Parmiter's School

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

Last Reviewed: May 2025
Next Review Date: May 2026

ICT in Teaching & Learning

Individual Chromebook Scheme

All students in **Years 7 to 11** have access to their own personal Chromebook, a device which provides access to G Suite for Education. These devices are filtered and monitored in the same way as other school devices. All students in **Years 7 to 11** sign the Chromebook and E-Learning Code of Conduct (students complete this via Google Form but it is included as Appendix 1 for reference). Failure to follow this code of conduct will result in the partial or full loss of access to a Chromebook and connectivity to the school's Wifi / network services during the school day. Further disciplinary action may be taken in line with the school's behaviour policy. Where inappropriate activity is severe and may constitute a criminal offence, external agencies, including the police, may be contacted.

In addition, the E-Learning code of conduct, it is expected that:

- Chromebooks are brought into school every day as a standard piece of equipment.
- Chromebooks are fully charged at home. Chromebooks **cannot** be charged during a lesson.
- Chromebooks must only be used in lessons when directed by a teacher.
- Students must allow access to monitoring software when requested by a member of staff during the school day, or beyond the school day if the student is on the school site or on school trip/activity.
- Students take care of their Chromebook. If not in use or when walking around, the Chromebook must be in its **case and stored in an appropriate school bag**.
  - Bags with devices in must be kept with the student at all times or left securely in their lockers
  - When travelling to and from school students must keep their device out of sight (in their school bag).
- If the device is damaged or broken the following steps must be followed:
  - If the chromebook is covered by the School Scheme warranty the device should be brought to the Network Resources department (located in the Learning Resources centre) as soon as possible. The team will loan a temporary device to the student whilst theirs is being repaired.
  - Parents/carers of students who provide their own devices must arrange for repairs privately.
- All Chromebooks **must** be licenced before they can use the school networks. Parents/carers of students providing their own chromebook must purchase this licence from the school.

Bring Your Own Devices (BYOD)

Students in **Year 12 to 13** are expected to have their own device in school each day. Year 12 and 13 students are allowed to use any device that is most appropriate for their studies. This does not have to be a Chromebook - any laptop will suffice, however mobile phones will simply **not** fulfil the functionality expected.

Students in Years 12 & 13 must use their device in accordance with the school's Acceptable Use Agreement (see Appendix). In addition they are expected to adhere to the following:

- Prior to bringing a personal device into school for the first time, students and their parents/carers 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 follow teachers' directions as to appropriate use of their devices in class. 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.
- Student devices which are deemed to be a health & safety risk will not be allowed to be used in school

Information about Parmiter's School role for Individual Chromebooks and BYoD:
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 Year 7 to 11 students with establishing network connectivity with personal devices not purchased via the Freedom Tech/Edde portal or if they do not have an approved licence.
- **Accepts no responsibility or liability for loss or damage to, or for maintenance or repair of, a student's device unless insured with Freedom Tech**/Edde
- **Does not provide any insurance cover for personal devices, unless purchased through Freedom Tech**/Edde**.**

Information for Teachers for Individual Chromebooks and BYoD: :

- 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.**
- From September 2024 for safeguarding purposes when staff ask their students to use Chromebooks they must monitor their use via Classroom Cloud
- 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.
- Teachers should avoid planning lessons that rely on the use of stylus and/or touch screens as not all chromebooks are equipped with these.

For further information about the rationale for, and benefits of, one-to-one devices in teaching & learning, please refer to the school's Teaching & Learning policy.

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 any time, 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.

Artificial Intelligence (AI)

The use of generative AI within education is evolving, and we recognise this presents both opportunities and challenges for staff and students.

Generative AI for staff

We encourage staff to try generative AI tools and explore how they may be able to support teaching and learning. We also encourage staff to explore how generative AI can be used to reduce workload, both in delivering the curriculum and in non-student facing activities.

Staff should be aware of the limitations of generative AI tools and must use their professional judgement to check any content produced for appropriateness and accuracy. Whatever tools or resources are used to produce resources or documents, the quality and content remains the professional responsibility of the person who produced it.

Access to generative AI platforms is not restricted on staff devices. The use of AI is acceptable within the following parameters:

Staff must:

- only create accounts on AI platforms for work-related use using their school e-mail/link to Google
- acknowledge any use of AI in creating materials
- not provide the AI platform with any student details, their personal details, or details of colleagues
- not enter student work into any AI system where inputs are used to train the LLM
- not use AI to mark student work (although AI can be used to support assessment practice)
- not use AI to write complete student reports/gradesheets

Use of AI with students

If staff want students to have access to a generative AI platform as part of a learning activity, they should contact Network Resources in the first instance. Please be aware that all age restrictions will be adhered to by the school and the platform will only be made available to students for a limited time period. In line with policy, when students are using their Chromebook, staff must monitor this through ClassroomCloud; when using AI platforms staff must be especially vigilant.

Staff are encouraged to openly engage in discussion with students about the appropriate and transparent use of generative AI, highlighting the opportunities and the limitations of this technology.

Staff must reiterate that all work submitted by students for assessment must be their own work. If generative AI is used in producing the work, this must be acknowledged. Failure to acknowledge the use of AI is considered malpractice. If a student submits work that staff believe includes AI generated content, in the first instance this should be discussed with the student and the student given the opportunity to amend and resubmit the work. If on the second submission the work includes AI generated content that is not acknowledged, usual departmental procedures for non-completion of homework should be followed.

Live streamed lessons

Where a teacher offers a live streamed lesson, this will be done via the Google Meet functionality within Google Classroom. No other platforms will be used for live streamed lessons. All staff and students will use their school accounts when delivering / accessing a live streamed lesson.

Live streamed lessons are used to provide continuity of education during a partial or full closure of school. They also provide students with a level of familiarity and connection to school during their absence.

The audience for live streamed lessons are the students of Parmiter's school. Any student accessing a live streamed lesson must take reasonable steps to ensure other members of their household are not viewing or disrupting a live streamed lesson.

Students must recognise that joining a live streamed lesson cannot replicate the learning experience in a classroom. There may be some classroom activities that students joining virtually cannot actively participate in. A live streamed lesson may vary in length; teachers will use their professional judgement as to whether the student is required to remain on the live streamed lesson for the full lesson, or whether once they have received instruction regarding the work they complete the set tasks offline.

A teacher reserves the right to record a live streamed lesson and will inform all students joining the lesson. It is recommended that any one-to-one live streamed lessons, for example tutorials, are recorded; again the student will be informed the session is being recorded. Recordings will be deleted at the end of the course. Under **no** circumstances must a student record or take photos of a live streamed lesson. Any student doing so will be sanctioned in line with the school's Behaviour Policy.

Appendix 5 details the school's expectations with regard to student conduct, good practice and acceptable use when using Google Meets to join a live streamed lesson.

Where a live streamed lesson is offered we expect students to attend; non-attendance will be recorded. The school's Behaviour Policy, applies to students who are accessing learning through a live streamed lesson; there is no change to our expectations of student conduct or our rewards and sanctions procedures. The school reserves the right to turn off a student's microphone, remove a student from a live streamed lesson and/or deny student access to future live streamed lessons.

Staff must familiarise themselves with the school's guidance on staff good practice and acceptable use for live streamed lessons; this will be reviewed regularly and updated to reflect emerging best practice. This document is available in the Staff Handbook and on the school's internal Teaching & Learning website.

If staff are hosting an online meeting for parents/carers this must only take place on GoogleMeets using their school Gmail account.

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.

Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Content filtering is applied to Chromebooks and devices used by students in Years 7 to 13 at all times, on the school network. In addition, this filtering is applied at home for students in Years 7 to 11.

Only authorised network resources personnel and the Designated Safeguarding Lead (and Deputies) may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. In addition to this, teaching staff will be required to monitor student's online conduct when using ICT equipment during lessons.

Our online filtering and monitoring services are procured through Herts for Learning and are provided by RM Safetynet and all Chromebooks have the Classroom Cloud software added for monitoring purposes.

Roles & responsibilities

Academy Governance

The Academy Governance must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The Community Governors Committee will review the DfE filtering and monitoring standards, and discuss with the Headteacher and members of the Senior Leadership Team what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) and Deputies are set out in our Child Protection and Safeguarding Policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Network Resources Team to make sure the appropriate systems and processes are in place
- Working with the Headteacher, Network Resources Team and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's Child Protection and Safeguarding Policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school Behaviour Policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and Academy Governance
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

The Network Manager

The Network Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

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.

All staff

All staff are expected to have an awareness of online safety and be vigilant to the potential dangers students may face online. In order to keep our students safe staff will:

- Have an up to date knowledge of school policy and procedures, most notably this policy, the Child Protection & Safeguarding Policy and the ICT Acceptable Use Agreement.
- Monitor what's happening on students' screens whilst using online technology
- Address any device misuse immediately
- Report any safeguarding concerns to the Designated Safeguarding Lead (DSL) via CPOMS.

Staff are also required to inform the DSL and/or the Network Resources Team

- If they find that students can access unsuitable material
- If you become aware of a failure in the software or an abuse of the system
- If they think that there are unreasonable restrictions that affect teaching and learning
- If they are teaching topics that could create unusual activity on the filtering logs.

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, modelling 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 aware of the concept of their digital footprint, and the consequences of this for them now, and in the future.
- Students understand possible threats related to generative AI. This includes:
    - Unintentional harm caused as a result of biased or inaccurate responses from AI.
    - Intentional harm when AI is used to generate or manipulate data with the intention of misrepresenting an individual, group or situation.

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/Cyber Security 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: https://www.legislation.gov.uk/ukpga/2003/21/section/127. Accessed 7/05/2025)

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.

Incident 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 Mr Hughes (Designated Safeguarding Lead).

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 (Deputy Headteacher).

All such events will be logged.

Appendix 1: Parmiter’s School E-Learning and Chromebooks Code of Conduct

This code of conduct applies at all times when using any IT services provided by Parmiter’s School. It applies to any device (school owned or a personal device) that is connected to our WiFi network or Google Domain and applies both during school hours and outside of school hours.

Internet, e-mail and access to G Suite for Education will be provided for you to conduct research, communicate with others and access online learning resources and your personal online storage space on the understanding that you agree to follow this code. This code of conduct is not intended to be exhaustive. At all times you must use e-learning resources in an appropriate and responsible manner.

ICT Acceptable Use Agreement: Students (see Appendix 2)

All services provided by Parmiter’s School are subject to monitoring services which will automatically flag inappropriate content to the school’s dedicated safeguarding team. If the safeguarding team feels that content needs further investigation, your services can be accessed and your activity reviewed. All activity on your account is your responsibility as your area is password protected. Any inappropriate activity will be assumed to be yours.

Chromebooks

All students in school have access to their own personal Chromebook, a device which provides access to G Suite for Education. These devices are filtered and monitored in the same way as other school devices. In addition to following the E-Learning Code of Conduct, students who have access to their own personal Chromebooks must also adhere to the following guidelines.

- Chromebooks must be brought into school every day as a standard piece of equipment.
- Chromebooks must be fully charged at home. You cannot plug your Chromebook in to charge it during a lesson.
- Chromebooks must only be used in lessons when directed by a teacher.
- Years 7 to 11 must not bring unlicenced Chromebooks to use in school.
- Students must allow access to monitoring software when requested by a member of staff during the school day, or beyond the school day if the student is on the school site or on school trip/activity.
- Take care of the Chromebook. If not in use or walking around, it must be in its **case and stored in an appropriate school bag**.
    - Bags with devices in must be kept with the student at all times or left securely in their lockers.
    - Do not leave bags with devices in around the school site unattended.
    - When travelling to and from school you must keep your device out of sight (in your school bag).
- If the device is damaged or broken you must do the following:
    - Students with devices bought through the school scheme will bring the chromebook to Network resources for the repair to be processed. They will be issued with a loan device to use until their Chromebook is repaired.

Failure to follow the code of conduct

Failure to follow this code of conduct will result in the partial or full loss of access to a Chromebook and connectivity to the school's Wifi / network services during the school day. Further disciplinary action may be taken in line with the school's behaviour policy. Where inappropriate activity is severe and may constitute a criminal offence, external agencies, including the police, may be contacted.

Using the internet at home and outside of school

We encourage students to use the internet at home to enhance their learning. While using your school Chromebook at home you will receive the same internet filtering and monitoring as you get in school.

We request parents/carers work with us to ensure students' online activity is safe and positive. Whilst social media applications are blocked on Chromebooks, we recognise students have access to these on other devices. We therefore remind parents that most social media sites limit users to a minimum age. We treat all types of bullying, including cyberbullying very seriously. If cyberbullying is reported in school, we follow appropriate actions as deemed necessary.

Student name: .... Tutor group: .... Date: ....

My parents/carers and I have read and discussed the above and agree to follow it. We understand the consequences of not following the code of conduct.

Student signature: ....

Appendix 2: 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
- I will not install any hardware or software without the permission of Network Resources
- 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 are responsible, sensible and follow 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.
- If using generative AI, I will do this in an appropriate and responsible way. This means considering the limitations of any content generated by an AI platform. If I do use AI to help produce work I will, at a minimum, acknowledge this by stating the AI platform used, the link to the platform and the date the content was generated.
- I will not use AI tools and generative chatbots (such as ChatGPT or Google Gemini):
    - During assessments, including internal and external assessments, and coursework
    - To present AI-generated text or imagery as my own work
- I will not take, create (including generated by AI) 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 Headteacher.

- 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. This action is for safeguarding purposes and to reduce the risk of exposure to radicalisation / extremism as stated in the Prevent Statutory Guidance.
- 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 3: ICT Acceptable Use Agreement: Staff and Governors

ICT (including data) and 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 or Mr Hughes.

- I will only use the school's ICT systems for professional purposes or for uses deemed 'reasonable' by the Headteacher 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 Headteacher 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 only create accounts on AI platforms for work-related use using your school e-mail/link to Google.
- I will not provide the AI platform with any student details, my personal details, or details of colleagues.
- Any use of AI in creating materials must be acknowledged.
- I will not enter student work into any AI system where inputs are used to train the LLM.
- I will not use AI to mark student work (although AI can be used to support assessment practice).
- I will not use AI to write complete student reports/gradesheets.
- 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 Headteacher.
- 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 Headteacher.
- I will not click on links or attachments from suspect sources and if they are suspect I will forward the email immediately to Network resources.
- 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 Parmiter's.

Name:.. Date:..

Signature: ....

Please return this form to Network Resources

Appendix 4: 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 Headteacher.
- 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 Headteacher.
- 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:..................................

Appendix 5: Student conduct, good practice and acceptable use when attending a live streamed lesson

- Live streamed lessons will only be taught via the Google Meet functionality within Google Classroom. This can be found on the left hand side of the Stream page.
- If you are invited to a Google Meet taking place outside of the Google Classroom you must use your **school email address.**
- It is **your responsibility to join the live streamed lesson at the correct time** - you will not be reminded. **Be patient**, the teacher may need a few minutes to prepare the classroom before they admit you to the lesson.
- **You must NOT record or take photos of the session.** Please do not use your mobile phone during the session (except to access the Google Meet).

When joining the live lesson you must adhere to the following:

- **Dress:** students MUST be appropriately dressed for a video meeting, as if it were face-to-face.
- **Background:** Consider what is visible in the background that will be seen over the camera. Think about which room you are sitting in and check there is nothing inappropriate in the background.
- **Microphones and cameras:** Students MUST mute their microphones before joining so there is an orderly start to the session. If you need to get the attention of the teacher you should use the 'raise hand' function. Please be respectful of the fact the teacher has students in the class they may be talking to and they may not respond immediately. You MUST follow the instructions of your teacher regarding the use of your camera.
- **Use of earphones:** Students should, where possible, use earphones as it is helpful in cutting out sound echoes across the Google Meet, and make it easier for individuals to hear and avoid distractions from background noise.
- **Text Chat:** Students can only use this to ask, or respond to, a question. It must not be used for off-topic chat.
- **Respectful behaviour:** As always, it is expected that students are courteous and respectful to one another and the teacher. They should not interrupt when someone else is speaking etc. or talk to each other when the teacher or others are speaking.
- **Other people in the household:** When using Google Meets for lessons, students must avoid other people watching or being involved in the lesson.

Behaviour in the virtual classroom MUST mirror that in the physical classroom. The school Behaviour Policy applies, including rewards and sanctions. The school reserves the right to turn off your microphone, remove you from a live streamed lesson and/or deny you access to future live streamed lessons if behaviour causes any disruption to the lesson.

Helpful advice when you are on a live lesson:

- **Device position:** The device being used for the Google Meet should be placed on a stable surface and not held/carried.
- **Lighting:** To get the best picture from your camera try to have the main light source of the room behind the camera, not behind the subject.
- **Materials etc:** Gather together everything you need for the lesson before you start, so that it is not necessary to leave your computer/device during the call.
- **Connection quality:** The quality of call, especially with video, that is experienced by each user will be largely influenced by their connection speed and/or wifi coverage. It may be helpful to request that other people in the household do not use broadband-heavy applications during the Google Meet, such as streaming high quality video across the same connection.

Appendix 6: Staff conduct, good practice and acceptable use when using Google Meets (Live Lessons) - ICT & e-safety Policy Appendix

Live/streamed lessons may take place in the following scenarios:

- Full or partial school closure means all/some students are learning remotely;
- A student's specific circumstances means that the school has agreed that they may join your normal, timetabled lesson remotely;
- You are isolating or quarantining and so you teach / lead the lesson from home. In this situation, a cover teacher or member of SLT will be in the classroom with the students.

When teaching a live/streamed lesson you must adhere to the following guidance which **MUST be read in conjunction with the most UP TO DATE version of the safeguarding policy**

Guidance for staff regarding live/streamed sessions:

1. Where possible, we strongly recommend that you do such lessons from your classroom at school and not from home:
   a. If you have to run a live lesson from home, you must choose a neutral background in an appropriate room. No other members of your household should be in the room with you during the session.
   b. You must be dressed professionally, as you would be in school, with a school ID badge visible.
2. You must only use Google Classrooms and the Google Meets feature for these sessions.
3. It is best practice to use the Google Classroom Meets feature **on the Classroom stream** rather than inviting student(s) via email or calendar invite: see this **guide** (updated Jan 2023) on how to do this.
4. Staff and students must use their school Google accounts. If a student tries to join the session using a personal account, our recommendation (from experience) is that you let the student join the session, tell them they must leave the session, switch to their school account and rejoin the session.
5. The live stream lesson must be at a **time when the students would normally be in your lesson**
6. Sessions do **not** need to be the full hour; this will depend on the circumstances. Teachers are welcome to split the group and offer smaller sessions to aid better interaction for Q&A.
7. You **MUST** follow the guidelines and support given in previous training - See this link for training materials and ensure you understand the student guidance and are aware of the ICT & E-Safety policy.

Helpful advice when you are on a live lesson:

- **Students' microphones & cameras**: Students should join the session with their microphones on mute as this helps ensure an orderly start to the session. If you want a student to speak you must tell them to unmute their microphone. You can mute them, but not unmute them. Please encourage students to keep their cameras on as this allows you to engage with the students more easily; however, this is your choice.

- **Device position:** Where possible, the device being used for the Google Meet, both by the organiser and participants, should be placed on a stable surface and not held/carried.
- **Lighting:** To get the best picture from your webcam try to have the main light source of the room behind the camera, not behind the subject.
- **Connection quality:** The quality of call, especially with video, that is experienced by each user will be largely influenced by their connection speed and/or wifi coverage. It may be helpful to request that other people in the household do not use broadband-heavy applications during the video-conference, such as streaming high quality video across the same connection.