Acceptable Use Policy

Responsibility	Finance & Resources	
Status	Statutory	
Ratification date	24 11 2020	
Review cycle / date	1	Autumn 2021
Reference	010/3	

The school has a detailed Risk Register which the Trust Board uses to monitor and measure the impact of its decisions as well as informing its planning.

To ensure that Risk Management permeates the working of the Trust Board, this policy is referenced in the Risk Register and the committee responsible for the policy should consider the “likeliness” and “impact” level for the appropriate risks.

Contents

1 Introduction

Networked resources, including Internet access, are potentially available to students and staff in the school. All users are required to follow the conditions laid down in the Policy. Any breach of these conditions may lead to withdrawal of the user's access to the network, monitoring and/or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational and work related administrative purposes, and may only be used for legal activities consistent with the rules of the school.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to students in the use of such resources. Unsupervised student-use of the school's network or internet is not allowed. All computer systems will be regularly monitored to ensure that they are being used responsibly.

The Responsible Person under this Policy will be the **Deesh Grewal, Lead Practitioner** or such other person from time to time designated by the Head Teacher.

2 Linked Policies

- Staff Code of Conduct
- Child Protection and Safeguarding Policy
- Positive Handling Policy
- Disciplinary Policy and Procedures
- Online Safety Policy
- Acceptable Use Agreement
- Data Protection and GDPR Policy
- Whistleblowing Policy

3 Conditions of use

3.1 Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and students will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for immediately reporting any misuse of the network to the Responsible Person.

3.2 Limitation

Users may not hold themselves out in any correspondence as representing the school unless they are specifically authorised to do that. Any personal view relating to school or the local authority must be endorsed with a disclaimer making that clear.

3.3 Monitoring and Consent

The School has the right to monitor employees' use of computer equipment where there is evidence to suggest misuse. (Regulation of Investigatory Powers Act 2000).

Any user of network services shall be deemed to consent to the monitoring of their use of those services and to the copying and retention of any data arising from that use by the Responsible Person or anyone authorised by them and the disclosure, copying and transmission of that data for any purpose reasonably connected with the running of the school.

4 Acceptable use

Users are expected to utilise the network systems in a responsible manner. It is not possible to set rules that cover everything that is and is not acceptable but the following list provides guidelines for responsible use:

4.1 Guidelines

These guidelines include, but are not limited to, the following:

1. Users must login with their own user ID and password and must not share this information with other users. They must also log off after their session has finished.
2. Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
3. Be polite when communicating via the network – never send or encourage others to send abusive messages.
4. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
5. Do not use language that could be construed to incite hatred against any ethnic, religious or other minority group.
6. Privacy – do not reveal any personal information (e.g. Home address, telephone number) about yourself or other users. Do not gain access to other users' files or folders.
7. Password – do not reveal your password to anyone. If you think someone has learned your password then change it immediately. If you are not able to do this, contact the IT Technicians to ensure that it is changed.

8. Electronic mail – is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the police or other authorities. Do not send anonymous messages or forward chain mail.
9. Disruptions – do not use the network in any way that would disrupt use of the network by others.
10. Students will not be allowed access to unsupervised or unauthorised chat rooms and should not attempt to gain access to them.
11. Staff or students finding unsuitable websites through the school network should immediately report the web address to their class teacher or academic tutor so that it can be blocked.
12. We strongly advise against the use of USB storage devices as they can introduce viruses and or loss of data. If in doubt, check with ClickOn IT.
13. Do not attempt to visit websites that might be considered inappropriate. Such sites would include those relating to illegal activity. All sites visited leave evidence in the network log, if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
14. System utilities and executable files (other than those needed for educational purposes) will not be allowed in students' work areas or as email attachments.
15. Files held on the school's network will be regularly checked by IT Technicians (ClickOn IT).
16. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the network does not occur.

5 Unacceptable use

Examples of unacceptable use include but are not limited to the following:

1. Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. This would include making postings on social sites such as Instagram, Facebook or Twitter.
2. Accessing or creating, transmitting or publishing any defamatory material.
3. Receiving, sending or publishing material that violates copyright law, this includes through video conferencing (Google Meets) or broadcasting (Google Stream, Streamyard)
4. Receiving, sending or publishing material that violates the Data Protection Act or breaching the security this act requires for personal data.
5. Transmitting unsolicited material to other users (including those on other networks).
6. Unauthorised access to data and resources on the school network system or other systems.
7. User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.
8. Unauthorised download or installation of software.
9. Using any network facility in a way which does or might bring the school into disrepute or expose it or anyone employed at the school to a civil or criminal claim or charge.
10. Systematic (as opposed to occasional) use of facilities in connection with a non-school business or personal activity and any such use which involves the unauthorised use of printer consumables.

6 Services

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any loss or damage suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system, by third parties or your errors or omissions. Use of any information obtained via the network is at your own risk. The school does not warrant that the system is secure or that your personal data cannot be accessed by third parties and no responsibility will be accepted for the consequences of this. Users are warned not to keep personal passwords or private data on the system.

7 Network Security

Users are expected to inform ClickOn IT or the Responsible Person immediately if a security problem is identified. Do not demonstrate this problem to other users. Users identified as a security risk may be denied access to the network or have their use regulated.

7.1 Physical security

All members of staff are expected to ensure that portable IT equipment such as laptops, tablets and webcams are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes, for example, will need to be physically protected by locks and or alarms.

8 Wilful Damage

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

9 Media Publications

Named images of students and staff (e.g. photographs, videos, streams, presentations, web pages etc.) must not be published under any circumstances. Written permission will be obtained before photographs of students are published on the school website.

Students' work will only be published (e.g. photographs, videos, presentations, web pages etc) if parental consent has been given.

10 Behaviours that may result in disciplinary procedures

10.1 Gross misconduct

Examples:

1. Any use of network services which is or is incidental to the commission of any Criminal *act – for example in relation to child pornography, or fraud*

2. Visiting pornographic sites or viewing sexually explicit materials except where this forms an authorised part of the employee's job *(for example 'an investigation by an approved member of staff resulting from a suspicion or complaint').*

3. Harassment – using network services to forward or publish inappropriate emails or printed emails sent to a colleague or a third party, even if sent or published as a joke. *Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace.*

4. Using network services to create, forward or publish obscene, offensive or racist jokes or remarks.

5. Downloading or installation of unlicensed products

6. Using chat rooms to arrange sexual activity or to use offensive, racist or obscene language.

7. Software media counterfeiting or illegitimate distribution of copied software

8. Using the school network or printing resources to support an external business or activity other than by sending and receiving emails or accessing the internet during work breaks.

9. Obtaining credit or goods for personal or other non-school use by making representations of authority or status within the school which might induce the supply of such credit or goods.

10.2 Misconduct

Examples:

1. Frivolous use of computing facilities that risks bringing the school into disrepute or that waste staff time, such as the distribution of 'chain emails' or other forwarded messages which are spread by forwarding.

2. Using network facilities to enter into contracts binding the school without authority. Contracts are legally binding agreements and an employee must not enter into any agreements via the internet to

procure goods or services where the school is liable for this contract, without first consulting the school's financial procedures. Where such contracts are entered into for reasons of personal or third party gain this will be gross misconduct

3. Deliberate or reckless introduction of viruses to systems

This list is not exhaustive, but sets out the framework of the school's approach to the misuse of computing systems.

Any authorisation envisaged by this Policy must be given in writing or by email by the Responsible Person or the Head Teacher.

Confirmation of Receipt of Acceptable Use Policy

Name:

Date of joining school:

Post:

Date of induction:

Name and designation of member of staff responsible for induction:

I confirm that I have reviewed and read the School's Acceptable Use policy.

Signature: _____

Name: _____

Date: _____

Please sign and return this form to the Designated Safeguarding Lead.