Omagh Academy

Online Safety Policy

A subsection of the Safeguarding/Child Protection Policy

September 2018

Date Approved by the Board of Governors: _____

Date of next review: _____

Signed: _____ **(Chair of Board of Governors)**

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
- The CCEA Requirements for using ICT
- The Data Protection Act (1998), Computer Misuse Act (1990) and Freedom of Information Act (2000)

Related School Policies

- Behaviour Management & Discipline policy
- Safeguarding/Child Protection policy
- ICT Acceptable use policy for pupils
- Policy on Pupil use of Mobile Devices
- Anti-bullying Policy
- ICT Acceptable use policy for staff
- I-Pad Acceptable use policy for Staff

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 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 online Safety Officer takes day-to-day responsibility for online safety within the school. She is responsible for the online safety policy and its implementation including the training and updating of staff on online safety matters. She also monitors 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. He/She 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 online Safety Officer. 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".
  (Details of persons with specific responsibilities relating to online safety can be found in Appendix 1)

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.
- In order 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 is 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 subject to the relevant AUP at all times.
- 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. Where relevant parents also will be consulted.
- 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. Additional access is available via a bookable i-pad facility which utilises the c2k Wi-Fi service.

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.

1. **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. The contribution of each subject to this curriculum by year group is outlined in Appendix 4. Raising awareness of the potential risks when engaging with online technologies is also addressed during assemblies and P.D. classes and by participation in awareness raising events such as 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. **Online safety awareness for school staff**

The Online Safety Officer will keep staff informed of online safety matters and will provide training in the delivery of online safety. She will also work alongside other Heads of Department, the ICT co-ordinator, the PD co-ordinator and pastoral staff to design and resource a cohesive and progressive age appropriate online safety curriculum.

3. **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 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, end of term newsletters and on bulletin sheets and letters delivered with school reports.

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 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.

2.5 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.

The online safety officer, in collaboration with the Principal/Senior Management Team will monitor and review the effectiveness of the AUPs, particularly in the light of new developments in technology.

(Appendix 2 – Staff AUP/Staff i-pad AUP, and Appendix 3 – Pupil AUP/ Pupil Policy on the Use of Mobile Digital Devices)

3.0 Managing and reporting incidents

3.1 Investigating breaches of online safety guidelines

All incidents of malpractice should be reported in the first instance to the Online Safety Officer (Mrs Clarke) 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 Online Safety Officer (Mrs Clarke) or a member of the senior management team (SMT).
- 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 Online Safety Officer (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 Mrs Clarke, the pupil's Year Head or a member of the SMT 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 Online Safety Officer 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 Online Safety Officer, the designated teacher and the Principal should be informed. Guidance will then be sought from the EA and if appropriate the PSNI informed.
- The Online Safety Officer or in her absence a 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 Online Safety Officer 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 Mrs Clarke, who will also inform the principal of the breach and how it was managed.
- The Online Safety Officer 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.

3.2 Examples of breaches of online safety guidelines

- Examples of incidents which should be reported to the Online Safety Officer include plagiarism or copyright infringement, downloading materials or images not relevant to the subject, using someone else's password or sending nuisance text messages.
- More serious 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 our anti-bullying policy.

4.0 The School's Website and Facebook Profile:

The school's website and Facebook profile 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. (Mrs Donnelly). 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 Facebook profile and its associated published statuses are monitored by Mrs Donnelly who also regularly updates this social media presence and ensures all published material is in keeping with school protocols.

5.0 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 with responsibility for the website who will keep a register of the accounts and who has editing access to them. 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. All material posted on Facebook accounts associated with the school will be duplicated on the official Omagh Academy Facebook page.

The school endeavours to educate pupil 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 Online Safety Officer. In addition, the school retains the right to discipline pupils for incidents of cyberbullying, whenever or wherever they occur. (See Anti-bullying Policy).

6.0 Communication of the Policy

This policy has been written by the Online Safety Officer and pastoral leaders within the school. 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: Persons with Specific Responsibilities in Relation to Online Safety

- **The Principal:** **Mrs R Maxwell**

- **The Governor with Responsibility for Child Protection including Online Safety:** **Mr T Bradley**

- **The Online Safety Officer:** **Mrs K Clarke**

- **The Designated Teacher for Child Protection:** **Mrs C Gervais**

- **The C2 K Managers:** **Mrs K Clarke**

  Mr R Wilson

- **The Member of Staff with oversight of school Website:** **Mrs L Donnelly**

- **The Member of Staff with oversight of school's Facebook Profile:** **Mrs L Donnelly**

Appendix 2: Staff Acceptable Use Policies

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 system managers Mrs K Clarke or Mr R Wilson.

- 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 newssheets 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 or Learning NI 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 Child Protection Teacher, Mrs C Gervais, or the Deputy Designated Teacher, Mrs S Smith, as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Mrs K Clarke the C2k Manager, or Mr R Wilson the C2k Assistant 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 Managers Mrs K Clarke or Mr R Wilson, or to the ICT technician Mr A McGlinchey 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 Management Team.

- I will exercise caution when using social media sites such as Facebook and Twitter. 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 WELB, 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, Mrs R Maxwell.

- 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 by the Governors, Online Safety Officer and SMT and is subject to change.

Omagh Academy Acceptable i-Pad Use Policy for Staff

This policy is designed to help and protect staff in Omagh Academy. When using an iPad and Apple TV, supplied by the school, you are agreeing to/accepting that:

Provision of Equipment
Staff will be given an iPad, protective case and charger.

Administration and Security

1. The iPad and/or Apple TV are the property of the school.
2. Use of the iPad/Apple TV is for educational purposes and all relevant school policies are applicable.
3. The device must not be lent to any other party such as family members, friends etc.
4. The device can be recalled, by the school, at any time.
5. iPads can be taken out of school but should be available for use in school during the day.
6. Every precaution is taken to avoid damage to or loss of the devices.
7. The case provided by the school must be used as they provide adequate protection for the device and kept together with the iPad and charger
8. The Apple TV should not be taken home for personal use.
9. Staff should take caution of where they place their iPad in school.
10. A four/six digit security PIN must be used to secure the device.
11. The security PIN of the device is held by its specified users and must never divulged to pupils, or any other party including family members, friends etc.
12. Staff provided with an iPad or Apple TV must follow the School's Acceptable Use of ICT Policy and the Child Protection Policy at all times.
13. Staff will try out the core and subject specific apps that have been downloaded to their iPads;
14. Staff will attend all relevant training and complete any tasks assigned for review and progression evaluation;
15. Staff will look for, trial and demonstrate innovative teaching practice;
16. Staff will liaise with HoDs with a view to integrating the iPad as a learning and teaching tool in specific lessons.
17. Staff will share good practice with department colleagues and staff from other departments;

iPad Use and Data Storage

1. Use of the iPad in the classroom and other learning and teaching environments, must be for educational purposes exclusively. Use must be an integral part of planned learning and teaching programmes. Other uses are not permissible in the classroom and in other learning and teaching environments.
2. Files stored on the iPad will not be regarded as private. The school reserves the right to monitor, review and examine the content, internet history, usage, communications and files of users, and, where it deems it to be necessary, will intercept and delete material which it considers inappropriate, and prohibit the use of such material.
3. Documents on the iPad should be backed-up regularly using the Cloud Storage capabilities and one other online storage method preferably One Drive.
4. Materials used must be age appropriate. Professional discretion must be used in relation to materials stored or used.
5. Materials used must be previewed before use in the learning and teaching environment.
6. Contact with pupils and their parents must be kept strictly within an educational context. You must only use official school channels when communicating with pupils and parents.
7. No illicit, adult, gambling or other inappropriate content, that may bring the school into disrepute, should be accessed.

Staff should not:

1. Modify the settings of their iPad's in any way unless instructed by the ICT Co-ordinator, ICT Support Teacher or ICT Technician.
2. Apply any permanent marks, decorations or modifications to their iPads;
3. Remove their iPads from their protective cases.

Using the IPAD

1. The ICT Technician and iTeach will initially set up the iPad and these settings should not be changed by staff.
2. Staff should clean the screen often with approved cleaning towels (available from the ICT Technician upon request) and keep away from food and drink.
3. The iPad should only be charged with an Apple charger and standard wall outlet as the power source.
4. Any errors or problems with the iPad should be reported to the ICT Technician as soon as possible.

Apps

1. Apps for use in school should be requisitioned from departmental budgets via the school office staff in the normal way. These will then be installed by the ICT Support Teacher.
2. The ICT Support Teacher on request will enter the school Apple ID password to download whole school Apps.

3. Key apps have been pre-installed on each iPad by the ICT Support Teacher.
4. Individual members of staff are also allowed to purchase appropriate apps for themselves, using their own Apple ID, as long as they are in keeping with the School's Acceptable Use Policy. The cost of such apps will not be reimbursed.

Use of Digital Media

1. The use of the iPad camera must be in line with the school's Child Protection Policy.
2. Teachers are responsible for understanding and adhering to all copyright requirements and policies related to digital media and the use of this iPad.

Professional Development

1. Teachers must undertake professional development e.g. attend training sessions, collaborate with colleagues in the development of best practice and resources, and complete a PRSD lesson with the use of their iPad as a teaching tool.
2. Teachers must attend and contribute to departmental support sessions.

Reporting Incidents

1. Concerns are to be reported immediately to either the Principal, Vice-Principal, ICT Co-ordinator or ICT Support Teacher. For example, concern about: - inappropriate pop up messages or websites; receipt of inappropriate images or messages; about inappropriate activity; identity theft etc.

2. In the case of loss, theft or other damage occurring, either inside or outside of school, the ICT Coordinator and ICT Support Teacher must be informed as soon as possible.

The school expects and requires all users to comply with the standards outlined in this policy and to follow its protocols. Users in breach of the iPad Acceptable Use Policy may be subject to; disciplinary action, confiscation of the device, removal of content or referral to external agencies in the event of illegal activity.

Signature of teacher: .....

Signature of ICT Co-ordinator: .....

Date: .....

Note: This policy will be kept under review by the Senior Leadership Team and is subject to change.

Appendix 3: Pupil Acceptable Use Policies

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 user name 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 _____

Omagh Academy Policy on Pupil use of Mobile Digital Devices

In the interests of protecting pupils and of the smooth running of the school, the use of mobile phones and other electronic devices within school is limited.

1. A pupil who brings a mobile phone or other electronic device to school does so at their own risk.
2. Pupils are not permitted to use mobile phones in school or during formal school events taking place at other locations. Mobile phones must be kept switched off within the school premises between 8.30 am and 3.35 pm.
3. Pupils are prohibited at all times from using the camera facility on any mobile digital device e.g. phones within the school premises.
4. Digital cameras must not be brought to school without the permission of a senior member of staff [Head of Year, Head of Department etc.] and then only for a specific purpose, agreed in advance.
5. Any pupil discovered to be in breach of the above rules will be disciplined and have the device confiscated. Under normal circumstances, confiscated phones/cameras will be available for collection at 3.30 pm from the School Office.
6. Pupils and parents should be aware that use of any electronic digital device (e.g. camera phones, tablets etc.) 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.
7. Pupils sitting formal or public examinations are reminded that mobile phones MUST NOT be brought into the examination hall. Switching off the phone is NOT sufficient. Possession of a mobile phone in the examination hall is considered to be a serious infringement of the regulations, resulting at the very least in disqualification from that examination. A pupil discovered actually using a phone in an examination would be liable to disqualification from all examinations in the series. This decision is taken by the Examination Board not the School.
8. In exceptional cases a mobile phone may be used for communicating with parents/carers during the school day, but only with permission from a senior member of staff [e.g. Head of Year or Head of Department].
9. Digital devices owned by the school, such as i-pads, must be treated with care and only used in the way specified by the teacher.
10. Pupils in the sixth Form can use their own digital devices e.g. lap tops, within the Sixth Form centre, provided their use is restricted to private study. Permission to bring a personal digital device will be withdrawn if this restriction is breached. The safe keeping of any such device is the sole responsibility of the owner.
11. Breaches of this policy will be subject to disciplinary measures as outlined in the school's behavioural management policy.

Signed _____ (Pupil) Date_____

Signed _____ (Parent) Date_____

Appendix 4: The e-Safety Curriculum – School Provision Audit

Year 8	
Term 1	
History	Internet- dangers of using Wiki sites such as Wikipedia in terms of bias.
Art & Design	Creation of online Safety Posters for external or PSE competitions
PD	Bullying – Coping Skills
Term 2	
Term 3	
English	Analysing leaflets in the media – Collaborative unit between English and ICT. Pupils design a leaflet highlighting 'Internet Safety'.
ICT	Internet Safety – Advantages and disadvantages of using the internet. Highlights the dangers of using the internet and signs of grooming, problems with chat rooms, cyber-bullying. Putting in place strategies of how to stay safe online. Pupils produce an information leaflet suitable for parents.
PD	Personal Internet Safety

Year 9	
Term 1	
History **Art & Design** **PD**	Go conqur- danger of accepting friend requests from strangers. Graphics design- airbrushing in the media- airbrushing today vrs the airbrushing of Hans Holbein &The courts of Henry VIII & Elizabeth 1. Creation of online Safety Posters for external or PSE competitions Internet Safety
Term 2	
ICT	Graphics Design: Air-brushing in the media. False expectations of how we should look – impact on pupils' interaction on social media platforms.
Term 3	
English **Mathematics**	Analysing leaflets in the media – Collaborative unit between English and ICT. Pupils design a leaflet highlighting 'Internet Safety'. Financial Maths – ebanking, purchasing online, bank cards and dangers including privacy and sharing, strategies for banking/purchasing safely online.

Year 10	
Term 1	
History **ICT** **HE** **Art & Design** **Music**	Internet safety- fake news. Cyber-bullying and digital foot prints – consequence of inappropriate internet usage e.g. indecent images, suicide, loss of privacy and reputation. Pupils will produce an anti-bullying video in respect to cyberbullying. Shopping online Consumer Legislation, how to shop safely Creation of online safety posters for external or PSE competitions Copyright, royalties, marketing and protection of intellectual property in the music industry
Term 2	
English	The Media – analysing a range of texts and ascertaining how reliable they are. Looking at trustworthy sources and how the media manipulates the reader e.g. advertising.
Term 3	
PD	Healthy Relationships Safer social networking

Year 11	
Term 1	
History	Go conqur- danger of accepting friend requests from strangers.
Business Studies	Investigations into e-marketing and m-marketing How businesses target customers and keep track of buying habits. The convenience and dangers of Internet business
PD	e-Safety
Art & Design	Develop awareness of plagiarism in written and practical work – no art work should be photographed and shared online before moderation (copyright) How to use the departmental Facebook page appropriately and safely when sharing posts, commenting etc
Term 2	
Term 3	
HE	Online shopping – advantages and disadvantages

Year 12	
Term 1	
History	Go conqur- danger of accepting friend requests from strangers.
Business Studies	Investigations into e-marketing and m-marketing How businesses target customers and keep track of buying habits. The convenience and dangers of Internet business
PD	e-Safety
HE	Inform pupils about the danger of using untrustworthy websites for research
Modern Languages	GCSE FR/GR/SP: Social media and new technology – using the internet safely
Term 2	
ICT/Digital Technology	The rights and responsibilities of digital citizenship demonstrated through viewing and discussing the 'Tagged video https://www.esafety.gov.au/education-resources/classroom-resources/tagged Issues such as cyberbullying, sexting, and digital reputation discussed in an age-appropriate manner. Pupils complete and analyse their own Digital Footprint through completing a personal audit. Pupils acquire knowledge of how to protect themselves and others from cyberbullying, privacy and digital reputation issues. They recognise that unethical behaviours such as harassment and bullying can contribute to negative online experiences and have longer term consequences. Analyse different ways in which damage to a digital reputation occurs and how long it may last. Use One Drive to contribute to a collaborative piece of group work. Pupils will produce a e-Safety guidance document relating to a social media app taking the target audience into consideration.
Term 3	

Year 13	
Term 1	
Health and Social Care	Inform pupils about the danger of using untrustworthy websites for research.
History	Go conqur- danger of accepting friend requests from strangers.
Modern Languages	AS French & Spanish Influences on young people Social media and new technologies
Psychology	Examining Prejudice in the media. Minimal look at e-Safety
Business Studies	e-marketing and m-marketing and how businesses use social media
HE	Inform pupils about the danger of using untrustworthy websites for research.
Term 2	
Health and social Care	Inform pupils about the danger of using untrustworthy websites for research.
HE	Inform pupils about the danger of using untrustworthy websites for research.
Psychology	Revision of examining prejudice in the media. Minimal look at e-safety.
Term 3	
Health and Social Care	Inform pupils about the danger of using untrustworthy websites for research.
HE	Inform pupils about the danger of using untrustworthy websites for research.

Year 14	
Term 1	
Health and Social Care	Inform pupils about the danger of using untrustworthy websites for research.
HE	Inform pupils about the danger of using untrustworthy websites for research.
History	Go conqur- danger of accepting friend requests from strangers.
Psychology	Discussion of prevalence of depression and mental health in the media.
Business Studies	e-marketing and m-marketing and how businesses use social media
Term 2	
Health and Social Care	Inform pupils about the danger of using untrustworthy websites for research.
HE	Inform pupils about the danger of using untrustworthy websites for research.
Digital Technology	Pupils discuss and explain the ethical considerations around: online censorship; monitoring of personal behaviour; and the capture, storage and analysis of personal information.
Term 3	
Health and Social Care	Inform pupils about the danger of using untrustworthy websites for research.
HE	Inform pupils about the danger of using untrustworthy websites for research.

Geography – The Geography department ensures that pupils are guided to appropriate websites as and when required. This is the safeguarding method as in the case of Geography they may come across sites of mis-information or distressing images.

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

1. A home computer 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 agree with their children suitable days/times for accessing the Internet.

3. Parents should discuss the school rules for using the Internet with their children and endeavour to implement these at home. Parents and children should decide together when, how long and what constitutes appropriate use;

4. Parents should get to know the sites their children visit and talk to them about what they are learning;

5. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents' Information Network (address below);

6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities;

7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school 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 overtures from strangers, from unplanned expenditure and from fraud.

8. 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:

- http://www.thinkuknow.co.uk Thinkuknow - a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.

- http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf Aimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.

- http://www.parentscentre.gov.uk/usingcomputersandtheinternet A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.

- http://www.bbc.co.uk/webwise Includes an 'Internet for Beginners' course and a tool for answering your internet related questions.

- http://www.kidsmart.org.uk/ Explains the SMART rules for safe internet use and lots more besides.

- http://www.ceop.gov.uk/ The government's Child Exploitation and Online Protection Centre (CEOP)

- http://www.parents.vodafone.com Vodafone's site is designed to help parents and carers develop an understanding of their child's internet use.

Appendix 6 - Reporting Breaches of Online Safety

Incident Log Number: ☐ (To be completed by e-safety officer)	**Incident Reported by:** _____ Date reported : _____ /_____ /_____ (Orally) ☐ (In writing) ☐
Pupils involved in breach:	**Reported to:** Online Safety Officer _____ Pastoral staff _____
Details of incident:	
Action taken by Online Safety Officer	
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:** _____ /_____ /_____	