Title	**ICT and internet acceptable use policy**
Purpose	Sets guidelines and rules around acceptable use of ICT and internet for all members of the provision community
Relevant to	Governing roles, all staff, students, parents
Responsible Officer	Academy Development Director, BSET
Introduced	7/2021
Modification History	
Related Policies	Staff Discipline; Safeguarding; Data Protection
Date Due for Review	7/2023
Relevant committee for review	Oakbridge Board
Approved at	30/6/2021
Filed as	BSET_Pol.28_ICT_Acceptable_Use_OB_Vs1_0721

Contents

1. Introduction and aims

ICT is an integral part of the way our provision works, and is a critical resource for students, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the provision.

However, the ICT resources and facilities our provision uses also pose risks to data protection, online safety and safeguarding.

This policy is adopted from a model document published by "The Key" and aims to:

- Set guidelines and rules on the use of ICT resources for staff, students, parents and governors
- Establish clear expectations for the way all members of the Oakbridge community engage with each other online
- Support the provision's policy on data protection, online safety and safeguarding
- Prevent disruption through the misuse, or attempted misuse, of ICT systems
- Support teaching students safe and effective internet and ICT use

This policy covers all users of our ICT facilities, including governors, staff, students, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under relevant behaviour or staff disciplinary policies maintained by Barnet Special Education Trust.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2020
- Searching, screening and confiscation: advice for provisions

3. Definitions

"ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

"Users": anyone authorised by the provision to use the ICT facilities, including governors, staff, students, volunteers, contractors and visitors

"Personal use": any use or activity not directly related to the users' employment, study or purpose

"Authorised personnel": employees authorised by the provision to perform systems administration and/or monitoring of the ICT facilities

"Materials": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the provision's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the provision's ICT facilities includes:

- Using the provision's ICT facilities to breach intellectual property rights or copyright
- Using the provision's ICT facilities to bully or harass someone else, or to promote unlawful discrimination

- Breaching the provision's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the provision, or risks bringing the provision into disrepute
- Unauthorised sharing of confidential information about the provision, its students, or other members of the provision community
- Connecting any device to the provision's ICT network without prior approval from authorised personnel
- Setting up any software, applications or web services on the provision's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the provision's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the provision
- Using websites or mechanisms to bypass the provision's filtering mechanisms

This list is not exhaustive. The provision reserves the right to amend this list at any time. The provision manager or a relevant member of Senior Leadership Team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the provision's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of provision ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may only be granted at the provision manager's discretion.

Any user of provision ICT services who believes they may require exceptional permissions, should consult their line manager, so that the case can be properly considered following relevant technical, safeguarding, data protection or other legal advice.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the provision's Behaviour or Staff Discipline policies.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to provision ICT facilities and materials

The provision's Facilities Manager and wider team manages access to the provision's ICT facilities and materials for provision staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Permanently employed staff will be provided with unique log-in/account information and passwords that they must use when accessing the provision's ICT facilities.

At the provision manager's discretion, accounts may also be provided for temporary members of staff who are agency contractors.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should seek advice from the provision manager.

5.1.1 Use of phones and email

The provision provides each permanent member of staff with an email address.

At the provision manager's discretion, email accounts may also be provided for temporary members of staff who are agency contractors.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address provided.

Staff must not share their personal email addresses with parents and students, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the designated data protection lead (currently BSET Academy Development Director) immediately and follow provision data breach procedure.

Staff must not give their personal phone numbers to parents or students. Staff must use phones provided by the provision to conduct all work-related business.

Provision phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.2 Personal use

Staff are permitted to occasionally use provision ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The provision manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/non-break time
- Does not constitute 'unacceptable use', as defined in section 4
- **Takes place when no students are present**
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes

Staff may not use the provision's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the provision's ICT facilities for personal use may put personal communications within the scope of the provision's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are permitted to use their personal devices (such as mobile phones or tablets) in line with Staff Handbook guidance

Staff should be aware that personal use of ICT (even when not using provision ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where students and parents could see them.

Staff should take care to follow the provision's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal Devices

Staff may only use approved personally owned devices to access the provision network as necessary in the course of their normal work (See 8.5). However, the increasing use of cloud-based services for email and document applications means that more work may be safely undertaken on employees' own personal devices (smartphone, tablet, laptop). This will be permitted as long as the device adheres to a strong password and security policy.

Users are forbidden from copying sensitive data from cloud-based email, calendar and contact applications from their work accounts to other storage applications on a personal device.

Staff using personal devices to access cloud-based IT services in relation to their work will be subject to all standards of acceptable use outlined across this document.

Staff agree to a general code of conduct that recognises the need to protect confidential data that is stored on, or accessed using, a personal mobile device. This includes but is not limited to:

- Doing what is necessary to ensure the adequate physical security of the device
- Maintaining and keeping up-to-date the device's operating systems, software configuration and installed applications to ensure the latest digital security measures are applied.
- Ensuring the device's security controls are not subverted via hacks, jailbreaks, security software changes or security setting changes
- Preventing the storage of sensitive company data on the device.
- Immediately reporting a lost or stolen device.

Support needs or issues related to personal smartphone and tablet devices remain the responsibility of the device owner.

Barnet Special Education Trust and Oak Lodge Provision will accept no responsibility for loss or damage to any personal device.

5.2.2 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The provision has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access the provision's ICT facilities and materials remotely. This is managed as a supplementary service of London Grid for Learning; use of which requires additional software to be installed on a provision computer and a secondary security device.

Remote access facilities will only be granted to provision owned equipment. Staff may request remote access arrangements through the Facilities Manager.

Staff accessing the provision's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the provision's ICT facilities outside the provision and take such precautions as the Facilities Manager may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

A copy of the Data Protection Policy is available at www.oakbridgesen.org.

5.4 Provision social media accounts

The provision does not currently operate any social media accounts. This aspect of policy will be kept under review.

5.5 Monitoring of provision network and use of ICT facilities

The provision reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The provision monitors ICT use in order to:

- Obtain information related to provision business
- Investigate compliance with provision policies, procedures and standards
- Ensure effective provision and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Students

6.1 Access to ICT facilities

- Unless designated for specific personal use (such as a communication aid), computers and other forms of ICT equipment are available to students only under the supervision of staff.
- Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff.

- "Where appropriate and according to their needs and abilities, students will be provided with a limited function account linked to the provision's network, which they can access which they will be able to access under staff supervision.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the provision has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under provision rules or legislation.

6.3 Unacceptable use of ICT and the internet outside of provision

The provision may sanction students, in line with the behaviour policy, if a student engages in any of the following **at any time** (even if they are not on provision premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the provision's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the provision, or risks bringing the provision into disrepute
- Sharing confidential information about the provision, other students, or other members of the provision community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the provision's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

The provision will contact relevant external agencies where it is suspected or believed that an unlawful action has been undertaken, or where wider safeguarding concerns may arise from breaches of our acceptable use policy.

7. Parents

The online world is a continually evolving, innovative and sometimes disruptive environment that can present considerable safeguarding challenges for children and young people.

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online. Parents can play a vital role in helping support appropriate online behaviour for their children.

Where individual student's use of the internet and social media gives cause for concern, provision will consult with parents in order to safeguard student's safety, health and wellbeing.

A recommended, comprehensive and up-to-date store of digital guides for parents, carers and teachers to help them keep children and young people safe on the internet is available at https://parentzone.org.uk/advice/parent-guides.

8. Data security

The provision takes steps to protect the security of its computing resources, data and user accounts. However, the provision cannot guarantee security. Staff, students, parents and others who use the provision's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the provision's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or students who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All of the provision's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the provision's ICT facilities.

Any personal devices using the provision's network must also be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the provision's data protection policy.

A copy of the Data Protection Policy is available at www.oakbridgesen.org.

8.4 Access to facilities and materials

All users of the provision's ICT facilities will have clearly defined access rights to provision systems, files and devices. These access rights are managed by the Facilities Manager.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Facilities Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The provision ensures that its own devices and systems have an appropriate level of encryption.

Provision staff may only use personal devices (including computers and USB drives) to access provision network data, work remotely on the provision network, if the devices have appropriate levels of security and encryption, as defined by the Facilities Manager and they have been specifically authorised to do so by the Provision Manager.

For further policy on use of personal devices refer to section 5.2.1

9. Internet access

The provision wireless internet connection is secured and filtering software monitoring is in force for all provision users.

There is a separate wireless network available for guests or non-provision devices. Parents and visitors to the provision will not generally be permitted to use the provision's Wi-Fi access unless specific authorisation is granted by the provision manager.

The provision manager will only grant authorisation if:

- Parents are working with the provision in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the provision's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Monitoring and review

BSET Academy Development Director and Facilities Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the provision.

This policy will be reviewed every 2 years.

The governing board is responsible for approval of this policy.

Appendix 1: Facebook Guidance for Staff

Don't accept friend requests from students on social media

10 rules for provision staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your students
6. Don't use social media sites during provision hours
7. Don't make comments about your job, your colleagues, our provision or your students online – once it's out there, it's out there
8. Don't associate yourself with the provision on your profile (e.g. by setting it as your workplace, or by 'checking in' at a provision event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or students)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the provision manager about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the provision
    - Students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable Use Standards for Students

When a student uses the provision's ICT facilities (like computers and equipment) and get on the internet in provision, they do not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break provision rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Share a password with others or log in using someone else's name or password
- Bully other people

Students should understand that the provision will check the websites they visit and how they use the provision's computers and equipment. This is so that they can be helped to keep safe.

Students must tell a teacher or other member of staff immediately if they find anything on a provision computer or online that upsets them, or that they know is mean or wrong.

Students will always be responsible when they use the provision's ICT systems and internet.

Students should understand that the provision can intervene if they do certain unacceptable things online, even if they are not in provision when they do them.

Appendix 3: Acceptable Use Standards for Staff, Governors, Volunteers and Visitors

When using the provision's ICT facilities and accessing the internet in provision, or outside provision on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the provision's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the provision's network
- Share my password with others or log in to the provision's network using someone else's details
- Share confidential information about the provision, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the provision

I understand that the provision will monitor the websites I visit and my use of the provision's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside provision, and keep all data securely stored in accordance with this policy and the provision's data protection policy.

I will let the designated safeguarding lead (DSL) and Facilities Manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the provision's ICT systems and internet responsibly, and ensure that students in my care do so too.