ICT & E-SAFETY POLICY

Introduction

ICT (Information and Communication Technologies) plays an important role in the everyday lives of young people and adults and, when used appropriately, is a valuable resource for learning and teaching. Our aim is to use technology to deliver a rich learning experience, to support the pursuit of academic excellence and to develop skills that will support life-long learning and employment.

ICT covers a wide range of resources including web-based and mobile learning. It is important to recognise the constant and fast paced evolution of ICT and understand that our ICT policies cannot specifically refer to every ICT service available.

We are aware that much ICT, particularly web-based resources, is not consistently policed. Parmiter's is committed to investing in technologies and training to keep our students safe whilst using technologies provided by the school. However, we are aware that our students use a vast array of personal technologies and access web-based resources outside of school time. We fully understand our responsibility to educate our students on e-Safety issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the classroom. All users need to be aware of the range of risks associated with the use of these technologies.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet and include:

- Technologies provided by the school (such as PCs, laptops, mobile devices, whiteboards, digital cameras, etc).
- Technologies owned by students and staff that are brought on to school premises (such as laptops, wearable technology, mobile phones, and other mobile devices).

ICT in Teaching & Learning: Bring Your Own Devices (BYOD) & WiFi

There is **no requirement for Parmiter's students to bring their own laptop device into school,** but they may if they wish and believe it would be beneficial to their learning. Students will **not** be at a disadvantage in class if they do not have their own device.

Students may use their device to support their independent study and/or in lessons where the teacher has given permission. **The use of any device is at the discretion of the teacher and all students must use the device as directed. Students will not be at a disadvantage if they cannot bring their own device into school.**

Information for Students:

- Prior to bringing a personal device into school for the first time, students and their parents are expected to read this policy so they understand the responsibilities and expectations for use of personal devices at Parmiter's. By bringing a device into school students and parents are accepting the terms of this policy.
- Students must use their device in accordance with the school's Acceptable Use Agreement (see Appendix).
- Students must follow teachers' directions as to appropriate use of their devices in class and MUST NOT get out the device unless instructed by a teacher. Using a device without permission will result in the device being confiscated (refer to confiscation procedures in school behaviour policy)
- Students must connect their device to the designated wireless data network supplied by Parmiter's. Students must not connect to any other network, wired, wireless or cellular. Students must not bridge the Parmiter's designated network to any other network.
- The device should ONLY be used for educational purposes. All communication through internet and online communication services must be related to learning.
- Devices must be brought to school fully charged. The school does not provide facilities to charge devices.
- Each student is solely responsible for the care of and their conduct on their device whilst:
    - at school or at other school activities
    - travelling to and from school or to and from other school activities.
- Students are encouraged to clearly label their device; devices must be covered by a home insurance policy.

Information for Teachers:

- Teachers should encourage and facilitate the use of students' devices in their classes where they deem it appropriate or where the use of a word processor is the student's normal way of working. **Use of students' own devices in class is, however, at the sole discretion of the teacher.**
- Teachers should be aware that not all students own such devices and provision should be made such that all students can access the activities in the lesson.
- Teachers should follow standard discipline procedures if a student is using a device without permission.
- If a student is using a device for medical reasons, Curriculum Support or Matron will ensure teachers are made aware.

Information about Parmiter's School role:

The School:

- Will provide a wireless network with filtered and monitored internet connection to which students may connect their device.

- Does not provide **ANY** support to assist students with establishing network connectivity with the device.
- **Accepts no responsibility or liability for loss or damage to, or for maintenance or repair of, a student's device.**
- **Does not provide any insurance cover for personal devices brought to school.**

ICT in Teaching & Learning: Google

As part of our commitment to embrace technology, make the most of its associated educational benefits and work efficiently, Parmiter's School uses Google Apps for Education. To comply with GDPR and Google's Terms of Service (https://tinyurl.com/y72yyanv) and Privacy Statement (https://tinyurl.com/y96a7je2) on entry to the school all parents/carers are asked to provide consent for students to access the Google Apps for Education service.

What's included in Google Apps?

- Gmail: please note that emails sent from, and received by, students are monitored and recorded by the school as per the Acceptable Use Agreement.
- Google Calendar: this enables us to create and share calendars and offers an efficient way of organising and communicating events across the school.
- Google Docs: this allows students and staff to create and share documents, spreadsheets, presentations, drawings and forms. This also allows students to work collaboratively on projects in real time. Students will be able to access documents in school and at home, providing a seamless way of working.
- In addition to the above, there are a number of other third-party applications and services we will potentially use within Google Apps for Education to enhance teaching & learning, such use of third-party applications/services will be subject to stringent vetting as to suitability for student use.

What are the benefits of Google Apps and what's included?

- Students can access Google Apps at anytime, anywhere. It is designed to work in any browser (Google Chrome, IE, Firefox etc.) and on any web-enabled computer or tablet. This provides access to email, calendars and documents from school or at home.
- Online storage means that no flash drives (memory sticks etc.) are required.
- Students can work collaboratively. During collaborative work, teachers can monitor the progress of each student and provide instant feedback visible to the group or to the individual.
- Online portfolios of work can be developed by students.

Within Parmiter's School Google Apps service:

- There will be no advertisements and all work is kept in secure storage.

- All email communication and comments within collaborative work are monitored by Parmiter's School.
- Work uploaded to Google Drive remains the property of the creator and Parmiter's School; it is not copied or kept by Google if it is removed by the creator.

Student Access

Students will be shown how to use Google Apps for Education. They will be provided with unique usernames and passwords and we expect them to follow school policies for appropriate use of ICT when using Google Apps. The service is an extension of the school's own network. The school has the right and ability to monitor user accounts for policy and e-safety purposes as well as having the ability to remove access to some, or all, Google Apps.

e-Safety

The school's primary aim is for each Parmiterian to be self-assured and caring, an active and well-rounded citizen with integrity, who respects others and contributes to society. Our school ethos and aims and our Behaviour Policy also reiterate our commitment to:

- creating a healthy, happy, disciplined and supportive environment which promotes an independent work ethic and a love of learning;
- engendering respect for individuality and difference so that all will feel secure and equally valued;
- nurturing a sense of social responsibility and spiritual and personal development;
- fostering integrity, confidence, resilience, creativity, good manners and sensitivity to the needs of others.

Roles & responsibilities

e-Safety is an important aspect of school life. The named e-Safety coordinator in this school is Mrs Stevens, Deputy Headteacher. It is the role of the e-Safety coordinator, with the support of the Director of ICT, to keep abreast of current issues and guidance.

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection & safeguarding, health and safety, home–school agreements, behaviour and anti-bullying.

e-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the students on a regular and meaningful basis. e-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety. With this purpose:

- The school has a framework for teaching internet skills and e-Safety in the curriculum.
- Educating students about the online risks that they may encounter outside school is done

through the e-Safety curriculum and more informally when opportunities arise.

- Students are aware of the relevant legislation when using the Internet, such as data protection and intellectual property.
- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher or trusted staff member, OKtoTell email or an organisation such as Cybermentors, Childline or CEOP report abuse button.

Students are taught to critically evaluate materials and learn good online searching skills through cross curricular teaching.

e-Safety Skills Development for Staff

- Our staff receive regular information and training on e-Safety and how they can promote the 'Stay Safe' online messages in the form of briefing notices, INSET and updated policies.
- New staff receive information on the school's acceptable use agreement and are required to sign this as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the School eSafety Messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-Safety policy is introduced to the students at the start of each school year.
- e-Safety posters are prominently displayed.
- The key e-Safety advice is promoted widely through school displays, newsletters, class activities etc.

Social Media & Communications

We acknowledge that all members of the Parmiter's family may access social media sites and recognise the professional and personal benefits of these technologies. However, we are aware of the need to ensure the safety of our students and staff at all times as well as preserving our school's reputation. This policy sets out the principles that Parmiter's staff, governors and students are expected to follow when using social media and real-time communication applications.

Definition and Role of Social Media

When referring to social media, we are referring to any tool, application, website or mobile technology that allows people to create, share or exchange information, ideas, and pictures/videos online. This includes e-mail.

Parmiter's acknowledges the role of social media in increasing opportunities to learn and communicate. The school has a number of 'official' social media accounts that allow us to use real-time communication to keep the school community informed of news and events. We also acknowledge the increasing use of personal social media by all members of the Parmiter's family.

Parmiter's Social Media Principles of Acceptable Use

Matters posted to social media sites have the potential for considerable breadth of dissemination and individuals choosing to post on such sites should be mindful of this.

Nothing should be posted onto a social media site that could be considered as victimising and or humiliating to someone on account of their race, gender, religion, nationality, culture, disability or sexual orientation. Users must refrain from posting anything that is disrespectful to individuals, obscene, sexually explicit, inappropriate, inflammatory or defamatory towards the school or any person.

Parmiter's therefore expects that the online contributions of students, staff and governors are polite and non-offensive.

Parmiter's Social Media Acceptable Use Agreement Regulations

When posting material onto social media sites students, staff and governors should be conscious at all times of the need to keep their school/professional life and personal life separate. All information posted on a Parmiter's official social media site or any 'open' social media site will be publicly available and therefore publicly accessible on the Internet. All members of the school community using any social media site should be aware that their name may appear next to any information posted and could be linked and traced accordingly.

As such, students, staff and governors must not:

- Put themselves into a position where anything posted might bring Parmiter's into disrepute.
- Represent their own personal views as those of Parmiter's on any social media sites.
- Post any narrative that could be considered either implicitly or explicitly as insulting, threatening, harassing, illegal, abusive, obscene, defamatory, slanderous, or hostile towards any individual or towards the school.
- Discuss or post personal or confidential information or images relating to students, any member of staff or any other member of the Parmiter's family.
- Allow any other individual or entity to use their identification for posting or viewing comments.
- Post comments under multiple names or using another person's name.
- Impersonate any individual or group when using social media.

Students, staff and governors must adhere to the following guidelines:

- If any member of staff is aware of any inappropriate communications involving any student in any social media, these should be reported as an e-Safety concern.
- Members of the whole school community are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
- Staff should not use personal email accounts or mobile phones to make contact with students, nor should any such contact be accepted except in exceptional circumstances. Any such contact should be reported to the e-safety officer.

In addition, staff and governors must not:

- Have current students as 'friends' on any personal social media account. We also strongly discourage staff and governors from having former students as friends.
- Have any communication received from students on any personal social media site. Any such communication must be reported to the designated safeguarding lead (DSL) or one of the Deputy DSLs.

All users of social media and communications should be aware of Section 127 of the Communications Act 2003 detailing offences relating to the 'Improper use of public electronic communications network':

1. A person is guilty of an offence if he—
   a) sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or
   b) causes any such message or matter to be so sent.

2. A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he—
   a) sends by means of a public electronic communications network, a message that he/she knows to be false,
   b) causes such a message to be sent; or
   c) persistently makes use of a public electronic communications network.

(Communications Act 2003. [ONLINE] Available at: http://www.legislation.gov.uk/ukpga/2003/21/section/127/2015-04-13. Accessed 15/11/19)

Students will not be able to access social media with age limits on the school network and are discouraged from doing so through private networks before they turn 13.

All material posted onto a Parmiter's official social media site becomes the property of Parmiter's. Individuals posting comments or materials onto Parmiter's official media sites lose all subsequent rights to this material which may be disseminated by the school in whatever way it decides. Parmiter's reserves the right to delete comments from Parmiter's official social media sites and will take all reasonable steps to have offensive material removed from other websites on behalf of their students and staff or in order to preserve the reputation of the school.

Monitoring and reporting

Breaches

A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure/Behaviour Policy or, where appropriate, the HCC Disciplinary Procedure or Probationary Service Policy.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

All e-Safety concerns or issues must be reported to Mrs Stevens (e-Safety coordinator).

All security breaches, lost/stolen equipment or data (including remote access), virus notifications, unsolicited emails, misuse or unauthorised use or suspected misuse of ICT and all other policy non-compliance must be reported to Mr Baker (Director of ICT).

All such events will be logged.

Monitoring

All internet activity and email is logged by the school's internet provider. These logs may be monitored by authorised HCC staff. Our school internet filtering system also flags up and reports students who have accessed websites deemed to be inappropriate or a safeguarding concern, these reports are sent regularly to our eSafety coordinator.

Appendix 1: ICT Acceptable Use Agreement: Students

ICT (including data) and the related technologies such as email, the internet and mobile devices are a part of our daily working life in school. This policy is designed to ensure that all students are aware of their responsibilities when using any form of ICT.

- I will only use ICT systems in school for educational purposes.
- I will only log on to the school network, other systems and resources with my own username and password and will not use anyone else's account.
- I will follow the school's ICT security system and not reveal my passwords to anyone and will change them regularly.
- I will only save files on the network/Google Drive that are related to school work. I will not use filenames that could be considered offensive.
- I will not attempt to make any unauthorised alterations to the technical environment provided by the school and I will not download, install, modify or run any software on school technologies that were not made available to me by the school.
- I will not attempt to bypass the internet filtering system.
- I will not play games on school ICT systems without a member of staff's permission.
- I will only use my school email address for school business. I will check my email regularly and carry out routine 'housekeeping' of my email messages.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible and follows the guidelines in all relevant policies.
- I will respect the privacy and ownership of others' work online at all times.
- I will be responsible for my behaviour when using the internet and online services. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone I have contacted online.
- I will not take or publish images/video/audio recordings or other identifying media of students and/or staff without the express permission of a member of staff. Images/video/audio recordings or other identifying media will only be stored and used for school purposes in line with school policy and will not be taken outside the school network or used outside of official school platforms without the permission of the Headmaster.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others upset or distress or bring the school or an individual into disrepute.
- 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 and parents.
- I will respect ICT equipment and will not deface or damage it.
- I will log off when leaving a computer.
- 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 parent/ carer may be contacted.

Appendix 2: ICT Acceptable Use Agreement: Staff and Governors

ICT (including data) and the related technologies such as email, the internet and mobile devices are a part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are required to sign this policy and adhere at all times to its contents. Any governor or visitor accessing using the ICT facilities or network must be made aware of this policy. Any concerns or queries should be discussed with Mr Baker (Director of ICT) or Mrs Stevens (e-Safety coordinator).

- I will only use the school's ICT systems for professional purposes or for uses deemed 'reasonable' by the Headmaster or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities. Users are required to use a 'strong' password and change it regularly as instructed by Network Resources. Any suspected breaches of security must be reported to Mr Baker.
- I will ensure that others do not have access to my account when I am not at my computer (this means locking or logging off if you are away from your computer.) I will take particular care when accessing the school systems remotely. It is advised that staff do not use the remote access from a public place; if it is necessary to do so, staff must take particular care to ensure systems and data are kept secure.
- I will ensure that all electronic communications with students, staff and parents are compatible with my professional role.
- I will only use the approved, secure email system for any school business and communication with students, their parents/carers and staff.
- I will not give out my own personal details, such as mobile phone number or personal email address, to students or parents/carers.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or downloaded when authorised in advance by the Headmaster or Governing Body. Personal or sensitive data taken off site in an electronic format must be encrypted. Staff leading a trip are expected to take relevant student information with them but this must be kept secure at all times.
- I will not install any hardware or software without permission of Network Resources.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images/video/audio recordings or other identifying media of students and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer and staff member. Images/video/audio recordings or other identifying media will not be taken outside the school network or used outside of official school platforms without the permission of the parent/carer, member of staff and Headmaster.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sound or text that could upset or offend any member of the school community.
- I understand that all my use of the internet/email and other related technologies can be monitored and logged and can be made available, on request, to my SLT Line Manager or Headmaster.
- I will respect copyright and intellectual property rights. If I am unsure about this, I will seek advice from a member of the LRC staff.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will support and promote the school's ICT & e-Safety and Data Protection policies and help students to be safe and responsible in their use of ICT and related technologies.
- I have read and will follow the guidance in the Protocol for Communication between Parents and Staff at Parmiter's and the Protocol for Staff Communication at Pamiter's.

Name:.....Date:.....

Signature: .....

Please return this form to Network Resources

Appendix 3: ICT Acceptable Use Agreement: Visitors

Visitors may be issued with a guest login for the Parmiter's network. Visitors can also request a wifi login from Reception so they can use their own devices during their visit. This policy is designed to ensure that all visitors are aware of their responsibilities when using any form of ICT. **By logging on to our network or using the wifi login, you are agreeing to the following:**

- I will only use the school's ICT systems for professional purposes or for uses deemed 'reasonable' by the school. If I am unsure, I will ask Network Resources.
- I will not share visitor login details with anyone, other than Network Resources.
- I will ensure that all electronic communications with students, staff and parents of Parmiter's are compatible with my professional role.
- I will ensure that personal data (such as data held on SIMS) shared with me is kept secure and is used appropriately. No personal data will be taken off the school premises.
- I will not install any hardware or software without permission of Network Resources.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images/video/audio recordings or other identifying media of students and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer and staff member. Images/video/audio recordings or other identifying media will not be taken outside the school network or used outside of official school platforms without the permission of the parent/carer, member of staff and Headmaster.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sound or text that could upset or offend any member of the school community.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Headmaster.
- I will respect copyright and intellectual property rights. If I am unsure about this, I will seek advice from a member of the LRC staff.
- I will support and promote the school's ICT & e-Safety and Data Protection policies and help students to be safe and responsible in their use of ICT and related technologies.

Network login details: **user name: .....password:.....**

Wifi login details: user name: .....password:.....