“AWIGE”) is committed to protecting your privacy when you use any of our services. This Privacy Policy explains how we use information about you and how we protect your privacy. If you have any questions about how we look after your personal information, please contact AWIGE’s Data Protection Officer: Ms. Belinda Siago, at contact@awige.org Personal information is anything that directly or indirectly identifies and relates to a living person, such as a name, address, telephone number, etc. We may need to use some information about you to support and promote AWIGE, to contact you about our services to get your views, which helps us to manage them, to help investigate any concerns or complaints you have about our services, to check the quality of services, to help with research and planning of new services.

There are a number of legal reasons why we will need to collect and use your personal information in different circumstances. Generally, we collect and use personal information where you, or your legal representative, have given consent, you have entered into any sort of agreement or contract with us, it is necessary to perform our statutory duties or other legitimate purposes, it is necessary to protect someone in an emergency, it is required by law, it is necessary for any employment-related purposes, it is necessary for any possible legal cases, it is necessary for archiving, research, or statistical purposes. If we have consent to use your personal information for any particular reason, you have the right to remove your consent at any time. If you want to remove your consent, please contact contact@awige.org to let us deal with your request. The law gives you a number of rights in relation to what personal information is used by AWIGE, and how it is used. These rights are listed below. You can ask us to provide you with a copy of the personal information that we hold about you, to correct personal information about you which you find as necessary, to delete personal information about you if you think we no longer should be using it, to stop using your personal information.

If you think it is wrong, until it is corrected, to transfer your personal information to another provider, to not use automated decision-making processes to make decisions about your data, In some circumstances, we can use other organisations to either store personal information or use it to help deliver our services to you. Where we have these arrangements, there is always an agreement in place to make sure that the organisation complies with data protection law. We can have a legal duty to provide personal information to other organisations to prevent any crime or fraud. For all these reasons, the risk must be serious before we can override your right to privacy. If this is the case, we will make sure that we record what information we share and our reasons for doing so. We will let you know what we have done and why, if we think it is safe to do so. We closely co-operate with StorkSchool.com provider enabling remote EdTech work opportunities to female African teachers registered with us. This way we pass your data to them.

We have a legal duty to make sure we hold your personal information (on paper or / and electronically) in a secure way, and to only make it available to those who have a right to see them. Examples of our security include: encryption - meaning that information is hidden so that it cannot be read without special knowledge (such as a password), pseudonymisation - meaning that we can use a different name or identifier to hide parts of your personal information from view (this means that someone outside of AWIGE could work on your information for us without ever knowing it was yours), controlling access to systems and networks allows us to stop people who are not allowed to view your personal information from getting access to it. Training for our staff allows us to make them aware of how to handle personal information (and how and when to report when something goes wrong), regular testing of our technology and ways of working (including keeping up to date on the latest security updates - commonly called patches). The majority of personal information is stored on systems in the UK or the EU. However, there are some occasions where your information may leave the UK / the EU either to get to another organisation, or where it is stored in a system outside of the UK / the EU.

We will only hold your personal information for as long as it is necessary to fulfil our legal duties or statutory purposes. For all the independent advice about data protection, privacy and data sharing issues, you can contact the Information Commissioner Office in the UK at: www.ico.org.uk



www.awige.org