**ICT SYSTEMS ACCEPTABLE USE POLICY FOR STAFF WITHIN BRIGANTIA LEARNING TRUST**

# Introduction

The purpose of this policy is to provide a set of standards for users of Information & Communications Technology (ICT) systems in Brigantia Learning Trust.

The Trust offers new and exciting opportunities for staff, children & young people, and visitors by providing a rich and diverse range of ICT facilities. The Trust can only provide these excellent facilities by maintaining a robust set of policies and procedures, and by adhering to current legislation relevant to ICT.

# Scope

This policy applies to all members of staff using ICT systems within the Trust. It is essential that all users read, and abide by these guidelines and make themselves aware of their responsibilities and the potential liabilities of using ICT systems. “ICT Systems” means, for example, any piece of computing equipment, printer, photocopier, telephones, network and attached equipment, including where personal devices are attached to a BYOD (Bring Your Own Device) or guest network. This is not an exhaustive list and in the case of any doubt, clarification should be sought from Senior Management or ICT Technical Staff.

**Legal and Organisational Requirements**

In addition to anything set out in this policy, all users are bound by the following:

* [General Data Protection Regulation (GDPR)](https://www.eugdpr.org/)
* [Computer Misuse Act 1990](https://www.legislation.gov.uk/ukpga/1990/18/contents)
* [Copyright, Designs & Patents Act 1988](https://www.legislation.gov.uk/ukpga/1988/48/contents)
* Brigantia ICT Security Policy
* Brigantia Online Safety Policy
* Brigantia Staff Code of Conduct

Breaches of this policy will be treated by the Trust as a serious disciplinary offence, and may result in ICT facilities being withdrawn immediately, pending investigation and further action.

The Trust reserves the right to examine, move, or delete any files held on its computer systems, and must monitor internet access (including search terms used), and communications exchanged. Each Academy may also keep a log of telephone calls made and received.

# General Computer Use

ICT systems must be treated with care and used only in accordance with the operating instructions. These are available from ICT Technical Staff if required.

No attempt must be made to use equipment which is labelled out of order. Likewise, equipment must not be used if there is reason to believe that it may not be in safe working order. Any apparent fault with hardware should be reported promptly to ICT Technical Staff.

The use of any ICT equipment for downloading, storage, printing and/or transmission of materials which are illegal or which the Trust considers to be obscene or offensive is strictly prohibited. Some examples are - pornographic, obscene, violent, offensive, bullying materials. If you are in any doubt about any materials, ask a member of staff.

Users must take all reasonable steps to exclude and avoid the spread of malicious software, e.g. viruses, and must co-operate fully with all measures instituted by the Trust to prevent the spread of such software. In particular, users must not install or execute on a Trust computer any software obtained from a third party source, unless such software has been approved by ICT Technical Staff.

Priority must be given to use of resources for work or educational use. Personal use must not:

* Be of a commercial or profit-making nature, including private consultancy, or for any other form of personal financial gain. This includes using the email system for advertising items for sale
* Be of a nature that competes or conflicts with the Trust in any way
* Be excessive
* Interfere with your work or study. An example, of this would be personal use outside of allocated break times

If staff are in any doubt about what constitutes acceptable and appropriate use, they should seek the advice and guidance from their line manager, or ICT Technical Staff.

Where any of the Trust’s ICT facilities are used to access any external network and/or computer facilities, staff must also abide by any additional conditions pertaining to the external facilities that are imposed by the providers of such facilities.

Staff must not by any deliberate or careless act or omission, jeopardise or seek to jeopardise the integrity of any ICT equipment or its software or any information stored within it or accessed through it.

Staff must not access or attempt to access any ICT equipment, software or data which they are not authorised to access.

Staff must take all necessary steps to protect and maintain the security of any equipment, software, data, storage area and/or passwords allocated for their use. Passwords must not be printed, stored online, or shared with others.

Food and drink should not be consumed near computer equipment.

Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so.

A computer must never be left unattended whilst logged on. This is particularly important in a classroom or area where other people could gain unauthorised access to it. This is a serious breach of this Policy and may be treated as misconduct.

The amount of storage space for users’ data is finite. All staff should exercise good file and folder management to avoid wastage from duplication of information. Furthermore, users should avoid storing unwanted, outdated or irrelevant files.

Under no circumstances should non-ICT Technical Staff connect or disconnect any equipment to/from data points.

All computers have some restrictions in place. That is, the full functionality that would be expected from a personally owned computer will not be available. This is to ensure the device remains fully operational and security procedures are in place in case of unauthorised access.

**Portable Storage Devices (USB memory sticks, portable hard drives etc.)**

The Trust strongly discourages the use of any portable storage media. With the increasing availability of cloud services and remote access, portable storage media is no longer necessary. Moreover, it is strictly forbidden to use portable storage devices to store any file containing personal data, and such action is a serious breach of this policy which could be treated as misconduct, or in some cases, gross-misconduct.

# Copyright

Computer programs on the ICT systems are protected by copyright. The Trust has the appropriate licences for all of the software on its systems. Users must comply with all their legal obligations concerning copyright, and must not copy any software or other data without the prior authorisation from the copyright owner. Such action would be in breach of copyright law. Authorisation from the copyright owner does not constitute permission to store, execute or download on the Trust network. This includes storage of licensed music downloaded from the internet, or transferred from external storage media.

# Internet

All Internet access, including search terms, is logged.

It is a serious offence to attempt to bypass any filtering or security system. An example of this would be accessing or attempting to access proxy sites or anonymisers on the internet. Any such activity may lead to disciplinary action and may, in certain circumstances, be treated by the Trust as gross misconduct. If you think you have a legitimate request to download something that is blocked by one of the Trust security systems, you should submit a request to ICT Technical Staff who will evaluate the request and take the appropriate action.

Reasonable private use of the internet is permitted but should be kept to a minimum and should not interfere with your work. Excessive private access to the internet during working hours, and outside of allocated break times, may lead to disciplinary action and may, in certain circumstances, be treated by the Trust as misconduct.

The sites accessed by you must comply with the restrictions set out in this policy. Accessing inappropriate sites may lead to disciplinary action and may, in certain circumstances, be treated by the Trust as gross misconduct.

The amount of available disk space is finite and due care must be taken when downloading files.

In the interests of information security and online safety, the Trust restricts access to certain sites and prevents the downloading of certain types of file and content. You must not download, or attempt to download programs, viruses, hacking tools, copyrighted material. Likewise, you must not access, or attempt to access, sites which offer or promote such downloads. In some case, such activity is illegal. If you are in any doubt at all, you should contact ICT Technical Staff.

# Portable devices – e.g. laptops, tablets etc.

Portable devices issued to staff remain the property of the Trust. Therefore, only software licensed to the Trust may be installed on these devices, unless authority has been sought from ICT Technical Staff.

Portable devices that are used at home must not be used by other family members.

The increased use and ownership of portable devices has been accompanied by a rise in theft because they are easy to steal and open to opportunistic theft. Apart from the loss of the hardware there may be the loss of sensitive commercial information or personal data which is of a far higher value than the device itself. Users of portable devices must take all reasonable care to prevent theft or loss of, and damage to, laptops and the software and data stored thereon.

Sensitive personal data must not be stored on portable devices. Anyone wishing to access sensitive personal data must do so using the available methods of remote access.

Where portable devices are used in the classroom or other learning environment, the teacher is responsible for checking the devices before and after use. Any losses or damage must be reported to ICT Technical Staff immediately.

**Remote access**

Any member of staff using remote access must do so responsibly, safely, and legally, and take all reasonable steps to ensure that the information on screen cannot be seen by anyone else, including family members.

# Telephones (including Trust-owned mobile telephones)

Personal use of telephones (including Trust-owned mobile telephones) is permitted for staff. However, this should not interfere with work and should not be excessive.

Calls to premium and other high rate numbers, for example, Directory Enquiries, should be avoided. There are alternative methods of obtaining telephone numbers and these should be exhausted before using premium rate services.

Where personal use of a telephone (or fax machine) will incur a high cost, for example, international calls, this should be by arrangement with the appropriate line manager in advance of the call being made. The Trust reserves the right to charge for personal calls.

It is an offence to use a mobile telephone whilst driving, without a hands-free kit. Users of Trust-owned mobile telephones may also be subject to disciplinary action if found doing so.