‘

Parkhall Integrated College
E-Safety and ICT acceptable use policy

Agreed by Board of Governors: June 2023 **To be reviewed: June 2027**

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our college works, and is a critical resource for students, staff, governors and visitors. It supports teaching and learning, and the pastoral and administrative functions of the college. In using the ICT in a structured and supervised manner, Parkhall Integrated College:

- Encourages students to access ICT where it is beneficial and where such use supports their understanding of the Northern Ireland Curriculum and subject specifications.
- Ensures that students acquire skills that are useful for them not only in college but also in adult life, in continuing education and training and in employment.
- Protects students from undesirable experiences and/or influences while using ICT.

However, the ICT resources and facilities our college uses could also pose risks to data protection, online safety and safeguarding.
This policy aims to:
• Set guidelines and rules on the use of college ICT resources for staff, students, parent/guardians/guardians and governors
• Establish clear expectations for the way all members of the college community engage with each other online
• Support the college's policies on data protection, online safety and safeguarding
• Prevent disruption that could occur to the college through the misuse, or attempted misuse, of ICT systems
• Support the college in teaching students safe and effective internet and ICT use
This policy covers all users of our college's ICT facilities, including governors, staff, students and visitors.
Breaches of this policy may be dealt with under our addressing bullying policy, positive behaviour policy and staff code of conduct.

2. Unacceptable use

The following is considered unacceptable use of the college's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceeding.

Unacceptable use of the college's ICT facilities includes:

- Using the college's ICT facilities to breach intellectual property rights or copyright
- Using the college's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the college's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the college, or risks bringing the college into disrepute
- Sharing confidential information about the college, its students, or other members of the college community
- Connecting any device to the college's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the college's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the college's 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 college's ICT facilities
- Causing intentional damage to the college's ICT facilities
- Removing, deleting or disposing of the college's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the college
- Using websites or mechanisms to bypass the college's filtering or monitoring mechanisms

- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The college reserves the right to amend this list at any time. The Principal will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the college's ICT facilities.

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the college's policies on our addressing bullying policy, positive behaviour policy and staff code of conduct.

3. Staff

3.1 Access to college ICT facilities and materials

The college' IT Technician manages access to the college's ICT facilities and materials for college staff. That includes, but is not limited to:

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the college's ICT facilities. Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Technician.

3.1.1 Use of phones and email

The college provides each member of staff with an email address. This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s). All work-related business should be conducted using the email address the college has provided. Staff must not share their personal email addresses with parent/guardians 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. 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 that contains the personal information of another person, they must inform the Principal immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parent/guardians or students. Staff must use phones provided by the college to conduct all work-related business. College phones must not be used for personal matters.

3.2 Personal use

Staff are permitted to occasionally use college ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The IT Technician may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching 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 college'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 college's ICT facilities for personal use may put personal communications within the scope of the college's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the college's.
Staff should be aware that personal use of ICT (even when not using college ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where students and parent/guardians could see them.
Staff should take care to follow the college's guidelines on use of social media (see appendix 1) use of email (see section 3.1.1) to protect themselves online and avoid compromising their professional integrity.

3.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. The college has guidelines for staff on appropriate security settings for social media accounts (see appendix 1).

3.4 College social media accounts

The college has an official Facebook and Twitter account, managed by the Publicity Coordinator. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account. The college has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they always abide by these guidelines.

3.5 Monitoring and filtering of the college network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the college reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

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

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.
Where appropriate, authorised personnel may raise concerns about monitored activity with the college's designated safeguarding lead (DSL) and ICT manager, as appropriate.
The college monitors ICT use to:

- Obtain information related to college business
- Investigate compliance with college policies, procedures and standards
- Ensure effective college 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

4. Students

4.1 Access to ICT facilities

Computers and equipment in the college's ICT suite 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". "Sixth-form students can use the computers in the Sixth Form study room independently, for educational purposes only.

4.2 Search and deletion

The principal, and any member of staff authorised to do so by the principal, can search students and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or students, **and/or**
- Is identified in the college rules as a banned item for which a search can be carried out **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Principal or a member of the Senior Leadership Team.
- Explain to the student why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the student's co-operation.

The authorised staff member should:

- Inform the Designated Teacher of any searching incidents where they had reasonable grounds to suspect a student was in possession of a banned item.
- Involve the Designated Teacher) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.
When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has, or could be used to:

- Cause harm, **and/or**
- Undermine the safe environment of the college or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Principal or a member of the Senior Leadership Team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

• They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**

• The student and/or the parent/guardian refuses to delete the material themselves

4.3 Unacceptable use of ICT and the internet outside of college

The college will sanction students, in line with the positive behaviour management policy if a student engages in any of the following at any time (even if they are not on college 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 college's policies or procedures
- Any illegal conduct, or making 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
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the college, or risks bringing the college into disrepute
- Sharing confidential information about the college, other students, or other members of the college 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 college's ICT facilities
- Causing intentional damage to the college's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation

- Using inappropriate or offensive language

At Parkhall Integrated College posters covering e–Safety rules will be made available to display in every computer room to remind students of the e–Safety rules at the point of use. In addition, students take part in an e-safety awareness session hosted by external agencies, and safe and responsible use of ICT will be reinforced across the curriculum and subject areas.

5. Parent/guardians

5.1 Access to ICT facilities and materials

Parent/guardians do not have access to the college's ICT facilities as a matter of course.
However, parent/guardians working for, or with, the college in an official capacity may be granted an appropriate level of access, or be permitted to use the college's facilities at the principal's discretion.
Where parent/guardians are granted access in this way, they must abide by this policy as it applies to staff.

5.2 Communicating with or about the college online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.
Parent/guardians play a vital role in helping model this behaviour for their children, especially when communicating with the college through our website and social media channels.

5.3 Communicating with parent/guardians about student activity

The college will ensure that parent/guardians and carers are made aware of any online activity that their children are being asked to carry out.
When we ask students to use websites or engage in online activity, we will communicate the details of this to parent/guardians in the same way that information about homework tasks is shared.
In particular, staff will let parent/guardians know which (if any) person or people from the college students will be interacting with online, including the purpose of the interaction.
Parent/guardians may seek any support and advice from the college to ensure a safe online environment is established for their child.

6. Data security

The college is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.
Staff, students, parent/guardians and others who use the college's ICT facilities should use safe computing practices at all times.

7.1 Passwords

All users of the college'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. Parent/guardians, visitors or volunteers who disclose account or password information may have their access rights revoked.

7.2 Software updates, firewalls and anti-virus software

All of the college's ICT devices that support software updates, security updates and anti-virus products will have these installed and 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 college's ICT facilities.
Any personal devices using the college's network must all be configured in this way.

7.3 Data protection

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

7.4 Access to facilities and materials

All users of the college's ICT facilities will have clearly defined access rights to college systems, files and devices.
These access rights are managed by the IT Technician.
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 IT Technician 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 shut down completely at the end of each working day.

8. Monitoring and review
The principal and IT Technician monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the college.
This policy will be reviewed on an annual basis.
The governing board is responsible for reviewing and approving this policy.

9. Related policies
This policy should be read alongside the college's policies on:

- Addressing bullying policy
- Child protection policy
- Positive Behaviour management policy
- Staff discipline
- Data protection policy

Appendix 1: Social Media cheat sheet for staff

10 rules for college staff on social media

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 you don't, 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 college hours
7. Don't make comments about your job, your colleagues, our college or your students online – once it's out there, it's out there
8. Don't associate yourself with the college on your profile (e.g. by setting it as your workplace, or by 'checking in' at a college 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 parent/guardians or students)

What to do 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 parent/guardians. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the Principal or a member of the Senior Leadership Team about what's happening

A parent/guardian adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to one parent/guardian's friend request or message might set an unwelcome precedent for both you and other teachers at the college
  - Students may then have indirect access through their parent/guardian'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/guardian 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/guardian 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 agreement for students

Acceptable use of the college's ICT facilities and internet: agreement for students and parent/guardians	
Name of student:	
When using the college's ICT facilities and accessing the internet in college, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break college rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video • Share my password with others or log in to the college's network using someone else's details • Bully other people I understand that the college will monitor the websites I visit and my use of the college's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the college's ICT systems and internet responsibly. I understand that the college can discipline me if I do certain unacceptable things online, even if I'm not in college when I do them.	
Signed (student):	**Date:**
Parent/guardian/carer agreement: I agree that my child can use the college's ICT systems and internet when appropriately supervised by a member of college staff. I agree to the conditions set out above for students using the college's ICT systems and internet, and for using personal electronic devices in college, and will make sure my child understands these.	
Signed (parent/guardian):	**Date:**

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the college's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the college's ICT facilities and accessing the internet in college, or outside college 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 college's reputation • Access social networking sites or chat rooms • Display any student data to students on the college whiteboards. • 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 college's network • Share my password with others or log in to the college's network using someone else's details • Share confidential information about the college, 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 college	
I understand that the college will monitor the websites I visit and my use of the college'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 college, and keep all data securely stored in accordance with this policy and the college's data protection policy. I will let the Designated Teacher and ICT Technician 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 college's ICT systems and internet responsibly, and ensure that students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**