eSafety, ICT Acceptable Use and Digital Media Policy

1. INTRODUCTION

1.1 This policy acknowledges and complies with relevant DENI circulars relating to e-safety, digital media and acceptable use of ICT.

1.2 **The Internet, Cloud and Digital Media**

Internet –The Internet is not governed by an international body; therefore, there are dangers concerning the kind of information that is accessible to its users. However, the educational value of appropriate use of information and resources located on the internet is substantial.
Cloud – Cloud-based learning and teaching encompasses a broad range of educational resources available in an online environment. This includes My School, C2k approved Virtual Learning Environments (such as Google Classroom and MS Teams) and other online resources.
Digital Media – This covers all hardware, software, portable and non-portable devices used for educational purposes inside and outside school.

1.3 **Rationale for pupil use of the Internet, Cloud and Digital Media**

The School encourages pupils to use the rich educational information sources available on the Internet and Cloud, together with the development of appropriate skills using digital media to fully utilise such resources. On-line resources offer pupils a broad range of up-to-date information; provide independent research facilities; facilitate a variety of learning styles; and encourage pupils to take responsibility for their own learning. E-literacy is a fundamental requirement for all pupils in order to prepare for the continually developing technological age that we live in and to enable pupils to demonstrate a positive digital footprint.

This policy will help reduce risks of pupils and staff accessing harmful and inappropriate content, as well as teaching pupils how to keep themselves safe in the digital world.

1.4 **Networked Access to Internet, Cloud and Digital Media**

The school provides filtered internet access to pupils and staff on both the C2k and the School's non-C2k networks. **Only filtered internet connections provided by, or on behalf of, the school may be used to access on-line material at school.** Parents, pupils and staff are reminded that all mobile electronic devices must also be used in accordance with the *Mobile Phone Policy*.

1.5 **How will pupils gain access to the Internet, Cloud and Digital Media at School?**

- During ICT lessons
- Through subject use across the curriculum
- During extra-curricular activities
- In the study areas, during normal school hours and occasionally at other times
- Through C2k Wireless provision (filtered)

1.6 **Are there any dangers associated with using the Internet, Cloud and Digital Media?**

Since the Internet and Cloud are composed of information from a vast array of sources world-wide, they include some material that is not of any educational value in the context of the School. This material may include information that is inaccurate, abusive, profane, sexually oriented, racist or illegal.

In order to safeguard young people from any inherent dangers, it is the joint responsibility of the School and parents/guardians to educate pupils about their responsibility when using the Internet and Cloud. The School will keep parents and guardians updated of online safety concerns and awareness through updating the school website and through home-school communication.

1.7 **Promoting Safe Working Practices**

The School is determined to continue to provide high-quality training for staff and pupils to make best use of its ICT facilities. Pupils will be provided with appropriate training and guidance on how to safely use the Internet, Cloud and digital media during KS3 ICT classes. Staff will continue to receive appropriate training in the safe use of the Internet, Cloud and digital media.

Pupils and staff will also be advised of the Health & Safety issues surrounding the use of digital media technology.

1.8 **Promoting Awareness with Parents, Governors and Community**
The School is committed to ensuring all stakeholders are made aware of this policy. The policy will be disseminated to parents, governors and staff. It will also be available on the school web-site so that other interested stakeholders can have full access. In addition, regular references will be made to the policy in communications with all stakeholders.

2. RESPONSIBILITIES OF STAFF AND PUPILS

2.1 Pupils are responsible for good behaviour when using the Internet, Cloud and digital media just as they are in the classroom or elsewhere in the school. General school rules apply.

2.2 The School has a filtered internet, cloud and e-mail service. Pupils and staff will be made aware that internet, cloud and e-mail services are monitored and are not therefore private; internet, cloud activity and e-mail messages can be viewed by the Principal at any time. While normal privacy is respected and protected by password controls users must not expect internet and cloud activity, e-mail or files to be absolutely private.

Filtering of the network is monitored by the ICT Technician and adhere to ISO 27001 standard security across the C2k system. The School runs software to filter internet access and to monitor and block inappropriate websites on the legacy network. All staff and internal emails are filtered for inappropriate content.

Whilst access to the Internet on the C2k and non-C2k systems is heavily filtered to protect the interests of staff and pupils, in certain circumstances access may be granted to staff to sites which would normally be restricted. Requests for access to blocked sites should be made using the *Request for Access to and Risk Assessment of Blocked Media or Emerging Technology* pro-forma contained in Appendix 3. In accessing these sites, staff should exercise caution. These sites may contain inappropriate or questionable information including user-generated content. It is the responsibility of staff who wish to use these restricted sites to vet the links they plan to use.

Some sites, notably YouTube, may also have an impact on the School's internet bandwidth if used excessively, reducing the bandwidth available for other purposes. Therefore, consideration for other users should be exercised when accessing these sites.

The School will operate a Risk Register that will record possible online safety issues and highlight where data security might be potentially breached. This will be managed by the ICT Technician and monitored by the Head of ICT.

The school will operate a Register of Access that will outline who has access to the different pupil and staff data available on the C2k network and school system.

2.3 Particular care should also be taken while projecting information from a digital media device onto a whiteboard or other form of facility, as inappropriate material may be displayed.

2.4 Access to the Internet, Cloud and digital media requires parental permission and a signed declaration by pupils agreeing to the school rules for use of the Internet, Cloud and digital media (Appendix 2).

2.5 The School will ensure that all pupils understand how they are to use the Internet, Cloud and digital media appropriately and why the rules exist.

2.6 The Internet, Cloud and digital media are provided for pupils to conduct research, communicate with others and fulfil their curricular requirements. While the use of information and communication technologies is a required aspect of the statutory Northern Ireland Curriculum, access to the Internet, Cloud, digital media and C2k services remains a privilege and not a right. Access is granted to pupils who act in a considerate and responsible manner and will be withdrawn if they fail to maintain acceptable standards of use.

2.7 During school hours, teachers will guide pupils towards appropriate materials. Outside school hours, families bear responsibility for such guidance as they must also exercise care with information sources such as television, telephones, movies, radio, and other potentially offensive media.
Please note that any filtering available at home may not be subject to the same stringent requirements as we have in place to protect users at school.

2.8 When using the Internet, Cloud and digital media at school, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws.

2.9 If at any time pupils find themselves able to access, from within the school, internet sites which they think should be blocked, they should advise their teacher immediately. Likewise, staff should immediately advise the member of the Senior Leadership Team in charge of Digital Strategy (or, in his/her absence, another member of the Senior Leadership Team).

2.10 Any resources or materials downloaded by teachers, pupils or parents for use within school, must abide by the requirements of this policy and be suitable for use in the classroom. If an individual is unsure regarding the appropriateness of content, they should seek advice from the member of the Senior Leadership Team in charge of Digital Strategy before accessing the material within school (or, in his/her absence, another member of the Senior Leadership Team).

2.11 All school resources (including computers, laptops, tablets and other digital devices) and their associated accessories are provided for educational use; they must not be used for any other purpose. Only portable resources may be removed from school, to facilitate preparation for teaching and learning, in accordance with the details set out in Appendix 5; however, the resources may not be passed on to any third party. Staff members must sign Appendix 5 to ensure compliance with the policy.

2.12 Students should report any online safety issues to a member of staff. Issues of a serious nature that may relate to safeguarding and child protection, should be communicated to a designated teacher. Staff, students and parents are informed each year of the safeguarding team with displays in classrooms showing names and a photo of the Designated Teacher and Deputy Designated Teachers. E-safety issues relating to safeguarding will follow existing procedures outlined in the school's *Safeguarding & Child Protection Policy.*

2.13 Staff should be aware of specific types of online risk that students are exposed to when online. These risks are outlined in DE Circular 2017/04 (revised September 2023) and are categorised as being: Content Risks, Contact Risks, Conduct Risks and Commercial Risks. Through staff training and the taught curriculum, staff and students will be made aware of such risks. Training and education will also include highlighting online risks such as Grooming, Child Sexual Exploitation and radicalisation.

2.14 Sexting is the sending or posting of sexually suggestive images, including nude or semi-nude photographs, via mobile digital devices such as smart phones. Sexting between individuals in a relationship may be illegal under the Sexual Offences (NI) Order 2008 if anyone in an image is below 18. The school will use procedures outlined in the *Safeguarding & Child Protection Policy* as well as inform the PSNI for advice and guidance.
Sexting that involves an inappropriate image or links on the internet to an inappropriate image, **that is shared with intent to cause distress**, is an offence under the Criminal Justice Act 2015. The School is not required to investigate such matters and will report any incidents to the PSNI. Students are made fully aware of the dangers of sexting in assemblies and as part of the pastoral taught programme.

3 EXAMPLES OF ACCEPTABLE AND UNACCEPTABLE USE OF THE INTERNET, CLOUD AND DIGITAL MEDIA

3.1 **Activities which <u>are</u> encouraged include, for example:**

- the use of digital media for appropriate educational purposes only to communicate between colleagues, between pupil(s) and teacher(s), between pupil(s) and pupil(s), between schools and external agencies;

- use of the Internet, Cloud and digital media to research and develop topics related to social, personal, academic and professional development;
- use of the Internet, Cloud and digital media to investigate careers, continuing professional development and Further/ Higher Education; and
- the continuing development of pupils' and staffs' digital competence skills.

3.2 **Activities which are <u>not</u> permitted include, for example, to:**

- retrieve, store, send, copy or display offensive information;
- use obscene, racist or offensive language;
- harass, insult, bully (cyber bullying) or cyber attack others;
- share or use another user's password;
- leave a computer unattended when it is logged on;
- trespass in another user's folders, work or files;
- intentionally waste resources (such as on-line time and consumables);
- use the network for unapproved commercial purposes;
- share information with others relating to another without their prior consent;
- share intimate information or images about themselves or others;
- use ICT resources in any way that contravenes Health & Safety guidelines;
- search, download, view and/or retrieve materials that are not related to the aims of the curriculum or future careers;
- damage any school device, computer system or computer network. This includes hardware, software, files or information stored/displayed on any school device;
- load / connect any unauthorised outside software or hardware onto the school system;
- spread computer viruses (all downloaded files and external storage devices must be checked for viruses before being used on the school system);
- violate copyright laws – copy, save and/or redistribute copyright protected material;
- attempt to access the Internet independent of the school's filtered C2k and non-C2k system;
- subscribe to any services or order any goods or services, unless specifically approved by the School;
- play computer games or use social media chat sites;
- use the network in such a way that use of the network by other users is disrupted (for example, downloading large files during peak usage times; sending mass email messages);
- publish, share or distribute any personal data/information about a user (such as home address, email address, phone number etc.);
- any activity that violates a school rule;
- use any equipment to photograph, record or video any school activity for which explicit permission has not been given;
- use or distribute, including on social networking sites, any material relating to school activities, pupils or staff for which explicit permission has not been given. This includes the posting of material, images or video footage relating to school **staff,** pupils, the school environment or school name without prior written consent from the Principal or an appointed deputy. This applies to curricular and extra-curricular aspects of school life as well as to all school trips; and to
- engage in any activity that is harmful or hurtful to others.

4 SANCTIONS

4.1 Violation of the above rules will result in a temporary or permanent ban on Internet, Cloud and digital media use. Additional disciplinary action may be added in line with existing school behaviour policy rules on inappropriate behaviour. Where applicable, the PSNI or local authorities may be involved.

5 LOCATION AND PUPIL SUPERVISION

5.1 There is broad access to the Internet, Cloud and digital media covering most areas of the school including filtered wifi.

5.2 In order to reinforce good practice. it is important that pupils should be reminded frequently of their responsibility to use the Internet, Cloud and digital media in line with the school policy on acceptable use.

5.3 While using the Internet, Cloud and digital media at school, pupils should, where possible, be supervised directly by a member of staff.

6 STAFF USE OF INTERNET, CLOUD AND DIGITAL MEDIA

6.1 Teacher use of the C2k service, non-C2k networks and digital media devices must be in support of the aims and objectives of the school curriculum and School Development Plan. C2k in particular supports the implementation and sharing of effective practices and collaborative networking across the province, as well as nationally and internationally.

6.2 The internet, cloud and digital media training of staff will also focus on the use of C2k resources, amongst others, in their teaching and learning activities, to support the School's pastoral life and streamline administration procedures. Furthermore, staff will be given the opportunity to request additional training at any time.

6.3 All school staff (both teachers and non-teaching staff) are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the school.

6.4 Staff must not communicate with pupils, either personally or professionally, using social networking sites, email or other technologies which are not managed or approved by the school or C2k providers.
Staff are advised that it is neither acceptable practice, nor school policy, to befriend or browse the profiles of pupils or parents using social networking sites, e.g. Facebook. Similarly, it is not considered appropriate or acceptable for pupils or parents to request "friend" status with staff. Furthermore, for both professional and personal security, staff are strongly encouraged to regularly review their own personal security settings on social media sites in line with similar advice and guidance provided for pupils annually.

Please note that this policy should be read in conjunction with TNC 2016/2: *Disciplinary Procedure for Teachers Including Principals and Vice Principals in Grant-Aided Schools with Fully Delegated Budgets*.

All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, is still subject to General Data Protection Regulation (GDPR).

6.5 In the absence of available technical support, the integrity of the network must be preserved to a level which safeguards both data and safeguarding and child protection procedures.

7 ACCEPTABLE USE OF DIGITAL MOVING/STILL IMAGES OF PUPILS

7.1 All staff should follow the guidance below when dealing with taking, display, storage and use of moving/still images of pupils.

7.2 **Taking of Photographs/Video of Pupils**
Parents will be asked to give their consent in writing to a range of such activities. A central database will be maintained of those pupils for whom parental permission has and has not been received. Staff will be required to consult this database prior to taking any images of pupils.

7.3 **Display/use of Photographs/Video of Pupils**
Staff are permitted to capture and/or use moving/still images of pupils, for whom parental permission has been appropriately received, for display purposes and publicity in and outside school, in school publications, on the school digital signage and website. Where staff require additional guidance on the display/use of moving/still images of pupils, the Principal should be consulted. The Principal must grant permission for images of pupils to be distributed to any external media provider.

7.4 **Capture & Storage of Photographs/Video of Pupils**

Staff are encouraged to call upon the Teacher i/c of PR / Vice Principal i/c of Corporate Development, PR & Communications to assist with the taking of photographs/video for school business. It is recognised, however, that in many circumstances (for example, field trips, sporting events or incidental activities within departments) this is not always possible or appropriate. In these circumstances, staff are encouraged to capture moving/still images of pupils using hardware which has been procured by the school.
It is not considered acceptable to use personal mobile phones to capture any such images. Furthermore, it should not be normal practice to store images of pupils (however obtained) on school / personal digital media devices, in a printed format or on any external memory device as a matter of course for prolonged periods of time.

As a result, staff should ensure that:

1. Any images of pupils stored digitally should be stored on C2k staff folders. Technical support will be available from the ICT support staff to assist in the transfer of existing/new images.
2. Staff must transfer digital media from capture devices to C2k staff folders at the earliest possible opportunity. In order to maximise the efficient use of school resources, staff should do this by ensuring that:
    a. only files which are most suitable for school business are selected
    b. selected files are copied to a shared C2k staff folder
    c. remaining images from the initial capture device are deleted
    d. images are located in an appropriately named folder. (Consider *Activity – Year Group – Date* to be appropriate, e.g. "Residential Y8 20.5.23")
3. Staff are discouraged from storing images of pupils on school provided portable devices; however, it is recognised that, to facilitate editing or selection this may be essential. In these circumstances, personal portable devices should not be used. It is expected that, after initial use by staff, digital images of pupils should be deleted from portable devices as soon as possible.
4. Staff should not pass images of pupils to third parties without consulting the Principal. Please consult the Principal if you require further advice.

Some subjects, for example drama, media studies and physical education, have specialist course requirements which necessitate the use of digital moving/still images of pupils to address course criteria. In some circumstances, technical limitations of the C2k system prevent files from being usefully stored within the staff resources area. In subjects where these circumstances have been identified, the storage of digital images is permissible on external storage devices providing:

1. The storage device is owned by the school.
2. The storage device is normally retained within the school building.
3. All departmental staff members are fully aware of the purpose of the specific storage device and its normal secure location within the school building.

There may be a need, at certain times throughout the year, to facilitate formative and summative feedback or assessment. In these circumstances, the storage device may be taken home by the staff member concerned providing:

1. All reasonable precautions are taken to ensure the security of the storage device.
2. The storage device is returned to school at the earliest opportunity.
3. The storage device is strictly used for purposes approved by the school only.

8 INFORMATION AND DATA MANAGEMENT

8.1 The school values the importance of appropriate data management procedures and practices and requires all staff to be prudent regarding sensitive personal materials, whether paper based or electronic.

Staff are encouraged to use SIMS.net to access the personal information of pupils. This is provided within school and is always password protected.

Staff must **not** store electronic copies of sensitive personal information on the following:

- Any personally owned portable or non-portable device.
- Portable storage devices eg. portable hard-drive or memory stick. (Neither School procured nor personally owned portable devices are considered acceptable for sensitive data).

Staff may store basic pupil information electronically, for example, name, form class and performance statistics, for the purposes of recording pupil achievement throughout the year. This information may be removed from the school building to facilitate assessment activities. Staff must ensure that they hold the minimum amount of personal data necessary to enable them to perform their duties. The data must not be held any longer than necessary for the purposes it was collected for. Every effort must be made to ensure that data is accurate, up to date and that inaccuracies are corrected without any unnecessary delay. Staff are advised to be prudent about the sensitivity of this data and are required to maintain its confidentiality.

9 PERMISSION FROM PARENTS AND GUARDIANS

9.1 Parents/guardians will be provided with the e-Safety, ICT Acceptable Use and Digital Media Policy and permission will be sought for their child/ren to use the internet, cloud and digital media. Pupils are also required to sign an undertaking agreeing to their proper use of the internet, cloud and digital media. Details of the letter sent to parents and additional guidance information is included in the appendices to this policy.

10 WEBSITE & DIGITAL SIGNAGE

10.1 The school website and digital signage will be supported by a range of staff members in accordance with the guidelines set out in Appendix 4.

11 USE OF SOCIAL MEDIA SITES FOR EDUCATIONAL PURPOSES

11.1 Subject to the approval of the Principal, staff may use social media sites for educational purposes only.

Staff requesting the use of such sites for educational purposes must:

- Specify the proposed site;
- Specify who would be involved;
- Conduct a risk assessment;
- Provide a clear rationale stating the benefits of the proposed activity; and
- State how long the site will be operational.

Only one member of staff should be responsible for the operation of the site. Their login and password details must not be shared.
Another nominated member of staff should be responsible for the frequent moderation of the site. This will normally be the relevant Head of Department.
The social media site must only be used for educational purposes strictly related to the topic(s) being covered.
Any breech of this or unacceptable behaviour may result in the user being denied any further access to the site. The user will be subject to any appropriate disciplinary procedures in line with the school's disciplinary policy and the *e-Safety, ICT Acceptable Use and Digital Media Policy*.

Approval must be sought from the parents/guardians of any pupils who may be using the site before access is granted.

12 BRING YOUR OWN DEVICE (BYOD)

12.1 The use in school of devices owned personally by staff and pupils is subject to the same regulations/rules as if they were provided by the school. School policy on appropriate use of personal devises follows Department of Education guidance.

Please note: Some devices may not be suitable for use on the school network. The school can not guarantee connectivity or the quality of the wifi connection with personal devices**.**

The user/owner of a device being connected to the school network should adhere to the following conditions:

1. The device must be used in accordance with the e-Safety, ICT Acceptable Use and Digital Media Policy.
2. Any inappropriate content stored on the device in breach of the e-Safety, ICT Acceptable Use and Digital Media Policy must be removed before it is brought into the school premises.

3. An up-to-date anti-virus/internet security product must be installed on the portable device or external storage device.
4. As the school's insurance does not cover personal devices used in school, appropriate insurance measures should be in place to cover the device for this application.
5. As devices may have a tracking facility, it would be advisable to have it enabled when being used in school to assist in the relocation of the device if lost or stolen.
6. The school accepts no responsibility for any privately owned devices brought into school. Pupils/staff are solely responsible for the safety (including content) of devices on their way to school, during school and on the return from school. It is the responsibility of pupils/staff to look after their own personal devices and therefore they should keep the devices with them at all times. The school is in no way responsible for personal devices that are broken, lost or stolen while at school or during school activities.
7. Use of the internet, cloud and email is monitored and any use that is deemed to be inappropriate will be reported to the Principal. The Principal can request internet, cloud and email usage log for all users at anytime.
8. Devices may be checked at any time for inappropriate use.
9. If a student or member of staff finds inappropriate and/or illegal materials available on their device, the Principal should be informed immediately, giving details of their name, inappropriate material, time and date of incident.
10. There should be no use of camera facilities (if available on the device) to take images/ video of pupils or staff without permission.
11. Users who wish to connect their personal equipment to the school wireless network should have no expectations of hardware or software support from the school.
12. Devices should be named ideally with a UV pen in accordance with advice from the police.
13. Pupils and staff will be responsible for the security and protection of their passwords and if a device is left unattended the user should have either logged off or locked the device to prevent anyone using it in their absence.
14. All use of the Internet is governed by a legal agreement with our Internet Service Provider (ISP).
15. If a user suspects that their device has been affected by a virus or other malware, it should be removed from the school network and fixed before using it on the school network again.
16. Personal devices should not be connected to the school's peripherals, eg. printers.
17. Devices must be in silent mode while in school, unless otherwise allowed by a teacher.
18. Printing from personal devices may not be possible (Pupils are not permitted to bring their own personal printing devices).
19. Pupil owned personal devices should be charged before school and should run on battery power while at school (Devices are not permitted to be charged in school).
20. Portable devices/electrical items owned by staff members or pupils are not to be brought into the school unless they have a current Test Certificate (i.e. within the last 12 months). In all instances, the school is to be made aware of the intention to use 'private' electrical equipment in the School.
21. The school is in no way responsible for the maintenance of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).
22. Filtering may not block all inappropriate content.
23. Internet access can be removed for individuals and appropriate sanctions applied.
24. Pupils and staff should be conscious of personal safety when carrying devices to/from and around school
25. Pupils and staff should be conscious of personal safety when communicating on-line, and therefore must not share unnecessary personal information about themselves or others.

26. The school reserves the right to withdraw permission, at any time, to allow any individual to use personal devices in school.

We hope that following these instructions will help to make the use of ICT a positive experience for both our pupils and staff.

REVIEW

This policy will be reviewed and updated as required. The School will ensure a clear understanding of current online safety provision by carrying out an audit of current provision on an annual basis. This will help inform safeguarding and child protection and other relevant school policies.

APPENDIX 1: Additional Advice for Parents with Internet access at Home

1. The device with Internet access should be situated in a location where parents can monitor access to the Internet. Devices should be fitted with suitable anti-virus, anti-spyware and filtering software.

2. Parents should agree with their children suitable days/times/durations for accessing the internet.

3. Parents should discuss with their children the school rules for using the internet, cloud and digital media and implement these at home. Parents and children should decide together when, how long, and what comprises appropriate use.

4. Parents should get to know the sites their children visit, software/apps they use and talk to them about what they are learning.

5. Parents should consider using appropriate internet filtering software for blocking access to inappropriate material. Further information is available below.

6. It is not recommended that any child under 16 should be given unmonitored access to social media 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 or by C2k, they should immediately inform the school.

9. Please note for your own information that many social networking sites have a minimum age restriction. In the case of Facebook, for example, the recommended age for use of this site is 13 years of age.

Further free advice for parents is available from the following sources:

http://www.thinkuknow.co.uk/ - a website designed to inform children of the potential hazards involved with online chatrooms.

http://www.parentsonline.gov.uk/ - promotes home school links by helping parents understand the role of Information Communications Technology (ICT) in learning.

www.kidsmart.org.uk

http://www.wiseuptothenet.co.uk/ - The Home Office guide to Internet safety with downloadable leaflets for parents

http://www.getnetwise.org/ - information about filtering programs for home use

Protecting Your Home Computer
To protect you home computer, parents are advised to ensure the following items of software are installed on their home computers:

- Anti-Virus / Internet Security, Filtering and Anti-Spyware Software.

APPENDIX 2: Letter to Parents/Guardians

Dear Parent (s) /Guardian (s),

Internet, Cloud & Digital Media/Images Permission Form

Please note the e-Safety, ICT Acceptable Use and Digital Media Policy can be viewed on the School Website

As part of the school's Digital strategy, we offer pupils access to a filtered Internet service. Before being allowed to use the Internet, all pupils must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter.

Access to the internet and cloud will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with other users throughout the world. Families should be warned that some material accessible via the internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for internet/cloud use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the internet/cloud, in the form of information resources and opportunities for collaboration, exceed any disadvantages. We have put in place a filtered internet, cloud and e-mail service to minimise the dangers of pupils gaining access to unsuitable materials. In addition a clear set of rules and procedures for pupil use of the internet, cloud and digital media has been implemented. Ultimately, however, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

During class, teachers will guide pupils towards appropriate materials. Clear rules and procedures are in place for proper use of the internet, cloud and digital media. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media. Appropriate home use of the internet, internet, cloud and digital media by children can be educationally beneficial and can make a useful contribution to home and school work. It should, however, be supervised, and parents should be aware that they are responsible for their children's usage at home.

An increasing number of mobile phones and other portable devices have the capability to access the internet/cloud. It is possible to access most of the internet in much the same way you can at home or at work, and in the same way, you should endeavour to protect yourself and your child online.

Whilst we endeavour to continue to educate in this challenging area, pupils are only permitted to access online materials using internet connections provided and filtered by, or on behalf of, the school. We appreciate your ongoing support as we work together to ensure the safety of your child and those in our wider school community.

The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with our audiences in new and exciting ways. However, we would ask for your cooperation in relation to our *e-Safety, ICT Acceptable Use and Digital Media Policy.*

Please note for your own information that many social networking sites have a minimum age restriction. In the case of Facebook, for example, the recommended age for use of this site is 13 years of age.

In addition to the enclosed guidance documents, free advice for parents is available from the following sources:

http://www.thinkuknow.co.uk/ - a website designed to inform children of the potential hazards involved with online chatrooms.

http://www.parentsonline.gov.uk/ - promotes home school links by helping parents understand the role of Information Communications Technology (ICT) in learning.

www.kidsmart.org.uk

http://www.wiseuptothenet.co.uk/ - The Home Office guide to Internet safety with downloadable leaflets for parents

http://www.getnetwise.org/ - information about filtering programs for home use

We would be grateful if you could read the enclosed guidance documents and then complete the permission form which follows.

Yours sincerely

_____
Dr F Vasey
Principal

Internet, Cloud & Digital Media/Images Permission Form

Please complete and return this form to Reception **to enable internet / cloud access to be provided for your child**

Name of Pupil: _____

Form class: _____

Pupil

As a school user of the internet and cloud, I agree to comply with the School's *e-Safety*, *ICT Acceptable Use and Digital Media Policy*

Pupil Signature: _____ Date: _____

Parent

As the parent or legal guardian of the pupil signing above, I **grant permission** for my son/daughter to use electronic mail and the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the internet may be objectionable* and I accept responsibility for setting standards for my daughter / son to follow when selecting, sharing and exploring computer information and media.

I have read and understood the ***e-Safety, Acceptable Use of ICT and Digital Media Policy*** and give my son/daughter approval to use any personal ICT device which they may bring to 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 below**.

I understand that my son/daughter must comply with the School's *e-Safety*, *ICT Acceptable Use and Digital Media Policy*

*** The School endeavours to take all practical precautions, based on best practice guidance, to prevent access, whether purposeful or accidental, to objectionable or inappropriate material. These measures include filtering of known inappropriate websites, chatroom services etc. However, it is not possible to predict every possible avenue of access, although we act continually to improve the efficiency of our systems.**

****The school accepts no liability in respect of any loss/damage to personal ICT devices while at school or during school activities. The decision to bring a personal ICT device into school rests with the student 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 students to bring personal ICT devices into school, that the parent/guardian countersigning the permission slip accepts this disclaimer.**

This contract will remain in force throughout my son's/daughter's time at school and may be revised to take account of technological advancements in the interests of pupil and staff safety.

Parent Signature: _____ Date: _____

Digital Media/Images

I **grant permission** for still/moving images of my son or daughter to be used for display purposes and publicity in and outside school, in school publications, on the school digital signage and website in accordance with the school's *e-Safety*, *ICT Acceptable Use and Digital Media Policy.*

Parent Signature: _____ Date: _____

The information on this form is covered by the provisions of GDPR. Your signature on the form is deemed to be an authorisation by you to allow the School to process and retain the information for the purpose(s) stated.

APPENDIX 3: Internet Filtering within School

1. Access to the internet using the C2k System
The C2k service provides the school with the necessary hardware, software and connectivity to enable access to the internet and cloud. Access is controlled, by C2k, through a filtering mechanism. A filtering service, no matter how thorough, can never be completely effective, and it is essential that all staff and pupils have a clear understanding of the acceptable use policy, and that adequate supervision is maintained.

2. Non-C2k Networks
Non-C2k networks operate under the same rules of acceptable use as those for C2k networks. Non-C2k internet access must be protected by appropriate internet security and firewall software. Pupils must only be permitted access to non C2K networks/wifi through a suitable school approved filtered system with adequate supervision maintained.
Any non-C2k provided software, application or device to be used in school must have a risk assessment carried out before it is used. Any necessary protective procedures or actions must be in place and communicated to all staff and pupils affected.

General Points
Despite the filtering process, it is possible for unsuitable websites to become available, sometimes for short periods after they are launched. If at any time school pupils find themselves able to access, from within the school, internet sites which they think should be blocked, they should advise their teacher immediately. Likewise, staff should immediately advise the member of the Senior Leadership Team in charge of Digital Strategy (or, in his/her absence, another member of the Senior Leadership Team) giving details of the **site address and the time and date of access**.

To resolve the situation and enable the school to maintain an effective filtering mechanism, the member of the Senior Leadership Team in charge of Digital Strategy should contact the ICT Technician/Network Manager with details of the site(s)**.**

Any staff wishing to access sites that are not permissible using the agreed thresholds, should submit a request in writing to the member of the Senior Leadership Team in charge of Digital Strategy, using the 'Request for Access and Risk Assessment to Blocked Website' form, for wider consideration. After which, if the site meets with the approval of the Principal, the details of the site will be passed to the ICT Technician/Network Manager to enable authorisation. Access will not be granted until such time as approval has been given.

Request for Access to and Risk Assessment of Blocked Media or Emerging Technology

Name:
Website address (if applicable):

Access request for: Teacher ☐ Pupils ☐

Pupils - please state individual names and/or class & year group:

Content of media/Purpose of Educational Technology
(Please provide a brief summary and indicate the reasons why our filtering system has restricted access or the technology may fall outside the restrictions of our existing policy provisions. This information may be available from the ICT Technician)

Educational value of the media/technology
(i.e. rationale for use)

As the teacher requesting access to this media/technology, I understand that:

- The media/technology requested may contain inappropriate material that exceeds the thresholds of our school filtering solution.
- For media/technology made available to staff only:
  - it is especially important to ensure that a computer on which the member of staff has logged on should not be left unattended
  - particular care should be taken while projecting the media on a whiteboard, as inappropriate material may be displayed.

Teacher's Signature: _____

Authorised by: _____
(SLT i/c of Digital Strategy)

Date: _____

REQUESTS FOR ACCESS TO BLOCKED MEDIA ON THE SCHOOL NETWORK SHOULD BE MADE TO THE MEMBER OF SLT RESPONSIBLE FOR ICT.

APPENDIX 4: Website & Digital Signage Guidelines

Purpose of the School Website & Digital Signage

The school values the contributions that a school website and digital signage system can make towards:

Providing information for:

- pupils
- parents of existing students
- parents of prospective students
- Staff
- wider community outside the school
- School Alumni

Raising standards in:

- Teaching and learning
- School – Parent Communication

Promote:

- The values, aims and objectives of the school
- The achievements of the students

Website Structure

The School Website address is www.grosvenorgrammarschool.org.uk

The safety of the students and other users who appear or are referred to on the published site is of paramount importance.

1. Access and Approval

- The ultimate responsibility for the contents of the website rests with the Principal through her appointed Senior Leadership Team member with specific responsibility for Public Relations and Communications.
- The Vice Principal i/c of Publications and Communications has full access to the School published website with and of publishing rights in consultation with the Principal.
- Content for publication across the school digital signage shall be reviewed and uploaded by the Vice Principal i/c of Publications and Communications in accordance with the standards used for external publication on the school website.

2. Images and Names

- Group images will be used wherever possible.
- No personal details, addresses or e-mail addresses will be published for adults or students.

3. Content

- Links to external websites will be checked before inclusion on the School website. The sites will be checked for the suitability of their content for their intended audience. They will be provided solely for information and not to endorse or promote other sites.
- Whilst the school makes every effort to review the content of any external links, the variable nature of internet content should be appreciated. Therefore, the school does not accept responsibility for the appropriateness of the content on third party sites.
- All content will be reviewed before inclusion.

4. Privacy

- Adults have the right to refuse permission to publish their image on the website.
- Parents/guardians have the right to refuse permission for their child's work and/or image to be published on the website and can be done so on the return of the Internet & Digital Media/Images Permission Form.

5. Monitoring

- Staff who submit information to the Member of SLT i/c of Publications and Marketing so that it can be uploaded to the website will check material before it is uploaded. They should ensure that it is suitable

and complies with the record of parents/guardians who have not given permission for their child's image to be used and with copyright restrictions (as far as is reasonably possible). Any persons named on a web page can ask for their details to be removed.
- The web pages will be regularly reviewed for accuracy and will be updated as required.

6. Maintenance and Editing
- School website structure will be maintained by the Vice Principal i/c of PR and Communications.
- The final editing rights remain with the Principal or her appointed Deputy.
- At least two people in the school shall have the knowledge of maintaining and editing the website and digital signage and they must pass on their knowledge to a successor at the end of a term of office.

7. Legal Issues and Copyright.
- Every effort will be made to ensure that the site's content is up to date and accurate. However, the content is published in good faith as a general guide but must not be taken as a legal statement unless specifically specified.
- Every effort will be made to ensure that copyright material is not used illegally on the site.
- Copyright on all original images used within the website is held by the school. Images must not be used without specific written permission by the school.

Appendix 5: SCHOOL EQUIPMENT LOAN AGREEMENT

Staff must comply with the following conditions

- All school resources (including computers, laptops, tablet devices) and their associated accessories are provided for educational use; they must not be used for any other purposes. Only portable resources (such as laptops, ipads, tablet devices) may be removed from school, to facilitate preparation for teaching and learning, in accordance with the details set out below. Additionally, the resources may not be passed on to any third party.
- All electronic devices are expensive and therefore must be looked after appropriately and must be kept in a safe place, including those taken off site.
- All staff are reminded that the school does not insure property for out of school use. As such it is the responsibility of individual staff taking electronic devices off-site to provide adequate insurance cover for the full-replacement cost of the electronic device including software and accessories. This amount can be advised by the Vice Principal i/c of LMS.
- No equipment or resources can be taken off-site without the prior permission of the person in charge of those resources.
- Users must not give unauthorised access to any confidential material relating to the school or its pupils.
- It is the duty of the user to ensure that all passwords and access codes are kept strictly confidential.

Staff wishing to take any electronic device off-site must have signed below to indicate their agreement of these conditions, a copy of which will be retained in his / her staff file and by the Senior Leadership Team member responsible for facilities.

☐ I have read and understood the school's *e-Safety, ICT Acceptable Use and Digital Media Policy* and agree to abide by this policy.

☐ I accept responsibility for the full replacement value of all equipment which I take off-site.

☐ I accept that before taking any equipment out of School I must have the permission of the teacher in charge of those resources.

NAME: _____ (Please Print)

Signed: _____

Date: _____