USH Acceptable Use Policy for the SIMS Learning Gateway

Introduction.

Parents are offered online access to the School's Information Management System (SIMS) via the SIMS Learning Gateway (SLG). Through this website, parents can access information produced by the school about their child via a secure Internet connection. This policy applies to all those who access the USH SIMS Learning Gateway system (subsequently referred to as the SLG system). This policy applies whenever and wherever information is accessed, whether the computer equipment used is owned by USH or not.

Access is granted strictly on condition that the individual formally agrees to the terms of this Policy through the return slip attached to this policy.

Authorised SLG Users.

Only relevant members of staff and persons who are legally responsible for students currently attending the school are provided with online access to the USH SLG system. Even then they only have access to information relating to the students where they have that legal responsibility.

Requests for access to the SLG system must be made to USH using the SLG Parental Access Return Slip. The authorising member of school staff and the parent/guardian/carer concerned must confirm that there is a legitimate entitlement to access information for the student(s). The name(s) of the student(s) must be stated on the SLG Parental Access return slip which the school will keep for audit purposes. It is important to manage access to the schools SLG system effectively. The school is required to arrange the removal of access of users who are no longer entitled to access to that SLG within 1 week of being informed of that change in status.

Acceptable Use of the SIMS Learning Gateway – All Users

- Access to the SIMS Learning Gateway is a privilege, not a right. Users are responsible for their behaviour.
- Conditions of use are respected: any breach of the conditions of use may lead to withdrawal of a user's access. In some instances, such a breach could lead to criminal prosecution; in the case of staff it may be considered a disciplinary matter.
- The system should not be used in any way that might bring the name of the school or Trust into disrepute.
- Staff, parents and students are expected to use the resources for the purposes for which they are intended.
- All users accept personal responsibility for reporting any misuse of the system to a teacher or to a member of the school technical team.
- No user should access, create, transmit, display or publish any material, including images and data from the SLG system, which is likely to cause offence, inconvenience or needless anxiety.
- No user should create, transmit, display or publish any material, including images and data from the SLG system that might be considered defamatory.
- Staff, parents and students should not make unauthorised attempts to access data and resources on the SLG system by bypassing security or password protections.
- No user should take any action designed or likely to cause corruption or destruction of other users' data, or violate the privacy of others.
- Users should inform the school immediately if a security problem is identified. They should not demonstrate this problem to other users.
- Users should inform the school immediately if they appear to have access to content that is not authorised. They should not demonstrate this problem to other users.

Information Security

This Policy is intended to minimise security risks. These risks might affect the integrity of USH data, the Authorised SLG User and the individuals to which the SLG data pertains. Information made available through the SLG system is confidential and protected by law under the Data Protection Act 1998. In order to comply with this Act:

- 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 for that student.
- 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 such as an Internet café or public place.
- Users must not transfer information from the SLG system to any form of portable media such as pen drives or by electronic means such as e-mail without the express permission of the school
- Passwords for SLG accounts should be complex and consist of at least six characters including a combination of capital letters, lower case letters and numbers. Ideally, at least one symbol should be included as well.
- Users must always keep their individual user name and password confidential. These usernames and passwords should *never* be disclosed to anyone. Never use anyone else's username or password.
- If you think someone has learned your password then contact the school or change it immediately if possible.

Denial of Access

Users are liable for any potential misuse of the system and/or breach of the Data Protection Act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document. USH reserves the right to revoke or deny access to the SLG system of any user under the following circumstances:

- If the validity of parental responsibility is questioned.
- A Court ruling preventing access to child or family members is issued. Please advise us if such a ruling is in place.
- Where a user or users are found to be in breach of the SLG Acceptable Use Policy.
- If any child protection concerns are raised or disputes occur the school will suspend access for all parties concerned pending investigation.
- If a user is identified as a security risk.

Enquiries.

SLG users should forward any enquiries about the USH SIMS Learning Gateway system to Lisa Harding
email: lisa.harding@ushschool.org