HILL HOUSE SCHOOL

Acceptable Use Policy

Scope of this Policy

This policy applies to all members of the school community (except pupils), including staff, parents, governors and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

This policy works in conjunction with the school's bring your own device (BYOD) policies. This policy concerns the access and use of school equipment but also has general guidelines on general behaviour that should also apply to the BYOD scheme.

Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.
- Staff should use only the school email system to contact pupils and parents and then only on official school matters.

Using the school's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

Printing

Printed material should be collected from the school's printers as soon as possible. Where data is of a personal or sensitive nature these must be printed to a secure location (the school office or staff room) or printed using the 'print release' method. Practical guides on printing can be found in the school's "GDPR help sheet" document which can be found on the N drive.

Security

The school has an obligation to take all practicable measures to protect personal and sensitive data it processes. Under GDPR regulation such 'appropriate technical and organisational measures' is referred to as the 'security principle'. Members of staff are expected to understand how such technical and organisational measures pertain to them and to act accordingly. This document details all such measures staff should be aware of and comply with. The school will provide training, technical infrastructure and management to enable staff to comply. In addition, staff should read the 'Internal Operations Guidelines' document that covers details of procedures and processes staff are expected to adhere to.

- All paper copies of personal and sensitive data need to be filed securely.
- Access to paper documents should be restricted to the staff that need access to them.
- Paper documents should be retained only as long as such data is required and in accordance with the school's Storage and Retention of Records Policy.
- Electronic personal and sensitive data should be secured by password and if being used off-site via encryption.

- Paper or electronic data should be stored only if there is a legal basis for keeping such data.
- Paper and electronic data should be deleted in accordance with the school's retention policy.
- Staff should never attempt to access or modify data without due authority.
- Data should never be disclosed to parties (Hill House or external) without the correct authority.
- Staff should verify the identity of any organisation or individual with whom they share data or who have requested alterations to such data.
- Staff should read, and understand, all school policies and attend data protection training when required.
- Certain systems may require multi-factor authentication methods when accessed off-site. Staff (academic and non-academic) are not exempt from these restrictions; where access to the multi factor technology is challenging the school will endeavour to help staff but these restrictions are not optional.
- Staff are given regular and mandatory cyber-security awareness training.
- Staff should take care when accessing messages (email, text or voice) to ensure they validate senders and do not breach cyber security or GDPR regulations.
- Where staff suspect they are in receipt of a fraudulent or malicious communication they have a responsibility to report this to the schools IT department.

It should be stressed that the school considers its responsibilities regarding data protection and security as priority. Staff should be aware that a breach of data protection policy carries a significant financial penalty and will cause distress to individuals and embarrassment to the school. As such any breaches by staff may result in significant disciplinary measures and penalties.

Working off-site

The school recognises that staff need to take data off-site from time to time as part of their professional activities. It is important that staff understand the implications and guidelines around working off-site.

Personal and sensitive data should only be taken off-site only when absolutely necessary and returned to school as soon as possible. Data should be destroyed at school and not disposed of off-site.

A practical guide to working in such situations is listed as part of the school's "Data protection (GDPR) internal operations guidelines" document which is available on the school's N drive.

Physical data

Physical copies of personal and sensitive data should be taken off-site only if absolutely necessary and kept secure at all times. Data should be returned as soon as work is complete and never disposed of off-site.

Electronic data

The school permits users to take electronic data off site but in the case of personal and sensitive data certain precautions must be in place; data must always be secured by password AND encryption. Users should attempt to use the school's systems remotely rather than copying data and storing data on devices (such as tablets, mobile phones, laptops etc).

Compliance with related school policies

Staff should ensure that they comply with all of the school's policies relating to I.T. usage at school.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter as per the school's Disciplinary Procedure. In addition, a deliberate breach may result in the school restricting a member of staff's access to school IT systems.

If any member of staff becomes aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the school's designated safeguarding lead (Mrs Belinda McCrea). Reports of this nature will be treated in confidence.

Reviewed: September 2021