Parkhall Integrated College

Acceptable use of the Internet and Digital Technologies
Code of Practice

To go to BOG 17th September 2019 **To be reviewed: Date September 2022**

Rationale
Since all pupils seek to use ICT to enhance their learning across the curriculum, they all interact with material on the Internet. Teachers should guide pupils to appropriate websites where their use of such websites contributes to their learning and improves the quality of their learning experience. In order to guard our pupils from any inherent dangers, it is the responsibility of school staff to take appropriate steps to protect them from the dangers of open access to material found on the Internet while encouraging its use where its benefits are clear.

Purposes
In using the Internet in a structured and supervised way Parkhall Integrated College:

- encourages pupils to access the Internet where it is beneficial and where such use supports their understanding of the Northern Ireland Curriculum and subject specifications
- ensures that pupils acquire skills that are useful for them not only in school but also in adult life, in continuing education and training and in employment.
- protects pupils from undesirable experiences and/or influences while using the Internet.
- encourages pupils to work with due consideration of other users when using computer equipment.
- trains pupils in good practice when using the Internet and the computer network.

Guidelines
Code of safe practice for safe and effective use.

Pupil code of practice:

- I will only access the system with my own login and password, which I will keep secret.
- I will not access other people's files.
- I will only use the computers for school work and homework.
- I will not misuse or damage any computer hardware.
- I will not put any disk into the computer unless I have been given permission.
- I will ask permission from a member of staff before printing.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and responsible.
- I will not give my home address or telephone number, or arrange to meet anyone.
- I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

Staff code of practice:

- All ICT activity should be appropriate to staff professional activity or the student's education.
- Staff should be aware of the Departments policy and strategy on ICT use in Teaching and Learning via www.empoweringschools.com
- Access should only be made via the authorised account and password, which should NOT be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- All on line activity both in school and outside school should not bring your professional role into disrepute.

- Staff should be actively discouraged from communicating with pupils using social network sites or other technologies outside of school.

- It is forbidden to browse, download, upload or distribute any material that could be considered offensive, illegal or discriminating.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Users are responsible for all e-mails sent from their account and for contacts made that may result in e-mails being received.
- If sending students an e-mail, only use C2K accounts.
- As e-mails can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Staff should keep all school related data secure both in school and out of school. This includes all personal, sensitive, confidential or classified data; staff should not copy lists of pupils' confidential details from SIMS to any portable storage device e.g. USB, portable hard drives etc.
- Staff have a weekly allowance for printing. If bulk colour printing is required, authorisation must be sought from the Principal.
- Any movement or addition of hardware or software that is required must first be agreed with either the ICT Coordinator or the technician.
- Health and Safety requires pupils to have supervision at ALL times, remain seated, and refrain from eating or drinking when in the computer rooms. It is the responsibility of the teacher concerned to ensure these requirements are met. The ICT coordinator and ICT technician will carry out spot checks of any bookable ICT rooms/resources.
- A timetabling system is in operation for computer room access, it is important this system is followed by all staff (Maximum booking time is 4 weeks)
- Teachers should check pupils' work before allowing printing
- ONE pupil per machine at all times
- DO NOT arrange for substitute teachers to take your class to the computer room (unless scheduled for ICT etc.)
- Internet and Intranet use must be properly supervised
- PLEASE ENSURE COMPUTER ROOMS ARE LEFT CLEAN AND TIDY
- Report any damage/ graffiti etc. to the technician or ICT coordinator ASAP.

Legal monitoring of email and internet use:
Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents can be created, for example.

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during school hours or for professional purpose.

Education in Safe and Effective Practices.

Internet Safety Education for Pupils:
At Parkhall Integrated College posters covering e–Safety rules will be made available to display in every computer room to remind pupils of the e–Safety rules at the point of use.

- All users will be informed that network and Internet use will be monitored.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- Pupils in Years 8 and 11 will take part in an e-safety awareness session hosted by Antrim PSNI.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

Internet Safety Awareness for School Staff:
ICT use is widespread and all staff including administration staff and Induction of new staff will be made aware of the ICT policy.

- The e–Safety Policy will be formally provided to all members of staff.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Internet Awareness for Parents and Carers:
Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home.

- Parents will be encouraged to read and sign the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Interested parents will be referred to organisations dedicated to e-safety.
- See Appendix 1 for full acceptable use policy.

Health and Safety.
Mobile Phones – Health and Safety
Parkhall Integrated College does not permit pupils to use mobile phones and other personal devices such as Games Consoles, Tablets, PDAs and MP3 Players etc. during school hours.
Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.
Mobile phones can present a number of problems when not used appropriately.

- They are valuable items which may be stolen or damaged;
- Their use can render pupils or staff subject to cyber bullying;
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode;
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to pupils at the end of the school day.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff Use of Personal Devices

- Mobile Phone and devices should be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it should only take place when approved by the Senior Management Team.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Responsibility for Personal Technology Devices

- Staff must carefully consider the risk of damage to or theft of personal technology devices like mobile phones, cameras, iPods, MP3 players, or laptops/tablets. Responsibility for the safety of personal technology devices rests solely with the member of staff.
- NO LIABILITY WILL BE ACCEPTED BY THE SCHOOL IN THE EVENT OF THE LOSS, THEFT OR DAMAGE OF ANY PERSONAL TECHNOLOGY DEVICE BROUGHT TO SCHOOL.
- Access to the internet is via the C2K wireless connection. Connection of school bought devices is permitted (e.g. iPads). Connection of personal devices is not permitted.

Wireless Networks

Wi-Fi users can access and share data, applications, internet access or other network resources in the same way as with wired systems.

People using Wi-Fi, or those in the proximity of Wi-Fi equipment, are exposed to the radio signals it emits and some of the transmitted energy in the signals is absorbed in their bodies. The information below sets out the Public Health England (PHE) position regarding such exposure.

- There is no consistent evidence to date that exposure to radio signals from Wi-Fi and WLANs adversely affects the health of the general population. The signals are very low power, typically 0.1 watt (100 milliwatts) in both the computer and the router (access point), and the results so far show exposures are well within the internationally-accepted guidelines from the International Commission on Non-Ionizing Radiation Protection (ICNIRP).
- Based on current knowledge and experience, radio frequency (RF) exposures from Wi-Fi are likely to be lower than those from mobile phones. Also, the frequencies used in Wi-Fi are broadly the same as those from other RF applications such as FM radio, TV and mobile phones.
- On the basis of the published studies and those carried out in-house, PHE sees no reason why Wi-Fi should not continue to be used in schools and in other places. However with any new technology a sensible precautionary approach, as happened with mobile phones, is to keep the situation under review so that parents and others can have as much reassurance as possible.
- The signals from Wi-Fi are very low power, typically 0.1 watt (100 milliwatts), in both the computer and the mast (or router) and resulting exposures should be well within internationally-accepted guidelines.
- The frequencies used are broadly the same as those from other RF applications.
- Based on current knowledge, RF exposures from Wi-Fi are likely to be lower than those from mobile phones.
- On the basis of current scientific information, exposures from Wi-Fi equipment satisfy international guidelines. There is no consistent evidence of health effects from RF exposures below guideline levels and no reason why schools and others should not use Wi-Fi equipment

Digital Publishing and Software Licensing

Digital and video images of pupils on the school website

Parental permission will be obtained before publishing any photographs, video footage etc. of pupils on the school website, in a DVD or in any other high profile public printed media. This ensures that parents are aware of the way the image of their child is representing the school.

- Uploading of information is restricted to the school publicity coordinator and Senior Leadership Team;
- The school website complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;

- The point of contact on the website is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the website do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of pupils should be stored on a secure storage medium and is the responsibility of the creator in the management of such images;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- The school's Acceptable Use Policy for staff includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are only able to publish to their own 'safe' web-portal on the school VLE;

Making and storing digital and video images
Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included, nevertheless, the security of staff and pupils at Parkhall Integrated College is paramount.

Images of a pupil will not be published without the parent's or carer's written permission. Parkhall Integrated College will ask permission to publish images of work or appropriate personal photographs on entry to the school.

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.

Obscene publication provision.
The Data Protection Act is unlikely to apply in most cases where photographs or videos are taken in schools and other educational institutions.
If photos are taken for personal use they are not covered by the Act.
Photos taken for official school use may be covered by the Act, so pupils and students should be advised why they are being taken.
Examples
Personal use:

- A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.

- Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.

Official use:

- Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.

- A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used.

Media use:

- A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.

Copyright and Intellectual Property Rights
Copyright gives the creators of materials control over how they are used. Copyright protection comes into force as soon as something – which includes software and music, clip-art and images found on the Internet, as well as images and text - is created or fixed in some way, including electronically.

Intellectual property rights are a series of legal rights that give protection for different types of invention, design, brand name or original creation.
At Parkhall Integrated College it is the responsibility of the subject Teacher to:

- Ensure that there is no breach of copyright or theft of the intellectual work of others, however published, including digital music, clip-art images and software in digital teaching resources and/or pupil coursework / homework.

At Parkhall College it is the responsibility of the ICT Technician to:

- Ensure that any software used in school is properly licensed for the level of use intended.

Creative Commons License
Creative Commons is a nonprofit organisation that enables the sharing and use of creativity and knowledge through free legal tools. If an image, video, piece of text or music has a Creative Commons License attached to it then the owner has given permission for it to be used. In a nutshell, if staff and pupils at Parkhall Integrated College intend to download a piece of text or an image for manipulation then it should have a creative commons license attached to it. When searching for such text the words “creative Commons” should be attached to the end of the search in the search engine.

Social Software
Social software is a generic term for community networks, chat rooms, instant messenger systems, online journals, social networks and blogs (personal web journals).

Social environments enable any community to share resources and ideas amongst users. There are many excellent public examples of social software being used to support formal and informal educational practice amongst young people and amongst educators. They are also popular ways of enabling users to publish and share information, including photographs, streams of video from webcams, video files and blogs about themselves and their interests. Examples include Flickr, Facebook and Twitter.

The C2k school network filters out services which are misused and block attempts to circumvent the filters. The school will control access to social media and social networking sites.

- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Members of staff are prohibited from running social network spaces for pupil use on a personal basis.Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students’ use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students’ underage use of sites.
- Staff are advised that personal use of social networking, social media and personal publishing sites should be conducted in a professional manner. All social networking sites should be kept private.
- Staff should be aware that pupils may see what they publish on social networking sites.

Computer misuse in school
Parkhall Integrated College promotes responsible online behaviour for learners and staff.
Possible misuse of computers within school setting might include:

- Finding or guessing someone’s password, then using it to gain access to data or services, or posing as other
- Deliberately changing or deleting files belonging to others
- Changing computer settings
- Deliberately introducing viruses onto the network.

Although some might not see ‘victimless’ hacking, or playing around with computer settings as particularly serious, the reality is that such activities can seriously affect the operation of the network, inconveniencing

other users and creating additional work for staff. Parkhall Integrated College staff will monitor computer misuse in school and pass any concerns to the e-safety Coordinator.

Sanctions for misuse
Depending on the seriousness of incidents, sanctions might include verbal warnings, temporary bans, and involvement of parents and carers or, in extreme cases, permanent exclusion from the ICT classroom.
If illegal activity is suspected, the police will be involved at the earliest opportunity.

Managing and reporting incidents and securing evidence of misuse
Any incidents which occur should be noted and passed on to the e-safety coordinator. Incidents can be broken down into the following main categories:
Minor incidents
Minor incidents of misuse by pupils might include:

- copying information into assignments and failing to acknowledge the source (plagiarism and copyright infringement)
- downloading materials or images not relevant to their studies, in direct breach of the school's acceptable use policy
- misconduct associated with student logins, such as using someone else's password

In a minor case the pupil will be issued with a warning, and the incident documented. If the behaviour is repeated, or the misconduct escalates, it will then be responded to more seriously if the school has evidence of previous events.
The e-safety coordinator will monitor minor incidents to identify trends in pupils' behaviour, and will react proactively to any emerging issues. This could include raising awareness on a particular e-safety topic at a school assembly or offering staff additional training.

Incidents involving inappropriate materials or activities
While not illegal, there will be some material that is just not appropriate within the school environment, and, in the case of staff, not in keeping with the professional standards or code of ethics of those who work with children and young people. Examples might include soft-core pornography, hate material, drug or bomb-making recipes, or material that others may find offensive such as sexist or racist jokes, cartoons, or material which is used in low-level harassment.
Specific breaches of policy and rules include deliberately accessing, printing, showing or transmitting inappropriate (or age-restricted) material within the school's network, even if such material was not deliberately accessed by the pupil.

Serious incidents
More serious incidents relating to e-safety in school should be reported to the e-safety coordinator immediately. The e-safety coordinator will document the incident and decide on an appropriate course of action, which may include involving the Principal and external agencies. Child protection staff may be involved to provide follow-up counseling and support to both the victims and perpetrators. The e-safety coordinator will review e-safety policies as soon as possible after the incident in an attempt to prevent such an incident recurring, debriefing relevant staff accordingly, and providing school-wide training as appropriate.

What to do in the event of discovery of indecent material
Discovery of indecent material within the school's network is a very serious situation, and will reported to the police. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. Any such incident should be reported to the e-safety coordinator and if at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off. It may be necessary to shut down the whole network, but this will not be done unless instructed by the police.

e-safety review
In the event of a very serious incident occurring within school, a review of all e-safety policies and procedures will be conducted.

Reporting illegal content
A report will be made to the Internet Watch Foundation with anything that Parkhall Integrated College deem to be potentially illegal:

- Images of child abuse hosted anywhere in the world. As a guide, the word 'indecent' means any images of children, less than 18 years of age, involved in a sexual pose or activity. The term child abuse images reflect the gravity of the images but they are also commonly referred to as child pornography, child porn, child porno and kiddie porn.
- Criminally obscene content hosted in the UK. As a guide it could include images featuring acts of extreme sexual activity such as bestiality, necrophilia, rape or torture.
- Incitement to racial hatred content hosted in the UK. The law on incitement to racial hatred content makes it an offence to stir up racial hatred against a group of persons in Great Britain, defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins.

These policy Guidelines are translated into action through other policies and procedures, for example:

ICT Policy Child Protection Policy Anti-bullying Policy Pastoral Care Policy

Sanctions Booklet

Appendix 1

Parkhall Integrated College
Internet and Virtual Learning Environment (VLE)
Acceptable Use Policy

1 Pupils must obtain the permission of parent(s)/guardian(s) before they can be allowed to use the Internet or VLE. The Parental and Pupil Permission Form must be signed and returned to the school.

2 Pupils should only use the school computer systems for those activities and services (Internet and VLE) which they have been given permission to use.

3 Pupils must only use the school computers with the permission and under the supervision of a member of staff.

4 Activities which use the Internet during taught lessons will be directly related to school work. Use of the Internet outside of taught lessons is limited to extension of work therefore permission must be granted by a member of staff and supervised.

5 Pupils must only use the user name and password of the C2K system that they have been given.

6 Pupils should not download and use material or copy and paste content which is copyright. Most sites will allow the use of published materials for educational use. Teachers will give guidelines on how and when pupils should use information from the Internet.

7 The Internet access provided in Parkhall Integrated College is filtered to stop access to unsuitable material. As no filtering system can be 100% effective, it is important that parents are aware that users of the system are required to act responsibly. Under no circumstances should pupils attempt to view, upload or download any material that is likely to be unsuitable for children or schools. Pupils have a responsibility to inform the member of staff supervising them if they have accidentally accessed inappropriate content.

8 Pupils will be taught to respect the privacy of files of other users. They will be advised not to enter, or attempt to enter without permission, the file areas of other pupils or staff.

9 Parents are asked to explain the importance to their child of these rules for the safe use of the Internet and to sign and return to the school the Parental Permission Form.

10 The VLE service for pupils is provided for educational use. The service is only to be used in accordance with the school's policy and procedure. Pupils will use an individual username and password. It is important that they understand that all messages and material sent using this system is automatically screened for inappropriate language.

Failure to comply with these rules will result in one or more of the following:

- A ban, temporary or permanent, will be imposed on the use of the Internet and or VLE at school.

- Access for VLE will be withdrawn at home

- A letter will be sent informing parents of the nature and breach of rules.

If you do not understand any part of this “Acceptable Use Policy”, parents should ask a member of the ICT department for guidance. You should only sign the Parental Permission Form when you and your child have read, understood and agree to the rules of the policy.

Parental Permission for Pupil use of Internet and VLE Facilities At Parkhall Integrated College

The school has a connection to the Internet. The Internet provides a number of important and valuable contributions that can enhance learning and understanding in all of the school curriculum areas. Thousands of schools across the world now have access to the Internet, and many pupils and students are reaping the educational benefits this learning resource provides.

As a result of the open and unregulated nature of the Internet, there is some material that is unsuitable for viewing by children. Therefore, we have introduced procedures that should enable your son/daughter to use the Internet facilities safely and securely. A copy of the school's Acceptable Use Policy is attached to this letter. We will make every effort to ensure that unsuitable material is not viewed by your son/daughter. A member of staff will monitor each session. Each member of staff and parents of each pupil using the Internet must agree to the Acceptable Use Policy. This policy sets out the rules that must be adhered to for the protection of all users.

For your information the following website provides further information on "Safety on the Internet":

http://www.iwf.org.uk/ The Internet Watch Foundation website.

The form below must be completed, signed and returned to your child's ICT teacher for our records. Use of the Internet, VLE and email service will be withheld until this form is returned.

----------(please cut along dotted line)

I have read, understood and explained the Acceptable Use Policy to my child:

Pupil Name (PLEASE PRINT) _____of class _____

Name of Parent/Guardian (PLEASE PRINT) _____

Signature of Parent/Guardian _____

I have read and agree to comply with the Internet and VLE rules.

Signature of Pupil _____