Maryfield College
Roll No. 60840K

Acceptable Use Policy

The aim of this Acceptable Use Policy is to ensure that students will benefit from learning opportunities offered by the school's digital resources in a safe and effective manner. The responsible use of internet and digital technologies, both online and offline, and access to digital devices is considered an integral part of teaching, learning and assessment. To ensure a safe environment for our students, we have outlined the expectations and rules regarding use of both hardware and software in the school, as well as the consequences if these expectations are not upheld by students.

This policy should be read in conjunction with the following:

Code of Behaviour
Digital Learning Plan
Bí Cineálta Policy
Child Protection and Safeguarding Policy

The school's Code of Behaviour further underpins and supports this policy. In a case where a student's behaviour breaches both the Code of Behaviour and AUP, both documents will be used to determine an appropriate action.

This Acceptable Use Policy applies to students who have access to and are users of the internet at Maryfield College .

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges, detention, and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Maryfield College will deal with incidents that take place outside the school that impact on the wellbeing of students or staff under this policy and associated the Code of Behaviour and Bí Cineálta Policy. In such cases Maryfield College will, where known, inform parents/guardians of incidents of inappropriate online behaviour that take place out of school and impose the appropriate sanctions.

This policy also applies to members of staff, volunteers, parents, guardians and others who access the internet in Maryfield College and who have an assigned Maryfield College Office 365 licensed account. Breaches of this policy by members of the school community other

than students will be dealt with under the agreed procedures between school management bodies and teaching unions.

This policy has been developed by the schools' Senior Leadership Team in collaboration and consultation with teachers, students, parents/carers, and representatives of the Board of Management.

It is envisaged that school and parent representatives will revise the AUP at least annually.

The school requests that all parents accept and sign the AUP by signing the declaration in the student journal. Before accepting and signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

When using the internet students, teachers, and parents are expected to:

- To always treat others with respect.
- Not undertake any actions that may bring the school into disrepute.
- Social media should not be used in any way to harass, insult, abuse or defame students, their family members, staff, and other members of the Maryfield College community.
- Respect the right to privacy of all other members of the school community.
- Respect copyright and acknowledge creators when using online content and resources.

Student Access to Technology

In our school, students will be given a username and password for a licenced Microsoft Office 365 account when they join the school. They will use this account for communication, collaboration and storage during their time in the school, using the Microsoft Office suite only which includes Teams, OneNote, One Drive etc. These accounts are controlled and restricted by the school. In some cases, restrictions may apply to all students, while other restrictions may apply to specific year groups, but it is also possible to restrict or suspend specific users' accounts.

Students will also have access to school-owned hardware, including desktops, laptops, iPads and Samsung Tablets. Students will need to sign in to each of these devices to use them and again restrictions will apply to their use, which prevents them from downloading software and accessing specific websites. All iPads are configured to a guest user so that no data is stored on the devices.
Please see separate mobile phone policy outlined in this AUP on page 7 and 8.

The School's Responsibilities

Maryfield College employs several strategies to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

- The Board of Management will approve the policy and ensure its development and evaluation.
- The Principal and Deputy Principal will be responsible for the dissemination of the policy; the application of sanctions; and together with the Parents Association and

Year Heads schedule workshops and guest speakers for students and parents on this topic.

- Filtering software and/or equivalent systems will be used to minimise the risk of exposure to inappropriate material.
- Uploading and downloading of non-approved software will not be permitted.
- The use of personal external digital storage media in school, requires school permission for the school's senior leadership team.
- Virus protection software will be used and updated on a regular basis.
- Internet use within school will always be supervised by a teacher.
- Students are not permitted to access the school's Wi-Fi network on personal devices
- The school currently uses shared managed devices as part of teaching, learning and assessment.
- The school has implemented a mobile phone policy that requires the use of a mobile phone pouch by all students, therefore, students do not have access to personal devices during the school day.
- The school licenses one common virtual learning environment, Microsoft Office 365.
- Our school will only communicate with students, parents and other stakeholders through communication tools controlled by our school. By using Office 365 email Outlook, iClass app and VS Ware mail, we have greater control over the information we store and share and who can see it. Our nominated platforms for online meetings are Teams and Zoom.

Maryfield College implements the following strategies for promoting safer use of the internet:

- Pupils will be provided with education in internet safety as part of our curriculum which includes Digital Media Literacy, Social Personal & Health Education, Civic, Social & Political Education and Guidance.
- Internet safety advice and support opportunities are provided to students in Maryfield College through our pastoral care system and the incorporation of online safety talks annually for students from Zeeko.
- Class teachers and parents will advise students on safe internet use.
- Teachers will be provided with continuing professional development opportunities in internet safety and the use of online tools for teaching and learning.
- Maryfield College participates in Safer Internet Day activities to promote safer, more effective use of the internet and this is communicated to parents to encourage parents to educate their children on safe use of the internet.
- Students use of the internet during class time will always be supervised by the class teacher or supervisor.

Monitoring of this Policy

The implementation of this Acceptable Use Policy will be monitored by the Principal, Deputy Principal and members of the school's leadership team and teachers.

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (including sites visited).
- Internal monitoring data for network activity.
- Surveys and/or questionnaires of pupils, parents, and teaching staff.

Should serious online safety incidents take place, the school Principal and Deputy Principal should be informed.

Content Filtering

Maryfield College has chosen to implement the following level of content filtering on the Schools Broadband Network:

Level 4: This level allows access to millions of websites including games and YouTube but blocks access to personal websites category, and other similar types of websites, such as blogs and blocks access to websites belonging to the personal websites category and websites such as Facebook belonging to the Social Networking category.

Students taking steps to by-pass the content filter by using proxy sites or other means may be subject to disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion.

Internet Use

- Students will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will be encouraged to report accidental accessing of inappropriate materials in accordance with school procedures to any member of school staff.
- Students will report accidental accessing of inappropriate materials in school but outside the classroom to their Year Head for their year group or the Deputy Principal or Principal.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Students and staff will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.
- Students will use the internet for educational purposes only.
- Students will not engage in online activities such as uploading or downloading large files that result in heavy network traffic which impairs the service for other internet users.
- Students will not download or view any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

- Downloading materials or images not relevant to their studies by students is in direct breach of the school's acceptable use policy.
- Students will never disclose or publicise personal information or passwords.
- Students will be aware that any usage of the internet and school's digital platform, including distributing or receiving information, school-related or personal, will be monitored.
- Use of file sharing and torrent sites is allowed with staff permission.

Email and Messaging

- Students downloading materials or images not relevant to their studies is not allowed.
- The use of personal email accounts is not allowed at Maryfield College .
- Students will use approved school email accounts only for all communication/ collaboration with staff on teaching, learning and assessment.
- Students should not under any circumstances share their email account login details with other pupils.
- Students should not use school email accounts to register for online services such as social networking services, apps, games or online shopping services.
- Students will use approved class email accounts only under supervision by or permission from a teacher.
- Students should be aware that email communications are monitored.
- Students will not send any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
- Students should immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. This can be reported to any members of teaching staff, year heads, deputy principal and principal.
- Students should avoid opening emails that appear suspicious. If in doubt, pupils should ask their teacher before opening emails from unknown senders.
- Students will not reveal their own or other peoples' personal details, such as addresses, telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through emails or on the internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher
- Students will not forward email messages, screenshots of emails, or "reply all" without the permission of the originator.
- Students must only use their school email for school related activities and for registering on school-based activities. The use of personal email addresses is not allowed for school-based work.
- All emails and opinions expressed in email are the responsibility of the author and do not reflect the opinion of the school.

Social Media and Messaging Services for Staff and Students

The internet provides a range of social media tools that allow us to interact and keep in touch. While recognising the benefits of these media for new opportunities for

communication, this policy sets out the principles that members of our school community are expected to follow when using social media.

The principles set out in this policy are designed to help ensure that social media is used responsibly so that the confidentiality of pupils and other staff and the reputation of the school is protected.

This policy applies to personal websites such as social networking sites (for example Instagram and TikTok), blogs, microblogs such as X, chatrooms, forums, podcasts, open access online encyclopedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as Flickr and YouTube.

The internet is a fast-moving technology and it is impossible to cover all circumstances or emerging media.

The following statements apply to the use of messaging, blogging and video streaming services in Maryfield College:

- Use of instant messaging services and apps including Snapchat, WhatsApp, Viber, etc. is not allowed in Maryfield College.
- Use of blogs such as WordPress, Tumblr etc. is allowed in Maryfield College with express permission from teaching staff.
- Use of video streaming sites such as YouTube and Vimeo etc. is with express permission from teaching staff.
- All members of the school community must not use social media, messaging services and the internet in any way to harass, impersonate, insult, abuse or defame others.
- Staff and students must not discuss personal information about pupils, staff and other members of the Maryfield College community on social media.
- The use of What's App groups is strongly discouraged and must not be used for communication between staff and students. Microsoft Teams is the only channel of communication for such groups.
- Staff and students must not use school email addresses for setting up personal social media accounts or to communicate through such media.
- Staff and students must not engage in activities involving social media which might bring Maryfield College into disrepute.
- Staff and students must not present their personal views as those of Maryfield College on any social medium.
- Students will be provided with guidance on etiquette regarding social media.
- Teachers can read further information about the use of social media and Electronic Communication here: https://www.teachingcouncil.ie/en/news-events/latest-news/2021/guidance-for-registered-teachers-about-the-use-of-social-media-and-electronic-communication.html

Personal Devices

Students using their own technology with the sole permission of the school's senior leadership team, in school, should follow the rules set out in this agreement, in the same way as if they were using school equipment.

The following statements apply to the use of internet-enabled devices such as phones, tablets and smartwatches, in Maryfield College:

- Students are only allowed to bring personal internet-enabled devices into Maryfield College with expressed permission from either the Principal or Deputy Principal.
- Students are only allowed to use personal internet-enabled devices during lessons with expressed permission from teaching staff.
- Students are not allowed to use personal internet-enabled devices during social time.

Maryfield College Mobile Phone Policy

This policy is part of our Maryfield College Code of Behaviour. This section of the Code of Behaviour has been extracted and presented as a single document to ensure clarity for all students, parents and staff in relation to the use of mobile phones and mobile phone storage pouches in our school.

- Mobile phones must not be used by students on school property at any time of the school day.
- To support this policy all students are issued with a mobile phone pouch. The mobile phone pouch is the property of Maryfield College and the responsibility of the student. Students must have their name and class clearly displayed on the outside of the pouch. Lost or damaged mobile phone pouches must be replaced at the expense of the parent/guardian at a cost of €20
- Before entering the schools' grounds students must place their mobile device inside the pouch and lock it. All mobile devices must be switched off or on silent in the mobile phone pouch.
- Mobile devices must remain inside the locked pouch for the duration of the school day. This includes during breaktime, lunchtime and after school activities.
- Students must store their mobile phone pouch either in their locked locker or their school bag during the school day. Teachers may request for the mobile phone pouch to be placed on the desk during class.
- Students can open the pouch at the end of the school day at the unlocking points located inside the school building and at points of exit from the building and grounds.
- Students leaving school before the end of the school day will use the unlocking facility in the main office.
- Students who feel unwell during the school day must always report to the main office. The school office will contact home. Students do not use mobile devices to contact home during the school day.
- Photographing, videoing or recording of students or staff is not permitted at any time.
- Students must not charge their phones on school premises.

- Should a student be in breach the Code of Behaviour in relation to mobile phones the following procedure and sanctions apply:
- The student must surrender their phone and phone pouch to the member of staff who has found them in breach of the code. The student will be requested to turn off their phone before handing it to the member of staff.
- The staff member will record the name of the student and their class and bring the mobile phone to the main office as soon as is convenient for the staff member.
- A record of the breach of the code is made in the office on the record sheet provided by the teacher.
- The student will collect their mobile phone at the end of the school day. Students will not have phones returned to them at break or lunchtime.
- Parents will be notified of the breach of the code by the Deputy Principal.
- After school detention will be served by the student for breach of the code.
- The breach of the Code of Behaviour will be recorded on VS Ware.
- Sanctions under the Code of Behaviour will escalate for repeated breaches of the mobile phone policy.

Digital Learning Platforms (including video conferencing)

- Maryfield College digital learning platform Office 365 is owned and managed by the school and the school's IT Support provider. This platform should enable two-way communication.
- Students must only use their school email to access the school digital learning platform.
- Only school devices should be used for the purposes of capturing and storing media. Students and staff must use office 365 One Drive for the storage of all data.
- All school-related media and data should be stored on the school's platform.
- The use of digital platforms should be used in line with considerations set out in the school's data protection plan (GDPR).
- Each user of the platform will be provided with their own unique login credentials.
- Passwords for digital platforms and accounts should not be shared.
- Personal email addresses should not be used when creating accounts on school digital platforms.
- Prior acceptance from parents should be sought for student usage of the schools' digital learning platform.

Remote Learning Policy

Students who by arrangement with the senior leadership team are unable to attend school for reasons explained by parents and guardians and supported by sufficient evidence medical or otherwise, or for reasons justified by the school leadership team may access teaching, learning and assessment resources through the schools VLE, Office 365.

Teachers will, by arrangement with the Senior Leadership Team, be requested to ensure that resources are made available to the student on the VLE and for feedback to be provided to the student via the VLE also. Remote learning is only arranged on a case-by-case basis and in full consultation with the school and parents/guardians and in the case of a student being over 18 years of age themselves.

Audio, images and video

- Care should be taken when capturing audio, photographic or video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- At Maryfield College students must not record audio, take, use, share, publish or distribute images of others without their permission.
- Taking audio, photos or videos on personal digital devices on school grounds or when participating in school activities is not allowed under any circumstances.
- Recording audio, photos or videos on school grounds or when participating in school activities is only allowed with expressed permission from staff and must be done using a school device only.
- Written permission from parents or carers will be obtained before video, audio or photographs of students are published on the school website.
- Students must not share audio, images, videos or other content online with the intention to harm another member of the school community regardless of whether this happens in school or outside.
- Sharing explicit images/video and in particular explicit images/video of students and/or minors is unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved. Sharing explicit images/video of other students automatically incurs suspension as a sanction.

Inappropriate Activities

The following is a list of inappropriate activities that if undertaken will be deemed to be in breach of this policy the following legislation also covers this section of the policy;

Data Protection Act 2018 updated to Data Protection (Amendment) Act 2003

Child First Act 2015

Child Trafficking and Pornography Act 1998

Interception Act 1993

Video Recordings Act 1989

The Data Protection Act 1988

The General Data Protection Regulation 2016/67

Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law)

- Promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation.
- Misuse and fraud legislation
- Racist material
- Pornography
- Promotion of any kind of discrimination

- Promotion of racial or religious hatred
- Harmful content or threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- Online gaming
- Online gambling
- Online shopping
- Use of social networking sites, instant messaging and online forums
- Child sexual abuse material
- Any other activity considered questionable

School Websites

- Students will be given the opportunity to publish projects, artwork or schoolwork on the internet in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website. Students will continue to own the copyright on any work published.
- The website will be regularly checked to ensure that there is no content that compromises the safety, privacy, or reputation of students or staff.
- Webpages allowing comments or user-generated content will be pre-moderated and checked frequently to ensure that they do not contain any inappropriate or offensive content.
- Maryfield College will use only digital photographs, audio or video clips of focusing on group activities. Content focusing on individual students will only be published on the school website with parental permission.
- The publication of student work will be coordinated by a teacher.
- Personal student information including home address and contact details will not be published on Maryfield College web pages.

- Maryfield College will avoid publishing the first name and last name of pupils in video or photograph captions published online.
- The school will ensure that the image files are appropriately named and will not use students' names in image file names or ALT tags if published online.

Cyberbullying

- In accordance with the Anti-Bullying Procedures for Schools and Bí Cineálta Policy Maryfield College considers that posting a single harmful message/image/video online which is highly likely to be reposted or shared with others can however be seen as bullying behaviour.
- This type of bullying is increasingly common and is continuously evolving. It is bullying carried out using information and communication technologies such as text, social media, e-mail, messaging, apps, gaming sites, chat-rooms and other online technologies. Being the target of inappropriate or hurtful messages is the most common form of online bullying. As cyberbullying uses technology to perpetrate bullying behaviour and does not require face to face contact. Cyberbullying can occur at any time (day or night). Many forms of bullying can be facilitated through cyberbullying. For example, a target may be sent homophobic text messages or pictures may be posted with negative comments about a persons sexuality, appearance etc.
- Access to technology means that cyberbullying can happen around the clock and the students home may not even be a haven from such bullying. Students are increasingly communicating in ways that are often unknown to adults and free from supervision. The nature of these technologies means digital content can be shared and seen by a very wide audience almost instantly and is almost impossible to delete permanently. While cyberbullying often takes place at home and at night, the impact can also be felt in school.
- In accordance with the Anti-Bullying Procedures for Schools and Bí Cineálta Policy Maryfield College considers that a once-off offensive or hurtful public message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or reposted and circulated on line by other people will be regarded as bullying behaviour.

When using the internet students, parents and staff are expected to always treat others with respect.

- Engaging in online activities with the intention of harming, harassing, or embarrassing another student or member of staff is unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved.
- Measures are taken by Maryfield College to ensure that staff and students are aware that bullying is defined as targeted behaviour, online or offline, that causes harm. The harm caused can be physical, social and/or emotional in nature. Bullying is repeated over time and involves an imbalance of power in relationships between two people or groups of people in society. Posting a single harmful message/image/video online which is highly likely to be reposted or shared with others can however be seen as bullying behaviour.
- The prevention of cyberbullying is an integral part of the anti-bullying policy of our school.

- In accordance with the Department of Education Bí Cineálta Policy Procedures to Prevent and Address Bullying Behaviour for Primary and Post Primary Schools; Maryfield College considers that a school is not expected to deal with bullying behaviour that occurs when students are not under the care or responsibility of the school. However, where this bullying behaviour has an impact in school, schools are required to support the students involved. Where the bullying behaviour continues in school, schools should deal with it in accordance with their Bí Cineálta Policy

Artificial Intelligence

- Maryfield College recognises the potential benefits of Artificial Intelligence (AI) in education and is committed to its responsible and ethical use within our learning environment.
- Maryfield College provides training and professional development opportunities for teachers to effectively utilise AI tools in their teaching practices, ensuring they stay up to date with technological advancements.
- The selection of AI tools and technologies in Maryfield College aligns with educational goals, including supporting learner agency and promoting critical thinking.
- AI technologies are integrated into the curriculum to enhance learner outcomes and experiences.
- Maryfield College integrates AI into its educational processes to enhance learning, foster innovation, and promote the development of critical skills.
- Maryfield College will make necessary adjustments to our school's adoption and integration of AI based on review and feedback.
- A regular review of the impact of AI on learning outcomes is conducted to ensure continuous improvement.
- School staff and learners receive training on the ethical use of AI technologies, including understanding data privacy, identifying biases, and verifying AI-generated information.
- All AI tools authorised for use in Maryfield College comply with data protection regulations (GDPR). Microsoft Co-pilot is the only AI tools permitted for use within the Maryfield College community.
- Entering personal, sensitive, or confidential data into any AI system without proper authorisation is strictly prohibited.
- Learners will not create, share or send any AI generated material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
- Staff and learners must not use AI in any way to harass, insult, abuse or defame learners, their family members, staff, other members of the Maryfield College community
- Staff and learners must not engage in activities involving AI generated material which might bring Maryfield College into disrepute.
- Maryfield College promotes digital literacy and critical thinking skills to help learners understand AI, its implications, and responsible usage. This includes data literacy, verification of AI-generated information, and recognising potential biases in AI tools.
- AI systems used in Maryfield College ensure fairness, transparency, and accountability in decision-making processes.

- Learners must attribute AI text and images properly when used in assignments/homework.
- Teachers will attribute AI text and images when used.
- AI Generated material is allowed for the purpose of research, brainstorming, and revising text.
- AI Generated material is allowed for certain activities with prior school permission.
- If used for research learners must factcheck, check other sources and reference sources.

Legislation

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Data Protection Acts 1988 to 2018 and General Data Protection Regulations (GDPR)
- Copyright and Related Rights Act 2000
- Child Trafficking and Pornography Act 1998 and Criminal Law (Sexual Offences) Act 2017
- Children First Act 2015
- Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law)
- Criminal Damage Act 1991

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet. Resources are also available online including;

Webwise – https://www.webwise.ie

Be Safe Online (Gov.ie) – https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/campaigns/be-safe-online/

CyberSafeKids Resources – https://www.cybersafekids.ie

ISPCC / Childline (Irish Safer Internet Centre Partner) – https://www.ispcc.ie/digital-ready-irish-safer-internet-centre/

National Parents Council (NPC) – https://www.npc.ie

Coimisiún na Meán – Parents' Guides – https://www.cnam.ie/general-public/guides-resources/for-parents/

Sanctions

Misuse of the Internet and digital technologies should be referred to in the school's Code of Behaviour and Bí Cineálta Policy and related sanctions regarding misuse as appropriate

should be outlined therein. The school also reserves the right to report any illegal activities to the appropriate authorities, including An Garda Siochana.

This policy was ratified by the Board of Management on 25th March 2026

Maryfield College Student Acceptable Usage Policy Agreement

I agree to follow the school's Acceptable Use Policy on the use of the internet and digital technologies. I will use the internet and digital technologies in a responsible way and obey all the procedures outlined in the policy.

Student's Signature: _____

Parent/Guardian : _____

Date: _____

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if students access unsuitable websites.

In relation to the school website, I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing students' work on the school website.

Signature: _____ Date: _____

Please review the attached school Internet Acceptable Use Policy, and sign and return this permission form to the Principal.

School Name: Name of Student: _____

Class/Year: _____

Student: _____