THOMAS JOHNSON LOWER SCHOOL

Hurst Grove, Lidlington, Bedfordshire MK43 0SB
Tel: 01525 402377 / 01525 404743
email: office@thomasjohnsonschool.co.uk
Head teacher: Mrs M Haimes

Acceptable User Policy

Responsibility	Head teacher, Staff, Pupils, Parents and the Governing Body
Review Date	February 2024
Approved by Full Governing Body	February 2021
Storage: Electronic	School website

Introduction
This document outlines the purpose and management of computing technology at Thomas Johnson Lower School. This applies to all laptops, PCs, chromebooks, i-pads and mobile technology.

The requirement to ensure that pupils, staff, trainees, governors, volunteers and indeed all others in the school community are able to use the internet and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound. This Acceptable User policy (AUP) is to promote safe and appropriate use. As such it should be understood in the context of 'Safeguarding, child protection' and 'behaviour' policies that the school already has in place, as well as other existing policies in respect of its employees.

Given the array of new technologies now available to use for educational purposes and everyday life, the intention of this policy is:

- To maximise e-safety for all members of the school community
- To help everyone understand the potential risks
- To provide guidelines (including how the policy will be regulated and any sanctions) for safe and appropriate school and home use

As such the school more specifically intends:

- To provide a secure network for the school and secure means of home/school access by using a VPN with encryption on staff laptops
- To monitor traffic, log incidents and act accordingly using the CE-OP (Child Exploitation and Online Protection) website and in discussion with our IT support company
- To establish key standards and behaviour for e-safety across the school and the wider community by informing parents and carers of ways to safely search on all digital devices and how to report cyber bullying and/or inappropriate interactions

- To coordinate the activities for the school related to promoting best practice in e-safety, including the publication of guidelines and acceptable use policies for staff, pupils, parents and governors
- To ensure that we adhere to e-safety issues related to new government policies affecting schools
- To monitor the schools responses to e-safety matters and act accordingly

E-safety is a whole school issue, not something that is simply the responsibility of the Computing Subject Leader. As such the whole school has a responsibility to promote it.

Aims
The AUP aims to:

- Reflect the understanding that all members of the school community have responsibilities towards themselves, towards others and towards the school and that these responsibilities are not confined to the physical location of the school.
- Enable young people to develop their own protection strategies when adult supervision and technological protection are not available.
- Provide information on where to seek help and how to report incidents
- Help young people to understand that they are not accountable for the actions that others may force upon them, but that there are sanctions that the school will impose if they act inappropriately when on line.
- Provide guidelines for parents, carers and others on safe practice
- Ensure that the practice that it promotes is regularly monitored and reviewed
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme

Strategies
Parents will be informed through a home school agreement. E- Safety guidelines will be displayed in all computer areas within the school community. (See E-Safety Policy)

Children
E-safety will be the first unit of work undertaken in all year groups, every September. This will ensure the children are aware of e-safety, and will include all digital devices and use of social media. E-Safety will remain high profile throughout and regular reminders and updates will be delivered to the children throughout the academic year.

Passwords
Staff passwords are kept private and only the holder can change them. It is accepted that from time to time passwords will be forgotten in which case the Computing technician can help them create a new one. Generic children's usernames and passwords are given to them and are held on file by the Computing Subject Leader.
A breach of the agreement could result in the loss of internet privileges.

E-mails
It is accepted that staff may send e-mails and attachments to recipients outside the school and these should only be sent via the school email address allocated to each member of staff. Children may only do so under the supervision and direction of their teacher.

Anti-virus and filtering
The school has up to date anti-virus and operates filtering on all computers used by the children. The filtering and anti-virus monitoring is overseen by Partnership Education, our IT provider.

Inappropriate content and language
There will be zero tolerance to the use of inappropriate language and content on any Computing equipment in the school community. The type of language that is used in e-mails should be no different from that used in face to face situations .

Staff
The school aims to establish a clear understanding of the responsibilities of all those involved in the education of children with regard to e-safety. It is expected that all staff will read and seek clarification of this AUP policy if required. Staff will review their responsibilities under this AUP and complete the Staff Agreement Form.
This policy will be updated every three years or sooner if necessary.

Appendix 1
Guidelines for Acceptable Use of Computing with Thomas Johnson Lower School

Children are taught these guidelines and expected to follow them.

- My password is private and if I forget it I will tell my teacher. I will never use another person's password or username.
- When I am finished using the computer I will always 'log off' and when using a digital device will clear the 'Apps' used
- I will only use the internet for schoolwork and only access the sites my teacher has asked me to access
- I will use the same language on line/in an e-mail as I would when having a face to face conversation
- I will never send attachments with an e-mail without the permission from my teacher
- I accept that the school cannot be held responsible for personally owned devices brought into school or taken on a trip/visit
- If anything inappropriate appears on my computer screen/mobile device I will immediately minimise it (as taught in school) and inform my teacher

Appendix 2

Guidelines for Acceptable Use of Computing with Thomas Johnson Lower School Acceptable User Policy – Staff Agreement Form

This policy covers the use of digital technologies in school: email, Internet, intranet and network resources, learning platform, software, handheld devices, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- All school work should be completed on the laptop issued by Thomas Johnson Lower School
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality policy.
- Exporting or updating of Integris data must only be on school devices.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system for any school business. (Which is currently: gmail)
- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software.
- USB/ jump drive/flash drives should not be used in any school devices or in school to restrict spread of viruses. Failure to abide by this expectation could result in disciplinary action.
- I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems. I will do this by returning any 'loaned item back to the school premises fortnightly, making sure the item is switched on and updated before removing it from site again.
- I will not use personal digital cameras or any device with camera capabilities for taking and transferring images of pupils or staff without permission and will not store images at home without permission. In cases where permission is given, before the device leaves the school premises, images must be transferred onto the school network and after uploading, the memory card of each camera or device should be erased. Good practice would be to upload and delete memory cards the next working day.

- No camera/digital/mobile devices belonging to persons not employed by the school should be used to record images and or video's
- Photographs of children must be in line with Parental Photography Consent
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with or associated with my professional role or the school.
- I agree and accept that any computer, laptop, handheld device (including iPad) loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

I understand that failure to comply with this agreement could lead to disciplinary action.

iPad Acceptable Use Policy for Thomas Johnson Lower School

User Responsibilities

- The iPad is a school tool designed to enhance classroom practice.
- The iPad screen is made of glass and is therefore subject to cracking and breaking if misused; never drop or place heavy objects (book, laptops etc) on top of the iPad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Do not subject the iPad to extreme temperatures.
- Do not store or leave unattended.
- Users may not photograph any other person without that person's consent
- Photographs of children must be in line with Parental Photography Consent
- The whereabouts of the iPad should be known at all times.
- It is a user's responsibility to keep their iPad as safe and secure as possible.
- Images of other people may only be made with the permission of the person, or parents of the person, in the photograph.
- Upon returning the iPad to the school, it is the users responsibility to delete all pictures, passwords and e-mails from the device.
- If the iPad is lost, stolen or damaged, the Computing Co-Ordinator, ICT Technician or Head Teacher must be informed immediately.