JFS ONLINE REPORTING ACCEPTABLE USE POLICY

SIMS Learning Gateway (SLG) online reporting to parents is provided for parents/carers and employees of JFS students. Access by any other party is strictly prohibited.

This Policy aims to ensure all relevant aspects of the Data Protection Act (1998) and Fair Processing Policy are adhered to.

This Policy aims to promote best use of the SLG system to further the communication and freedom of information between JFS and Parents\Guardians. The Act states that the data can only be used for specific purposes and therefore all data will be recorded, processed, transferred and made available according to strict guidelines. Information made available through the SLG system is confidential and protected by law under the Data Protection Act 1998. To that aim:

- Users must not distribute or disclose any information obtained from the SLG system to any person(s) with the exception of the student to which the information relates or to other adults with parental responsibility.
- Users should not attempt to access the SLG system in any environment where the security of the information contained in the SLG system may be placed at risk e.g. a cybercafé.

Whilst every effort is made to ensure that the systems are working correctly, JFS will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, no-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or user errors or omissions. Use of any information obtained via the SLG system is deemed to be at the user's risk.

By using SLG you signify that you are a JFS parent/carer and that you have been authorised to use the system by JFS.

The School agrees to:

1. Provide user accounts for all contacts with parental responsibility.
2. Maintain accurate and up-to-date records.
3. Support users in accessing SLG information.

You agree:

1. To only access sites authorised for you to do so.
2. Not to reveal your password to anyone.
3. To report any security concerns immediately to the school.
4. To observe security guidelines as all times, following the requirements of the Data Protection Act (1998) and Computer Misuse at (1990).
5. To access all information in a secure and controlled environment.

You agree not to:

1. Attempt to access the service using another person's login details.
2. Introduce or attempt to introduce any form of malicious software into the network.
3. Change or attempt to change or remove software.
4. Carry out unauthorised configuration changes.
5. Deliberately delete files.

If you are identified as a security risk to the School's ICT facilities you will be denied future access to the system.

Last Updated: 10 December 2015