Burnside College
E-safety and ICT Acceptable Use Policy - Staff

Introduction

Burnside strongly believes in the educational value of ICT and recognises its potential to enable staff in delivering and supporting the curriculum. Burnside also believes that it has a responsibility to educate its pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and other related technologies. To this end the expectation of the School is that staff will play an active role in implementing E-safety and acceptable use through effective classroom practice.

This policy applies to the school governing body, all teaching and other staff, whether employed by the Local Authority or employed directly by the school, external contractors providing services on behalf of the school or the Local Authority, teacher trainees, other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

E-safety and ICT Acceptable Use is about ensuring that you, as a member of staff at the School can use the Internet, email and other technologies available at the school in a safe and secure way. This policy covers the use of ICT systems, the use of telephones, online tools, email and the internet provided by the School to support learning. It also extends to out of school facilities e.g. equipment; printers and consumables, managed learning environment and websites (where applicable).

The School recognises that for staff to effectively deliver and support the curriculum they must be able to make use of the ICT facilities of the School and have the opportunity to expand and develop the teaching material associated with their work. However, the School expects that all staff, will at all times, maintain an appropriate level of professional conduct in their own use of the School's ICT facilities.

Listed below are the terms of this agreement. Staff are expected to use the ICT facilities of the School in accordance with these terms. Violation of these terms will result in disciplinary action in accordance with the School's Disciplinary Procedures.

Please read this document carefully and sign and date it to indicate your acceptance of the terms herein.

1. Equipment

All computers and associated equipment are the property of the School and must be used in accordance with this policy which adheres to the Computer Misuse Act 1990, General Data Protection Regulation and the Data Protection Act 2018 (see Glossary). The School assumes responsibility of maintenance of all hardware and software. Misuse of equipment includes, but is not limited to the following:

- Modification or removal of software
- Unauthorised configuration changes
- Creation or uploading or computer viruses or other malware
- Deliberate deletion of files
- The uploading of computer files to the School's network.

The above actions can reduce the availability and reliability of computer equipment, put data at risk and increase downtime caused by repairs, thus delaying other essential work such as upgrades or enhancements.

Laptop Computers

Laptop computers are issued to all teaching staff and support staff as required. Laptops remain the property of Burnside at all times, and their usage is subject to the following guidelines:

- The equipment remains the property of the School at all times.
- Maintenance of the equipment is the responsibility of the School.
- All installed software MUST be covered by a valid license agreement held by the School or its ICT provider.
- All software installation MUST be carried out by ICT technician in accordance with the relevant license agreements.
- No software should be removed, uninstalled or disabled under any circumstances.
- Any software problems should be reported through the usual support channels.
- Antivirus software must be updated regularly. For laptop computers, it will be necessary to connect them to the School network to update the antivirus software. This should be done at least weekly.

- The user of the equipment is responsible for all personal files and data stored on the equipment.
- Where removable media is used the user must ensure that these mediums have not been used to download materials that are at risk of damaging the network. It is recommended that the school's facility to transfer files is used.
- The user of the equipment must not encrypt any data or password protect any files so as to ensure future usage of the equipment.
- The School cannot be held responsible for loss of personal data in the event of either a hardware or software failure or user error.
- From time to time, it may be necessary for ICT technician to perform software updates and maintenance for which the equipment must be made available in School when reasonably requested.

Use of Removable Storage Media

Memory sticks to transfer files between home and school, should be password protected and encrypted. They should not be used as the sole means of storage for important files.

Printers and Consumables

Printers are provided in the School for educational or work-related use only. All printer usage will be monitored and recorded.

- Always print on a black & white printer unless colour is absolutely essential
- Proofread your document on-screen and use the 'Print-Preview' facility to check the layout before printing.
- Do not print unnecessarily or waste ink or paper.
- Avoid printing directly from the Internet where possible. Internet pages are often not suitably formatted for printing and may cause wastage of paper and other consumables.

Data Security and Retention

All data stored on the School network is backed up daily. If you should accidentally delete a file or files in your folder or shared area, please inform ICT immediately so that it can be recovered.

2. Internet and Email

The School provides Internet filtering, designed to remove controversial, offensive or illegal content. It is impossible to guarantee that all controversial material is filtered. If you discover any websites containing inappropriate or offensive content, please report this to the ICT lead so appropriate action can be taken.

Acceptable use of the Internet

Use of the Internet should be in accordance with the following guidelines:

- Transmission of any material in violation of any United Kingdom or other national law is prohibited. This includes, but is not limited to, copyrighted material,
- threatening or obscene material or material protected by trade laws
- Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- The use of Internet chat sites is prohibited.
- The use of online gaming sites is prohibited.
- Do not print out pages directly from a website.
- Downloading or installing software from the Internet is not permitted.
- Staff are reminded that ALL Internet access is logged and actively monitored.

Email

Where Staff are provided with an email address this may be used for any legitimate educational or work-related activity. Staff should use the email in accordance with the following guidelines and are reminded that the School retains the right to monitor email communications at any time if this is deemed necessary.

- The sending or receiving of messages which contain any inappropriate material is strictly forbidden. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any other use which may be likely to cause offence. Disciplinary action will be taken in all cases.
- Messages relating to, or in support of any illegal activities will be reported to the relevant authority.
- Attachments received on an email should not be opened unless you are certain of both their content and origin. File attachments may contain viruses or other forms of malware that may cause loss of data or damage to the School network.
- Where digital personal data is transferred outside the secure local network, it must be encrypted. An encryption service is an option if you do not have encryption enabled on emails. An encryption service enables you to send documents in a safe and secure manner. These work by sending the recipient an email with a secure link to a repository where the associated document(s) can be downloaded over a safe connection. An encryption service also provides a full audit trail and logging of all emails and their attachments.
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Send the information as an encrypted document attached to an email
- Provide the encryption key or password by a separate contact with the recipient(s)

- When sending emails externally to more than one person, you must hide the recipients' email addresses. You can do this by putting just your own name in the "To" field, and putting the other addresses in the "Bcc" field.

3. Privacy and Data Protection

Passwords

- Never share your password with anyone or ask others for their password.
- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name. It is advisable to use a 'strong' password, which contains a combination of upper and lower-case letters, numbers and other punctuation characters. Current Government guidance is that a phrase should be used that is familiar to you e.g. W1ndinth3w1llows
- If you forget your password, please request that it be reset via your ICT technician
- If you believe that your password has been compromised, change it immediately.

4. Security

- Never attempt to access files or programs for which you have not been granted authorisation. Attempting to bypass security barriers may breach data protection legislation and such attempts will be subject to disciplinary action.
- Never grant or allow access to files or programs to unauthorised users. This is a breach of school policy and data protection legislation and such attempts will be subject to disciplinary action.
- Any security concerns should be reported immediately to ICT.
- Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with the School Disciplinary Procedures.

5. Access to the School network

Access to the School network is available to those staff who require it. Access is subject to agreement and is subject to the following guidelines:

- Password security is vital. If you believe that your password has been compromised, change it immediately.
- If you leave your computer unattended, particularly in a classroom, lock it by using the 'Windows and L key'.
- If you are connecting to an interactive whiteboard and projector, please be aware that any pupil information you display on your screen may also be displayed on the whiteboard if the projector is turned on. To ensure protection of sensitive data, please ensure that projectors are turned off or disconnected before connecting.

- When working from home Staff must ensure that their home Internet connection is secure from outside access particularly if a wireless network is used. Additionally

- staff should take due care regarding who may potentially have access to the PC or any material which may be printed at home.

6. Mobile Phones

Staff should not use their mobile phone or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person. In order to reduce the risk staff should limit their use of mobile technologies to specified breaks during the school day.

REQUIRED DIGITAL SIGNATURE

MEMBER OF STAFF

By logging in to the Burnside network, I understand and agree to the provisions and conditions of this agreement. I understand that any violation of the above provisions may result in disciplinary action being taken against me. I agree to use the School ICT systems in compliance with the terms outlined in this document and understand that my Internet access and any electronic communications may be logged or monitored.