THE HOLMESDALE SCHOOL
PUTTING PROGRESS FIRST

POLICY FOR	**Staff Acceptable Use of Technology**
PERSON RESPONSIBLE	**DSL**
REVIEW DATE	**October 2021**
NEXT REVIEW DATE	**October 2022**

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use The Holmesdale School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand The Holmesdale School expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that The Holmesdale School systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within The Holmesdale School both professionally and personally. This may include use of laptops, tablets, digital cameras and email as well as IT networks, data and data storage and online and offline communication technologies**.**

2. I understand that The Holmesdale School Acceptable Use of Technology Policy (AUP) should be read and followed in line with THS staff code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school’s ethos, code of conduct and safeguarding policies, national and local education and child protection guidance, and the law.

Use of Devices and Systems

4. I will only use the equipment and internet services provided to me by the school, for example school provided laptops, tablets, mobile phones and internet access, when working with learners.

5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Reasonable personal use of school IT systems and/or devices by staff is allowed.

Data and System Security

6. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    - I will use a ‘strong’ password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. Leaders should include any specific requirements, for example, how often passwords should be changed etc.
    - I will protect the devices in my care from unapproved access or theft. I will not leave my devices in a car overnight or leave them unsupervised in public places or transport.
    - I will ensure that no family members or cohabitees will have access to school devices*.*

7. I will respect THS system security and will not disclose my password or security information to others.

8. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the THS IT team*.*

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.

10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with THS Data Protection policy.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks or CDs, should be suitably protected such as using an encryption method approved by the IT team.

11. I will not keep documents which contain school related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones.

12. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

13. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

14. I will not attempt to bypass any filtering and/or security systems put in place by the school.

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT team as soon as possible.

16. If I have lost any school related documents or files, I will report this to the IT team and school Data Protection Officer as soon as possible.

17. Any images or videos of learners will only be used as stated in the school camera and image use policy.
    - I understand images of learners must always be appropriate and should only be taken with school provided equipment and

taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

18. I am aware of safe technology use in the classroom and other working spaces, including appropriate supervision of learners, as outlined in the school online safety policy.

19. I have read and understood the school online safety policy which covers expectations for learners regarding mobile technology and social media.
20. I will promote online safety with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used on site.
    - creating a safe environment where learners feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) (Emma Beal) or the DSL team as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with learners is appropriate.

21. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the school online policy.

22. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music are protected, I will not copy, share or distribute or use them.

THE HOLMESDALE SCHOOL

PUTTING PROGRESS FIRST

I have read, understood and agree to comply with The Holmesdale Staff Acceptable Use Policy

Name: ……………………………… Signed: ………………………….... Date: ………………..

Accepted by…………………………………… Date:…………………….