Omagh Academy

Online Safety Policy

Online Safety Policy

Target Audience	Parents/Guardians, School Stakeholders, staff
Review lead	Vice Principal
Personnel involved in the Review	C2k Manager, Head of ICT and eLearning, Teacher in Charge of PR and CR
Approved by:	Board of Governors
Approval date:	January 2026
Effective from:	January 2026
Review frequency	Every 3 years
Review date:	January 2029
Principal	Mrs R Maxwell
Chair of Governors	Mr Wm Reilly

Signed: _____ (Chair of Governors)

Date: _____

Record of amendments

Amendment	Date

CONTENTS **PAGE**

Online Safety Policy

Online safety is concerned with the safeguarding of a person while using electronic communication devices.

Aims

The aims of this policy are to:

- promote the use of new technologies in a safe and positive way.
- safeguard our young people in the digital world.
- create a framework for online safety curriculum development and review.
- provide a foundation for the monitoring and evaluating of online safety provision; and
- help facilitate self-evaluation and improvement.

Context of this Policy

This online safety policy takes account of and is set in the context of:

- School aims and policies
- DENI Circulars 2017/04, 2016/27, 2016/26, 2015/21, 2013/25, 2011/22 & 2007/1
- The Safeguarding Board for Northern Ireland (SBNI) Report January 2014
- CCEA Requirements for using ICT
- The Data Protection Act (1998) and UK GDPR, Computer Misuse Act (1990) and Freedom of Information Act (2000)
- Keeping children and young people safe: an Online Safety Strategy for Northern Ireland 2020-2025 NI Executive
- Growing Up Online Children's online activities, harm and safety in Northern Ireland - an Evidence Report Stranmillis College September 2023

Related School Policies

- Behaviour Management & Discipline Policy
- Safeguarding/Child Protection Policy
- ICT Acceptable Use Policy for pupils
- Policy on Pupil use of Mobile Digital Devices
- Anti-Bullying Policy
- ICT Acceptable Use Policy for staff
- Bring Your Own Device Policy for pupils

1.0 Management responsibilities in School

- The Board of Governors are responsible for the approval of the online safety policy. A log of all incidents is kept and the Designated Governor with responsibility for Child Protection will, as part of that role, keep an overview of any breaches of online safety procedures. The Principal has a duty of care for ensuring the safety, including online safety, of all members of the school community.
- The Head of ICT and e-learning takes day-to-day responsibility for online safety within the school. They are responsible for the online safety policy and its implementation including the training and updating of staff on online safety matters. They also monitor the use of ICT

in the school and will advise and assist in any investigation into a breach of procedures and/or protocols.

- The C2K Manager(s) ensure that the online safety technical structure is in place and will be responsible for reporting breaches to C2K. They may also be asked to assist in an investigation into a breach of online safety protocols. All breaches of online safety are reported by C2k to the Principal.
- Teachers are the first line of defence in online safety matters. They must model good practice and report all concerns about online safety to the Head of ICT and e-learning. Teachers also have a duty of care to report all child protection concerns to the Designated Teacher.
- All staff must comply with the school's 'Staff Acceptable use of ICT Policy'. As responsible adults they must report all suspicions of unacceptable behaviour to the appropriate member of staff.
- Safeguarding and promoting pupils' welfare around digital technology is the responsibility of all staff, teaching and non-teaching, in school and on school-based activities.
- Pupils must comply with all relevant the school policies including the "Acceptable use of ICT by pupils" and the "Policy on pupil use of mobile digital devices".

2.0 The Management of Risk

2.1 The C2k Service

C2k is responsible for the provision of an information and communications technology (ICT) managed service to the school. It aims to provide a service which enables the educational use of resources in a safe and secure environment which protects users and systems from abuse.

- Staff and pupils accessing the Internet via the C2k Education Network are required to authenticate using their C2k username and password. This authentication provides Internet filtering via the C2k Education Network solution.
- The school's access to the internet is filtered by C2k. At present there are no plans to move beyond these safeguards. All internet usage in school should be within the parameters set by C2k.
- Granular Controls: All users' access to the internet and the C2k system is allocated by the C2k Managers.
- To maintain the integrity of the network and to ensure that users are using the system responsibly, the c2k Network Managers may review files and communications. While normal privacy is respected and protected by password controls users may not expect files and messages stored on publicly funded networks to be private. All users are advised that the C2k system is monitored and that reports can be accessed by school principal.
- Staff and pupils should use their C2k email system for school business. Staff are strongly advised that they should not use home email accounts for school business, including on-line communications with pupils. Staff who use non C2K emails for school business do so at their own risk.
- The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

- Cloud Storage: Data and information are stored in the Cloud. This enables data to be accessed from any location. Over the next few years in preparation for the move to the Strule Shared Educational campus, staff and pupils will make more use of Office 365 with the aim of removing the need to carry less secure portable devices, such as data pens.
- Meru Wireless & Personal Devices: Pupils and staff using their own device within the school building are always subject to the relevant AUP.
- Access to the Internet via the C2k Education Network is fully auditable. All breaches of the system will be subject to the school's disciplinary procedures.

2.2 Management information systems: e.g. SIMS, ALIS, GL Assessments

- Authorisation will be sought from the Principal for all data which is to be transferred to third parties for further processing e.g. to GL Assessment for the organisation and analysis of CAT data.
- A 'Register of Access' outlines the level of access members of staff have to pupil and staff personal data.
- A 'Risk Register' is used to highlight circumstances where data security might be potentially breached.

2.3 Safe location and supervision of computers in schools

Internet access for pupils is available on computers located in classrooms, the library, the sixth form study and in computer suites and clusters in departments throughout the school.

Computer screens are positioned so that they are visible to other people circulating in the area and while using the Internet at school, pupils are supervised where possible. However, when appropriate, pupils and especially senior pupils may use systems independent of staff supervision. In all cases, pupils have a responsibility to behave in line with the school's policies and codes of practice.

2.4 Education in safe and effective practices

The internet and digital technologies are powerful educational resources when they are used effectively. As a school we seek to empower members of our school community so that they understand the technology and derive maximum benefit from it. We want pupils to have the opportunity to avail of all the positive benefits that come from learning, exploring and connecting with each other, while being aware how to protect themselves online. To facilitate the protection of our pupils, we seek to educate the school community about online safety matters.

2.4 Online safety education for Pupils

Pupils are encouraged to embrace technological advances and appreciate their educational benefits. However, the school also regards the safeguarding of our pupils as being of paramount importance and has in place a progressive and cross-curricular online safety curriculum. Raising awareness of the potential risks when engaging with online technologies is also addressed during assemblies and Personal Development classes and by participation in awareness raising events such as the annual 'Safer Internet Day'.

The school is proactive in educating our pupils on the risks associated with online activities and how to recognise and address such risks. We endeavour educate our pupils about and safeguard them against the following risks:

I. **Content Risks** - where the child or young person could be exposed to harmful materials.
II. **Contact Risks** - where the child or young person could participate in adult-initiated online activity or put themselves at risk of grooming.
III. **Conduct Risks** - where the child or young person may be a perpetrator of bullying behaviour in peer to-peer exchange or is at risk of bullying, entrapment or blackmail.
IV. **Commercial Risks** - where the child or young person is exposed to inappropriate commercial advertising, marketing schemes or fraud.

2.5 Online safety awareness for school staff

The Head of ICT and e-learning will keep staff informed of online safety matters and will provide training in the delivery of online safety. They will also work alongside other Heads of Department, the Personal Development co-ordinator and pastoral staff to design and resource a cohesive and progressive age-appropriate online safety curriculum.

2.6 Online safety awareness for parents and carers

By promoting Internet safety at home, parents can reinforce the messages taught in school and help to equip their children with the skills needed to use technology safely. The Acceptable Use of ICT Policy for pupils is provided to all incoming Year 8 pupils and to pupils who join other Year Groups. The school will regularly update parents with information relating to online safety. This information will be disseminated in a variety of ways e.g. via the school website and the School Gateway App. Parents are encouraged to download the Safer Schools App.

Parents and carers are advised to:

- discuss and agree with their children, rules for using the Internet such as when, how long, and what comprises appropriate use.
- get to know the sites their children visit and talk to them about what they are learning. Become aware of their children's online behaviour/digital footprint.
- ensure that they stipulate that they must give their agreement before their children share personal identifying information in any electronic communication on the Internet. Personal information includes images, addresses, phone numbers, the school's name, and financial information such as credit card or bank details. In this way parents can protect their children (and themselves) from unwanted or unacceptable overtures from strangers and from unplanned expenditure or fraud.
- encourage their children not to respond to any unwelcome, unpleasant or abusive messages, and to ensure that their children know that they should tell them if they receive any such messages or images.

2.7 Codes of practice for safe and effective use

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. Our "Acceptable use policies" (AUPs) make explicit to all users what is safe and acceptable and what is not. The policies relate to fixed and mobile devices, school PCs, laptops, and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but

brought onto school premises is subject to the same requirements as that of technology provided by the school.

Users must ensure that the use of Generative AI tools does not breach academic integrity or plagiarism rules. Personal data must never be entered into public AI prompts.

The Head of ICT and e-learning, in collaboration with the Principal/Senior Leadership Team will monitor and review the effectiveness of the AUPs, particularly in the light of new developments in technology.

(Appendix 2 – Staff AUP, Appendix 3 – Pupil AUP, Appendix Pupil Policy on the Use of Mobile Digital Devices)

3.0 Ethical and Acceptable Use of Artificial Intelligence (AI)

3.1 Principles of Use

The school recognises that Generative AI (e.g. Chat GPT, Gemini and Copilot) is a powerful tool for learning. However, its use must be characterised by Academic Integrity and Critical Thinking.

- Aide not author: AI should not be used as a 'personal tutor' to help explain concepts, brainstorm structures or check grammar. It must not be used to write final essays or complete assessments unless explicitly directed by a teacher.
- Verification: Pupils must treat all AI generated information as 'unverified'. Given the risk of 'hallucinations' (plausible sounding but false information), all facts and citations must be cross referenced with reliable sources.

3.2 Academic Integrity and Malpractice (in line with JCQ and CCEA regulations)

- Originality: All work submitted for marking or as part of a formal qualification must be the pupil's own. Submitting AI generated content as original work is considered malpractice and may lead to disqualification.
- Declaration: Where AI tools have been used to assist in the research or planning phase of a task, this must be clearly declared (e.g. *AI was used to generate a structure for this essay: all final content is my own*).

3.3 Data Privacy and Age Restrictions

- Personal data: Pupils must never input personal information (names, addresses or school details) or the personal data of others into AI prompts, as this data may be used to train public models.
- Age compliance: Pupils must respect the age limits of AI tools (typically 13+ or 18+). The use of these tools within the school network is subject to C2K filtering and supervision.

3.4 Prohibited AI Content

The use of AI to generate the following is a 'Category 1' breach of this policy:

- Deepfakes: Creating or sharing manipulated images or audio of staff or pupils.
- Harmful Content: Using AI to generate hate speech, extremist material, or bypass school security filters.

4.0 Managing and reporting incidents

4.1 Investigating breaches of online safety guidelines

All incidents of malpractice should be reported in the first instance to the C2k Manager or in the case of a member of staff to the Principal or Designated Teacher for Child Protection.

- Breaches of the school's online safety guidelines must be reported without delay to the C2k Manager or a member of the Senior Leadership Team (SLT).
- Where a member of staff is raising a concern, the initial oral report should be followed up by a written account of the incident within 24 hours and forwarded to the C2k Manager (See Appendix 6). If a pupil is raising the concern, then he/she will be asked for a similar account or will be interviewed by the pupil's Year Head or a member of the SLT to clarify the situation and facilitate completion of the report. Regardless of who is the recipient of the information the report must be passed to the C2k Manager for filing.
- If a computer or other electronic device is identified as suspect e.g. containing for instance indecent images or offences in relation to child protection, it should not be used nor the material viewed. The C2k Manager, the Designated Teacher and the Principal should be informed. Guidance will then be sought from the Education Authority and if appropriate the PSNI informed.
- The C2k manager will liaise with C2k as required and will oversee the security of the hardware and its eventual return to use.
- Investigations with pupils will be carried out by Pastoral staff acting in their usual roles but details of all breaches of online safety must be reported to the C2k Manager as soon after the incident has been raised.
- Disciplinary action taken will be in accordance with our policies and established practices. Sanctions may include the loss of access to ICT facilities e.g. a temporary or permanent ban on Internet use.
- The log of online safety breaches will be updated by the C2k Manager, who will also inform the principal of the breach and how it was managed.
- The C2k Manager will conduct a review of the school's e-safety policy and procedures following any major or serious incident.
- If appropriate the 'Risk register' will be updated to record possible online safety issues.

4.2 Examples of breaches of online safety guidelines

- Examples of incidents which should be reported to the C2k Manager include plagiarism or copyright infringement, downloading materials or images not relevant to the subject, using someone else's password or sending nuisance text messages.

- Artificial Intelligence Misuse (e.g. generating deepfake imagery of staff or pupils or using AI for mass plagiarism).
- Live streaming/Recording: unauthorised recording or live streaming of lessons or individuals on school premises.
- Further examples include the accessing of soft-core pornography, hate material, drug or bomb-making recipes, or material that others may find offensive such as sexist or racist jokes and cartoons or material which is libellous or intended to harass.
- Where the incident involves child abuse, the Designated Teacher for Child Protection must be notified. In cases relating to child protection or where a child is at risk the school's child protection procedures will be implemented as set out in the Safeguarding/Child Protection Policy.
- The harassment of another person using technology or breaching their right to privacy (e.g. reading their mail, accessing their files, using their computer account or electronic mail address), may have legal consequences.
- Instances of cyberbullying will be dealt with in line with the Anti Bullying Policy.

5.0 The School's Website and Social Media Profiles:

The school's website and social media profiles (Facebook & Instagram) are used to celebrate pupils' work, promote the school and provide information. The website is maintained by an external company who liaises with the teacher who has responsibility for the site (Teacher in charge of PR and Community Relations). The teacher responsible ensures that the website reflects the school's ethos, that information is accurate and well-presented, and that personal security is not compromised. As the school's website can be accessed by anyone on the Internet, the school is very careful to safeguard the personal data of our pupils and staff. The school's social media profile and its associated published statuses are monitored and regularly updated, ensuring all published material is in keeping with school protocols.

6.0 The Use of Social Media Platforms

Social media is a valuable vehicle for liaison with parents and the local community. A number of departments and extra-curricular activities use social media platforms such as Facebook to showcase their activities to good effect. The existence of all such pages must be made known to the Teacher in charge of PR and Community Relations. It is the responsibility of the account operator to ensure that the content reflects the school's ethos, is accurate and that personal security is not compromised.

The school endeavours to educate pupils about the positive and responsible use of social media websites. However, pupils and parents are advised that where a child is potentially at risk the matter should be reported immediately to the PSNI. Online abuse and harassment should also be reported to the software operator and to the pupil's Head of Year and C2k Manager. In addition, the school retains the right to discipline pupils for incidents of cyberbullying, whenever or wherever they occur.

7.0 Communication of the Policy

Parents, pupils, governors and staff (teaching and non-teaching) were consulted on its contents. The policy will be available on the school's website and in hard copy by request from the school office.

Appendix 1: Staff Acceptable Use Policy

Omagh Academy Staff ICT Acceptable Use Policy (AUP)

The Board of Governors encourage and support the positive use of Information and Communication Technology (ICT) to develop curriculum and learning opportunities. However, to maintain our pupil's safety it is important that all staff in Omagh Academy take all necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using ICT and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list, and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include fixed and mobile internet, networks, data and data storage, online and offline communication technologies and access devices. Examples include PCs, laptops, mobile phones, PDAs, digital cameras, webcams, video equipment, email and social media sites**.**

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by Omagh Academy for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my workstation as appropriate.

- I will not deliberately cause damage to computers, digital equipment or computer networks belonging to Omagh Academy or on lease from C2k.

- I will not intentionally waste resources such as online time or consumables – paper, toner etc.

- This AUP also covers the use of technologies owned by staff and brought onto school premises, for example, mobile phones, camera phones, PDAs and portable media players. I understand that the use of devices owned personally by staff is subject to the same requirements as technology provided by the school. I will use personally owned devices in accordance with the policy.

- I will respect system security, and I will not disclose my C2k or SIMS passwords or other security information.

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the C2k manager.

- I will ensure that any personal data relating to pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, online or accessed remotely. Any personal data which is being removed from the school site (such as via email or on memory sticks or CDs) will be stored securely.

- Any images or videos of pupils will only be used to promote the school on the school website or in newsletters and newspapers when written parental consent has been obtained.

- I will not keep professional documents which contain school-related sensitive or personal Information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the school system to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information. I will not use the school system for any unapproved commercial purpose.

- I will respect copyright and intellectual property rights.

- I have read and understood the school Online Safety Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I will report all incidents of concern regarding children's online safety to the Designated Teacher for Child Protection or the Deputy Designated Teachers as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the C2k Manager and designated staff for filtering as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the C2k Manager, or to the ICT technician as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. I will not give out my own personal details, such as mobile phone number and personal e-mail address to pupils. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership Team.

- I will exercise caution when using social media sites such as Facebook and X. I will ensure that care is taken not to compromise my professional status when adding friends who may be pupils or parents. Members of staff are advised to check their privacy settings on any personal social media sites they use. Please remember that once content is shared online it is possible for it be circulated more widely than intended without consent or knowledge, even if the content is thought to have been deleted or privately shared. I am aware that

pupils may have access to my personal website and/or personal area in a social software environment.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- Occasional personal use of the school's computers can be beneficial to the development of staff IT skills and to enable staff to maintain a positive work-life balance. However, permission for this is at the school's discretion and can be revoked at any time. Any online behaviour and activity by a member of staff whilst using the school systems must be in accordance of the school AUP and personal use must not interfere with the member of staff's duties or be for commercial gain.

- I will not create, transmit, display onscreen, print, retrieve, copy, or forward any material (text, sound, images or video), that is likely to harass, cause offence, insult, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, Omagh Academy or the Education Authority, into disrepute.

- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Principal.

- I understand that my use of the Internet, email and other related technologies can be monitored and logged to ensure school compliance.

- The school may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this AUP. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the PSNI.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ……..... Print Name: …….. Date: ……
Job title …… Accepted by: ……. (Print Name)

Note: This policy will be kept under review and is subject to change.

Appendix 2: Pupil Acceptable Use Policy

Omagh Academy Acceptable use of ICT by Pupils

1. I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.

2. I will not download or install software onto any school digital device unless instructed to do so by a teacher.

3. I will only log on to the school network with my own username and password.

4. I will follow the school's ICT security system and not reveal my passwords to anyone and will change them regularly.

5. I will use my school e-mail address for all school related communications and when in school I will
   only use the school's e-mail system.

6. I will make sure that all ICT communications with pupils, teachers or others are responsible, sensible and in good taste.

7. I will be responsible for my behaviour when using the Internet. This includes the resources I access and the language I use.

8. I will not deliberately browse, download, upload or forward material that could be considered offensive, obscene or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

9. I will not use the internet to give out any personal information such as my name, phone number or address. I will not use the internet to arrange to meet someone without the knowledge and permission of my teacher and/or parent.

10. Images of pupils and/or staff will only be taken with the permission of a teacher and subsequently stored and used for school purposes only in line with school policy. Images will not be distributed outside the school network without the permission of the person involved.

11. I will ensure that my online activity, both in school and outside school, will not cause my school, its staff, pupils or others distress or bring it into disrepute.

12. I will respect copyright, intellectual property and privacy rights of others' work online at all times.

13. I will not attempt to bypass the internet filtering system.

14. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.

15. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parents may be contacted.

Signed _____ (Pupil) Date _____

Signed _____ (Parent) Date _____

Appendix 3: Bring Your Own Devices Policy

Rationale

Sixth Form pupils have access to a limited number of private study periods during which they have the opportunity to focus on coursework, homework tasks and assignments. Traditionally much of this work has been completed using pen and paper but as the nature of exam courses change and more materials are made available in digital form, students are increasingly required to use and to produce materials in digital form e.g. via Teams. Omagh Academy recognises the benefits to learning from offering Sixth Form pupils the opportunity to use personal ICT devices in school to support learners and their learning. It is the intention of this policy to facilitate and support the use of personal ICT devices in school in furtherance of individualised student learning. Sixth Form pupils are expected to use personal ICT devices in accordance with this policy and must sign a declaration agreeing to be bound by the additional school rules and requirements set out in this policy before they will be permitted to use personal ICT devices in school.

Guidelines for Acceptable Use of Personal ICT Devices

· The use of personal ICT devices falls under the Omagh Academy Acceptable Internet Use Policy which all students must agree to and comply with. This policy can be accessed on the school website – www.omaghacademy.com

· The primary purpose of the use of personal devices at school is educational. Using the device for personal reasons should only take place after permission has been given from a teacher or other member of staff.

· Pupils are permitted to connect to C2K wireless networking services only while using a personal ICT device in school. No other wireless, wired or Internet service (including 4G or equivalent) is permitted.

· Pupils should keep their personal ICT device with them at all times.

· Use of personal ICT devices during the school day is at the discretion of teachers and staff. Students must use devices as directed by their teacher or study supervisor.

· The use of a personal ICT device is not to be a distraction in any way to teachers or other students. Personal devices must not disrupt class or private study areas in any way. Playing games or other non-school work related activities are not permitted.

· Pupils shall only use a personal ICT device while under supervision in Sixth Form Study or a subject classroom unless otherwise directed by a teacher e.g. on school visits or activities.

· Pupils shall make no attempts to circumvent the school's network security. This includes setting up proxies and downloading programs to bypass security.

· Pupils shall not distribute pictures or video or any other material relating to students or staff without their permission (distribution can range from emailing/texting one other person to posting images or videos online to a wider audience.

· Pupils must check their personal ICT device daily to ensure the device is free from unsuitable material and free from viruses etc. before bringing the device into school.

· Pupils must check their personal ICT device daily for basic Health & Safety compliance to ensure it is free from defects. Particular attention should be paid to the keyboard (all keys present; no bare metal exposed), the screen (free from flicker and damage) and the device battery (able to

hold a charge). Any personal ICT device that has obvious Health & Safety defects should not be brought into school.

- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass codes or PINS should be set on personal devices to aid security.
- Printing from personal devices will not be possible.

Consequences for Misuse/Disruption

In addition to dealing with misuse/disruption within the remit of Omagh Academy's Acceptable Internet Use Policy for Pupils and the Behaviour Management Policy one or more of the following sanctions may apply:

· Personal ICT device may be confiscated and kept in the School office until the end of the school day.

· Access to the C2K wireless network may be removed (temporarily or permanently).

. · Privilege of using personal ICT devices at school may be removed (temporarily or permanently).

· Serious misuse of Internet capable devices is regarded as a serious offence in direct contravention of Omagh Academy's Bring Your Own Devices (BYOD) Policy for Students, the Acceptable Internet Use Policy for Students and the Behaviour Management Policy and will be dealt with in accordance with these policies.

School Liability Statement

Pupils bring their personal ICT devices to use at Omagh Academy at their own risk. Students are expected to act responsibly with regards to their own device, keeping it up to date via regular anti-virus and operating system updates and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

Omagh Academy is not responsible for:

· Personal devices that are broken while at school or during school-sponsored activities.

· Personal devices that are lost or stolen at school or during school-sponsored activities.

· Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

· Parents should ensure they have adequate insurance cover in place to cover the cost of repair/replacement of a personal ICT device in the event of loss/damage to the device.

Disclaimer

Omagh Academy accepts no liability in respect of any loss/damage to personal ICT devices while at school or during school-sponsored activities. The decision to bring a personal ICT device into school rests with the pupil and their parent(s)/guardian(s), as does the liability for any loss/damage that may result from the use of a personal ICT device in school. It is a condition of agreeing to allow pupils to bring personal ICT devices into school, that the parent/guardian countersigning the permission slip accepts this disclaimer.

BRING YOUR OWN DEVICES (BYOD)

USER AGREEMENT FOR PUPILS IN YEARS 13 AND 14

Pupil Declaration:

I would like to use my own personal ICT device in school.

Device Type (please circle) You may register one of each device type if required:

Laptop **Smart Phone** **Tablet**

I have read and understood the Bring Your Own Devices Policy (BYOD) and I agree to be bound by the guidelines, rules and regulations contained in the BYOD Policy for Pupils, the Acceptable Internet Use Policy for Pupils and the Behaviour Management and Discipline Policy.

· I understand that the use of a personal ICT device in school is a privilege not a right and agree to use the device for **learning only**.

. · I agree to connect to the school-based C2K network service only while using my personal ICT device in school. I understand that connection to non-school provided wireless/networking services while using my personal ICT device in school is **prohibited**.

· I understand that I am **solely responsible** for the correct care, safety and security of my personal ICT device when in school.

Print Name: _____ Class: _____

Signed: _____ Date: _____ / _____ / _____

BRING YOUR OWN DEVICES (BYOD) USER AGREEMENT

Parent/Guardian Approval Disclaimer

Omagh Academy accepts no liability in respect of any loss/damage to personal ICT devices while at school or during school-sponsored activities.
The decision to bring a personal ICT device, including a Smart Phone into school rests with the pupil and their parent(s)/guardian(s), as does the liability for any loss/damage that may result from the use of a personal ICT device in school.

It is a condition of agreeing to allow pupils to bring personal ICT devices into school, that the parent/guardian countersigning the permission slip accepts this disclaimer.

I have read the **Bring Your Own Devices Policy (BYOD) for Pupils** and give my son/daughter approval to use a personal ICT device in school.

I understand my son/daughter is personally and solely responsible for the correct care, safety and security of the device.

I understand that the school accepts no liability in respect of any personal ICT device used in school by a student.

I understand and accept the disclaimer.

Signed: _____ (Parent/Guardian)

Date: _____ / _____ / _____

Appendix 4: Omagh Academy Policy on Pupil use of Mobile Digital Devices

The school recognises the widespread use of mobile digital devices in society and the workplace, and is committed to supporting pupils in developing disciplined, responsible, and effective use of such devices. To protect students and for the smooth running of the school, the use of mobile digital devices in school is controlled.

For the purposes of this policy, a mobile digital device includes, but is not limited to, mobile phones and smart phones as well as other 3G/4G and Wi-Fi enabled devices such as iPads, iPods, Tablets, smart watches, and laptops.

1. Pupils bringing a mobile digital device to school do so at their own risk.

2. Pupils are permitted to use mobile digital devices in school between 8.30am -3.30pm (or during school events taking place at other locations) only under the direction and supervision of staff. This means the devices should not be used in toilets, corridors, locker areas, changing rooms etc.

3. The camera facility on any mobile digital device may be used during lessons or on school trips and sporting events only when permission has been granted by the teacher in charge. The sharing/uploading of images (e.g., to social media) which would reflect negatively on the school or cause hurt or offence to others is strictly prohibited.

4. Mobile digital devices should be switched to silent during lessons/sixth form study periods. To facilitate this, pupils should set up 'Do not disturb' mode for school hours.

5. Pupils should not contact their parents/carers directly via phone, social media, or other electronic methods, to arrange to be collected. If unwell, pupils should report to the school office who will contact parents, if it is judged appropriate to do so.

6. Any pupil discovered to be in breach of the above rules will be subject to sanctions and have the device confiscated. Under normal circumstances, confiscated devices will be available for collection at 3.30 pm from the School Office and a Year Head's detention will be issued.

7. The use of any mobile digital device to record or transmit images or sound, without the prior agreement of the pupil or member of staff concerned, is potentially a serious matter that could result in suspension from school.

8. Pupils sitting formal or public examinations are reminded that mobile digital devices must not be brought into the examination hall as per JCQ guidelines. Switching off the device is NOT sufficient. Possession of a mobile digital device in the examination hall is considered to be a serious infringement of the regulations, resulting at the very least in disqualification from that examination. In accordance with the regulations set up by the exam board, a pupil discovered using a mobile digital device in an examination would be liable to disqualification from all examinations in the series.

9. Mobile digital devices owned by the school, such as iPads and laptops, must be treated with care and only used in the way specified by the teacher. Settings such as backgrounds and lock screens on such devices should not be adjusted by pupils.

10. Where a pupil asks to leave a lesson and permission is granted, the pupil's mobile phone should be left with the member of staff until their return to class. An exception will be made in

cases where a pupil has been given special permission to keep their phone with them for health-related reasons as specified and agreed by the Vice Principal (Pastoral Care)

11. Breaches of the above policy will be subject to disciplinary measures as outlined in the school's Behaviour management and discipline policy.

12. The school accepts no responsibility for theft, loss, damage or health effects relating to mobile telephones or other electronic devices. It is the responsibility of parents and pupils to ensure mobile telephones are properly insured.

Subject to the school's separate BYOD policy, Year 13 and 14 pupils are permitted to use their own digital devices e.g., laptops. Permission to bring a personal digital device will be withdrawn if BYOD policy conditions are breached. The safe keeping of any such device is the sole responsibility of the owner.

Appendix 5: Additional Advice for Parents with Internet Access at home

1. A home computer/laptop with Internet access should be situated in a location where parents can monitor access to the Internet. However, parents should be mindful of the fact that their child potentially has 24/7 access to the internet via mobile devices such as tablets and smart phones.
2. Parents should discuss the school rules for using the Internet with their children.
3. Parents should get to know the sites their children visit.
4. Parents should consider using appropriate Internet filtering software.
5. Parents should talk to their children about giving out personal identifying information in any electronic communication on the Internet, such as a photograph, an address, a phone number, the school's name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable communication, from unplanned expenditure and from fraud.
6. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school, they should immediately inform the school.

Further advice for parents is available from the following sources:

- https://www.ceop.police.uk/Safety-Centre/ The government's Child Exploitation and Online Protection Centre (CEOP)
- https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/staying-safe-online/ Childine – taking control of online safety
- https://reportharmfulcontent.com/?lang=en-gb Reporting harmful content
- https://www.internetmatters.org/ Digital safety
- https://www.childnet.com/ Helpful information and guidance on a range of key online safety topics
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/ Keeping children safe online
- https://onlinesafetyhub.safeguardingni.org/social-media-and-apps/ Safeguarding Board for Northern Ireland Hub
- Safer Schools App

Appendix 6 - Reporting Breaches of Online Safety

Incident Log Number: ☐ (To be completed by C2k Manager)	**Incident Reported by:** _____ Date reported : _____ /_____ /_____ (Orally) ☐ (In writing) ☐
Pupils involved in breach:	**Reported to:** C2k Manager_____ Pastoral staff _____
Details of incident:	
Action taken	
Review of Online Safety Policy/Strategies	
Update of logs: Online safety breaches Y / N Risk Register Y / N	**Recommended updates to online safety policy or OA procedures**
Signed: _____ **Date:** _____ /_____ /_____	