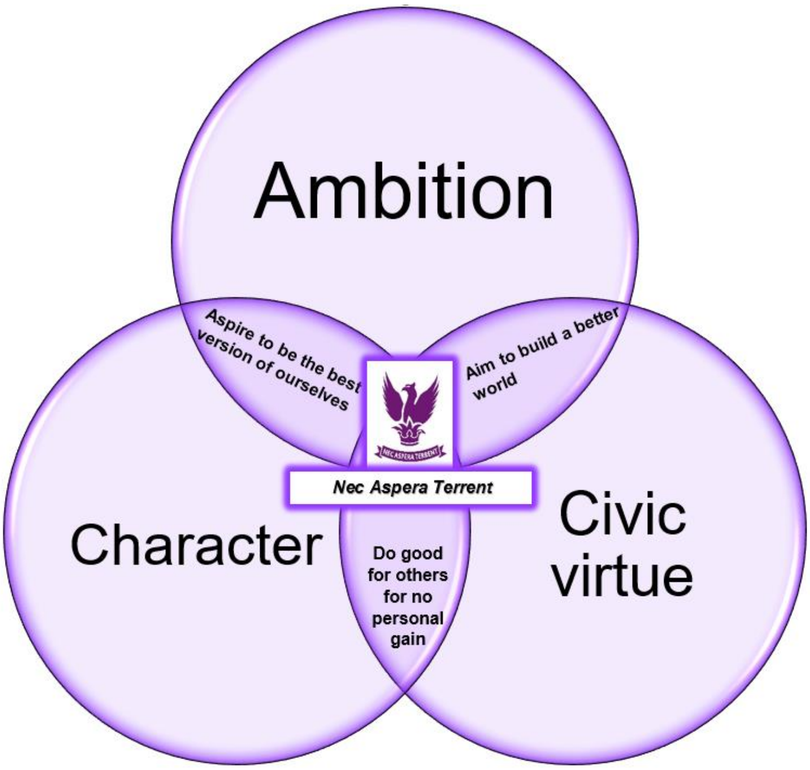
Item 15.5

DRAYTON MANOR HIGH SCHOOL

ONLINE SAFETY POLICY


Ambition
Aspire to be the best version of ourselves
Aim to build a better world
NEC ASPERA TERRENT
Nec Aspera Terrent
Character
Civic virtue
Do good for others for no personal gain

Reviewed by the Governing Body: 4 October 2024
Date of next review: October 2025

Contents

1. Aims

Our school aims to

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Heads and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Harmful online challenges and online hoaxes
- Filtering and monitoring standards

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.
The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Board

The governing board and Head have ultimate responsibility for ensuring that the policy and practices are embedded and monitored.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on Acceptable Use and Wireless Terms of Use and User License/Disclaimer (appendix 3 and 5)

- Receive appropriate online safety information/training as part of their safeguarding and child protection training; this should be received as part of their induction and be regularly updated.
- Ensure that the school leadership team and relevant staff have an awareness and understanding about of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

3.2 The Head

The Head is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and Deputy are set out in our child protection and safeguarding policy.

The DSL has overall responsibility for online safety in school, in particular

- Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head, IT manager and other staff, as necessary, to address any online safety issues or incidents
- The responsibility to manage filtering and monitoring systems
- Reviewing filtering and monitoring provision at least annually
- Ensuring that any online safety incidents are logged on the school's safeguarding platform (CPOMS) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety annually
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head and/or governing board

This list is not intended to be exhaustive.

3.4 The IT Manager

The IT Manager is responsible for

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that safeguard students, staff and governors.
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly in line with the Cyber Security Standards outlined in KCSIE, 2023
- Conducting a full security check and monitoring the school's IT systems on a regular basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on the school's safeguarding platform (CPOMS) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Reviewing the policy on a regular basis
- Deploying the Deputy IT Manager to support with these duties as necessary

This list is not intended to be exhaustive.

3.5 The Head of the Computing Department

The Head of Computing is responsible for

- Contributing to staff, student, parent and governor training
- Keeping abreast of updates and developments in IT and its usage
- Reviewing the policy on a regular basis

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on Acceptable Use of the school's ICT systems and the internet including wifi (appendix 3 and 5), and ensuring that students follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy and the Child Protection and Safeguarding Children Policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.7 Parents

Parents are expected to

- Notify a member of staff or the Head of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on
    - Acceptable Use of the school's ICT systems and internet (Appendices 1 and 2)
    - Wireless Terms of Use & User License Agreement/Disclaimer (Appendix 4)
    - Student Laptop Loan Agreement if applicable (Appendix 6)
    - Digital Student Charter (Appendix 7)

Parents can seek further guidance on keeping children safe online from the following organisations and websites

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum.

In **Key Stage 3**, students will be taught to

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, they will know*

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*
- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

Students can seek further guidance on keeping children safe online from the following organisations and websites

- For free and confidential advice - Childline
- To report and remove harmful online content - UK Safer Internet Centre

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or through the Parent Teacher Association. This policy will also be available to parents on the school website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes CCW and Computing lessons and other subjects where appropriate.

All staff and governors receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Drayton Manor High School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

using AI to include someone's likeness.

Drayton Manor High School will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the Drayton Manor High School

7. Acceptable use of the internet in school

All students, parents, staff and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Sixth Form students, staff, governors and visitors wishing to login to the wifi network as a guest user will also be asked to sign the Wireless Terms of Use & User License Agreement/Disclaimer (Appendices 4 and 5).

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the aforementioned agreements.

8. Students using mobile devices in school

Year 7-11 students are not permitted to bring mobile devices into school. Further details can be found in the School's Behaviour Policy.

Sixth Form students are permitted to use their mobile phones on school site but only in designated Sixth Form Centre and areas. Unless instructed by a staff member Sixth Form students are not to use their phones in

- Lessons
- Tutor time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2) and Wireless Terms of Use & User License Agreement/Disclaimer (Appendix 4).

Any breach of the acceptable use or wireless agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Students receiving laptops on loan from the school

Students who are loaned laptops by the school must carefully read, sign and adhere to the Student Laptop Loan Agreement (Appendix 6).

10. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT manager.

Work devices must be used solely for work activities. All school devices will be monitored in and outside school using a safeguarding monitoring tool.

11. How the school will respond to issues of misuse

Where a student misuses the school's IT systems or internet, we will follow the procedures set out in our behaviour policy and acceptable use agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, the staff bulletin and staff meetings).

The DSL and Deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Safe Use of images/film/camera

Taking of Images and Film

Permission must be obtained to take or store images of any member of the school community or public.

- Staff and parents can withdraw consent to the taking of images with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students; this includes when on field trips. However, with the permission of the Head, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on school field trips. However, with the express permission of the Head, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the student's device

Publishing Students' Images and Work

- Students' full names must not be published alongside their image and vice versa. E-mail addresses and postal addresses of students must not be published.

Storage of Images

- Images/films of students can be stored on the school's network and approved media
- Students and staff are not permitted to use personal portable media for storage of images (eg USB sticks) without the permission of the Head
- Rights of access to this material are restricted to the teaching staff and students within the confines of the intranet/Teams/Show My Homework
- The school has responsibility for deleting the images when they are no longer required, or the student has left the school

CCTV

The school uses CCTV for security and safety. The only people with access to this are designated by the Head. Notification of CCTV use is displayed at the front of the school

- Misuse of CCTV by any member of the school community will result in sanctions in line with school Behaviour Policy or Staff Code of Conduct.

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS.

This policy will be reviewed annually by the Designated Safeguarding Lead. At every review, the policy will be shared with the governing board.

15. Links with other policies

This online safety policy is linked to our

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Privacy notices
- Complaints procedure
- Online safety rules and acceptable use agreements (Appendices 1 and 2)
- Wireless acceptable use agreements (Appendices 4 and 5)
- Student Laptop Loan Agreement (Appendix 6)

APPENDIX 1

DRAYTON MANOR HIGH SCHOOL

ONLINE SAFETY RULES AND STUDENT ACCEPTABLE USE AGREEMENT (Key Stage 3 and 4)

At Drayton Manor High School, students enjoy excellent computer facilities and internet access to support students' learning. In addition to this we buy into and access many educational platforms to support you on your educational journey.

We require students to sign up to and respect the following rules to ensure that digital technology is used responsibly and safely at all times.

I agree that I will

- Only use school ICT systems, including but not limited to the internet, Microsoft Office, digital video, laptops and desktops for school purposes
- Not share any personal information such as full name, phone number or address unless guided to by a staff member
- Not download or install software on school technologies
- Not use the school resources to play games (either online or downloaded) other than those directed by a teacher
- Ensure that external storage devices used in school, including USBs, only contain files appropriate for school use
- Only log on to the school network and other platforms with my own user name and password
- Ensure that when 'unmuting' myself (for example of Microsoft Teams)
    - there is no inappropriate background noise
    - I will only do this when asked
    - I will contribute positively and appropriately when invited
- Not reveal my passwords to anyone and change them regularly
- Not browse, download, upload or share material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
- Seek approval from by my teacher and/or parent to meet someone as part of a school project
- Ensure that my online activity, both in school and outside school, will not cause distress to others
- Report any cases of cyber bullying to a member of staff immediately
- Respect the privacy of others' work on-line
- Not attempt to bypass school ICT security systems

- Make sure that all communication with others is responsible, appropriate and sensible, remaining polite at all times, writing in full sentences and using suitable salutations and sign-offs.
- Report any damage to technical devices, or inappropriate use of ICT systems immediately to a member of staff even if I am not responsible
- Always log off when I have finished working

I will not

- Use school communications systems for personal use
- Forward emails without consent of the person who wrote the email
- Visit inappropriate or banned websites, such as those that exhibit pornographic, sexist, racist, extremist or homophobic material
- Access social networking sites or chat rooms whilst on the school network
- Record, publish or distribute images or videos of other members of the DMHS community without formal permission
- 'Unmute' myself (for example on Microsoft Teams) when/if
    - I am not invited to
    - There are inappropriate background noises
    - I am not going to contribute positively or appropriately to the lesson
- Use digital technology in any way to bring DMHS into disrepute
- Download or stream any content that is not directly linked to my learning
- Use school ICT systems, including the internet, email, MS Teams, digital video, mobile technologies for to bully, harass upset or insult anyone
- Use personal communications systems eg Hotmail accounts for school use of any description
- Distribute, access or store images, text or materials that might be considered indecent, inappropriate, pornographic, discriminatory, sexist, racist, homophobic, extremist, obscene or illegal
- Access copyrighted information in a way that violates the copyright
- Broadcast unsolicited personal views on social, political, religious or other non-school related matters
- Transmit unsolicited commercial or advertising material (SPAM)
- Undertake deliberate activities that waste staff effort or networked resources
- Introduce any form of computer virus or malware into the school network
- Access another person's Microsoft Office account or any other password protected platform eg Show My Homework, Unifrog
- Share my passwords with anyone else
- Plagiarise work for homework, coursework, classwork at any time or share my work with other students for the purpose of plagiarism

I understand that

- All my use of the Internet and other related technologies will be monitored and logged both on and off site
- These rules are designed to keep me safe and that if they are not followed, school sanctions will be applied
- DMHS will check my computer files and may monitor the internet sites I visit and/or messages I send/receive both on and off site
- Lessons on Microsoft Teams/Zoom will be recorded
- If I fail to follow the rules outlined above, my access to the internet and/or the computer network will be affected and I will face sanctions as outlined in the school's Behaviour Policy.

ONLINE SAFETY RULES AND STUDENT ACCEPTABLE USE AGREEMENT (Key Stage 3 and 4)

Please read the Online safety Rules and Student Acceptable Use Agreement

We have discussed this document with our son/daughter ....
(Student's name)

who agrees to follow the Online Safety Rules and to support the safe and responsible use of ICT at Drayton Manor High School

NAME OF STUDENT ____
BLOCK CAPITALS PLEASE

SIGNATURE OF STUDENT ____

NAME OF PARENT ____
BLOCK CAPITALS PLEASE

SIGNATURE OF PARENT ____

DATE ________________________

APPENDIX 2

NEC ASPERA TERRENT

DRAYTON MANOR HIGH SCHOOL

SIXTH FORM ONLINE SAFETY RULES AND STUDENT ACCEPTABLE USE AGREEMENT

At Drayton Manor High School, Sixth Form students enjoy excellent computer facilities, a school email address and internet access to support students' learning. In addition to this we buy into and access many educational platforms to support you on your Sixth Form journey.

School email accounts will be set up for Sixth Form students and these will be used for the setting up of educational accounts with platforms such as

- Unifrog
- UCAS
- Project Q

Teachers may also contact students through the school's email system to communicate with them directly for educational purposes. Students may also use their school email addresses for communicating

- with Universities, Apprenticeship providers or other educational settings
- with Work Experience providers

We require students to sign up to and respect the following rules to ensure that digital technology is used responsibly and safely at all times.

I agree that I will

- Only use school ICT systems, including the internet, email, digital video, mobile technologies for school purposes
- Not give my email address to anyone unless they are relevant staff or educational/careers related settings
- Only use the DMHS email system to communicate with members of the school community and for educational purposes, or for communicating with educational or careers related settings eg UCAS, Universities, Work Experience providers about matters which support my education
- Not give out any personal information such as full name, phone number or address unless guided to by a staff member
- Not download or install software on school technologies
- Not use the school resources to play games (either online or downloaded) other than those directed by a teacher

- Ensure that external storage devices used in school, including USBs, only contain files appropriate for school use
- Only log on to the school network, email and other platforms with my own user name and password
- Not reveal my passwords to anyone and change them regularly
- Not 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
- Not arrange to meet someone unless this is part of a school project approved by my teacher and/or parent
- Ensure that my online activity, both in school and outside school, will not cause distress to others
- Report any cases of cyber bullying to a member of staff immediately
- Respect the privacy of others' work on-line
- Not attempt to bypass school ICT security systems
- Only use school email between 8am-6pm unless there is an emergency
- Make sure that all communication with others is responsible, appropriate and sensible, remaining polite at all times, writing in full sentences and using suitable salutations and sign-offs. More specifically, I will address those I am communicating with as Dear Sir/Madam or Dear *Mrs Bloggs*
- Report any damage to technical devices, or inappropriate use of ICT systems immediately to a member of staff even if I am not responsible
- Only contact teachers via email where it is absolutely necessary (for example if they have contacted me) and for educational purposes only
- Use my webcam and audio safely and appropriately when asked to by a staff member ensuring that
    - I have a neutral background
    - I, and any household members, are appropriately dressed and use appropriate language
    - I inform the staff member if the use of my webcam and audio if the above is not possible
- Always log off when I have finished working

I will not

- Use school communications systems for personal use
- Send group emails/messages
- Forward emails without consent of the person who wrote the email
- Visit inappropriate or banned websites, such as those that exhibit pornographic, sexist, racist, extremist or homophobic material
- Access social networking sites or chat rooms whilst on the school network
- Record, publish or distribute images or videos of other members of the DMHS community without formal permission
- Use digital technology in any way to bring DMHS into disrepute

- Download or stream any content that is not directly linked to my learning
- Use school ICT systems, including the internet, email, digital video, mobile technologies for to bully, harass upset or insult anyone
- Use personal communications systems eg Hotmail accounts for school use of any description
- Distribute, access or store images, text or materials that might be considered indecent, inappropriate, pornographic, discriminatory, sexist, racist, homophobic, extremist, obscene or illegal
- Access copyrighted information in a way that violates the copyright
- Broadcast unsolicited personal views on social, political, religious or other non-school related matters
- Transmit unsolicited commercial or advertising material (SPAM)
- Undertake deliberate activities that waste staff effort or networked resources
- Introduce any form of computer virus or malware into the school network
- Access another person's e-mail account or any other password protected platform eg Show My Homework, Unifrog
- Share my passwords with anyone else
- Plagiarise work for homework, coursework, classwork at any time or share my work with other students for the purpose of plagiarism

I understand that

- All my use of the Internet and other related technologies will be monitored and logged both on and offsite
- These rules are designed to keep me safe and that if they are not followed, school sanctions will be applied
- Lessons on Microsoft Teams/Zoom will be recorded
- Lesson recordings will be kept on file in the medium term (usually up to one year)
- DMHS will check my computer files and may monitor the internet sites I visit and/or emails I send/receive (both on and off site)
- If I fail to follow the rules outlined above, my access to the internet and/or the computer network will be affected and I will face sanctions as outlined in the school's Behaviour Policy.

SIXTH FORM ONLINE SAFETY RULES AND STUDENT ACCEPTABLE USE AGREEMENT

Please read the Sixth Form Online Safety Rules and Student Acceptable Use Agreement

We have discussed this document with our son/daughter ……………………………
(Student's name)
who agrees to follow the Online Safety Rules and to support the safe and responsible use of ICT at Drayton Manor High School

NAME OF STUDENT ______________________________
BLOCK CAPITALS PLEASE

SIGNATURE OF STUDENT ______________________________

NAME OF PARENT ______________________________
BLOCK CAPITALS PLEASE

SIGNATURE OF PARENT ______________________________

DATE ____________________

APPENDIX 3

NEC ASPERA TERRENT

DRAYTON MANOR HIGH SCHOOL

ONLINE SAFETY POLICY AND ACCEPTABLE USE AGREEMENT FOR STAFF AND GOVERNORS

This policy is designed to inform staff and governors of their professional responsibilities when using any form of ICT. Any concerns or clarification should be discussed with line managers or the Head.

I agree to

- only use the school's ICT systems for professional purposes or for uses deemed 'reasonable' by the Head
- ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute
- comply with the ICT system security and not disclose passwords
- ensure that all electronic communications with students and staff are compatible with my professional role, and never via personal email or phone
- not give out my own personal details, such as mobile phone number and personal email address, to students
- only use the approved, secure email system for school matters (staff)
- ensure that personal data is kept secure and is used appropriately, whether in school, off the school premises, or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head
- not install hardware or software without permission of the school IT Manager
- not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. I understand that to do so may constitute a disciplinary offence and in some cases a criminal offence
- respect copyright and intellectual property rights
- support and promote the school's Online Safety Policy
- help students to be safe and responsible in their use of ICT and related technologies
- ensure when using my webcam for remote lessons or meetings
    - the background is neutral
    - appropriate and professional dress and language is used at all times, by myself and any household members
- Record remote lessons for safeguarding purposes
- Exercise vigilance at all times when using platforms such as OneDrive. For example, never using the 'Share with People in Organisation' function
- Remind students of expectations and requirements when 'unmuting' themselves or enabling their camera (for Sixth Form only) through the use of Microsoft Teams

I also understand that

- images of students and/or staff will only be taken, stored and used for professional purposes and with written consent of the parent or staff member. Images will not be distributed outside the school network without the permission of the parent, member of staff or Head
- lesson recordings will be kept on file in the medium term (up to one year)
- all my use of the Internet and other related technologies will be monitored and logged

Drayton Manor High School Online Safety Policy and Acceptable Use Agreement

I have read this document and I agree to follow the Online Safety Rules.

Signature ………………………………………………………………

Full Name…………………………………………………..

Title………………………………………………………………

APPENDIX 4

NEC ASPERA TERRENT

DRAYTON MANOR HIGH SCHOOL

Wireless Terms of Use & User License Agreement/Disclaimer (SIXTH FORM)

The school offers Wi-Fi internet access services to students. This service allows Sixth Form students (you) to access the internet by connecting a wireless enabled device to the school network resources. Sixth Formers seeking to use the schools (our, we, us) network must first agree to the following terms of use

1. When and as available, we will allow students non-exclusive Wi-Fi connectivity while on the school premises. However, the school does not guarantee an internet connection; the bandwidth provided shall be at our sole discretion and your usage may be terminated by the school at any time without further notice.

2. While the school may agree to troubleshoot any connectivity problems on our network, we will not provide technical assistance for any devices not owned by us. Any assistance you might receive from us is strictly on an as is basis, without any warranties or representations.

3. The services may be used for lawful purposes only. Internet access through our Wi-Fi Service is filtered, and we may block or restrict access to certain websites based upon our security policies in place from time to time. Any content deemed illegal, inappropriate or unethical, including but not limited to content considered by us to be copyrighted, protected by trade secret regulation, threatening, defamatory, pornographic, illegal or terrorist in nature, may be blocked.

4. Personal Information. When using the service you must consent to the use of necessary cookies. Upon logging into the Wi-Fi network you will be required to provide minimal personal information, such as your user access credentials. You must not share or disclose your user access credentials with anyone else.

5. Using our service, you may download and upload content to and from your wireless access device. Be advised that content sent to and from a wireless access device using our Wi-Fi connection can be captured by anyone with appropriate technical knowledge. Although we incorporate wireless encryption technology into our service, use of our service is at your sole risk. We are not responsible for your content whether it is personal and/or educational in nature, and you assume sole responsibility for any theft, loss or corruption of your device or content.

6. We are not responsible for any loss of or damage to, your software and/or hardware, changes in configuration settings, security or data files while using our Wi-Fi Services. We are not responsible for any virus, Trojans, worms, malware or any other malicious software infecting your wireless access device while connected to our Wi-Fi network. We are not

responsible for any power anomalies or other events that may cause damage to your wireless access devices while using our services.

7. Your access to other devices on our private network such as printers, copiers, fax machines, scanners, etc., is strictly prohibited.

Our Wi-Fi services are provided -as is - we disclaim all warranties of any kind, either express or implied, including, without limitation, implied warranties of merchantability and fitness for a particular purpose.

In addition to what is outlined above I understand that

- These rules are designed to keep me safe and that if they are not followed, school sanctions will be applied
- If I fail to follow the rules outlined above, my access to the internet and/or the computer network will be affected and I will face sanctions as outlined in the school's Behaviour Policy.

Please read the **Wireless Terms of Use & User License Agreement/Disclaimer**

We have discussed this document with our son/daughter

____
(Student's name)
who agrees to follow the terms of use and to support the safe and responsible use of ICT and wifi at Drayton Manor High School

NAME OF STUDENT ______________________________
BLOCK CAPITALS PLEASE

SIGNATURE OF STUDENT ______________________________

NAME OF PARENT ______________________________
BLOCK CAPITALS PLEASE

SIGNATURE OF PARENT ______________________________

DATE ______________________________

APPENDIX 5

NEC ASPERA TERRENT

DRAYTON MANOR HIGH SCHOOL

Wireless Terms of Use & User License Agreement/Disclaimer (STAFF/GUEST USERS)

The school offers Wi-Fi internet access services to Drayton Manor Staff and other guests to the school. This service allows staff and guests by invitation (you) to access the internet by connecting a wireless enabled device to the school network resources. Staff and guests seeking to use the schools (our, we, us) network must first agree to the following terms of use

1. When and as available, we will allow staff and guests non-exclusive Wi-Fi connectivity while on the school premises. However, the school does not guarantee an internet connection; the bandwidth provided shall be at our sole discretion and your usage may be terminated by the school at any time without further notice.

2. While the school may agree to troubleshoot any connectivity problems on our network, we will not provide technical assistance for any devices not owned by us. Any assistance you might receive from us is strictly on an as is basis, without any warranties or representations.

3. The services may be used for lawful purposes only. Internet access through our Wi-Fi Service is filtered, and we may block or restrict access to certain websites based upon our security policies in place from time to time. Any content deemed illegal, inappropriate or unethical, including but not limited to content considered by us to be copyrighted, protected by trade secret regulation, threatening, defamatory, pornographic, illegal or terrorist in nature, may be blocked.

4. Personal Information. When using the service you must consent to the use of necessary cookies. Upon logging into the Wi-Fi network you will be required to provide minimal personal information, such as your user access credentials. You must not share or disclose your user access credentials with anyone else.

5. Using our service, you may download and upload content to and from your wireless access device. Be advised that content sent to and from a wireless access device using our Wi-Fi connection can be captured by anyone with appropriate technical knowledge. Although we incorporate wireless encryption technology into our service, use of our service is at your sole risk. We are not responsible for your content whether it is personal and/or educational in nature, and you assume sole responsibility for any theft, loss or corruption of your device or content.

6. We are not responsible for any loss of or damage to, your software and/or hardware, changes in configuration settings, security or data files while using our Wi-Fi Services. We are not responsible for any virus, Trojans, worms, malware or any other malicious software

infecting your wireless access device while connected to our Wi-Fi network. We are not responsible for any power anomalies or other events that may cause damage to your wireless access devices while using our services.

7. Your access to other devices on our private network such as printers, copiers, fax machines, scanners, etc., is strictly prohibited.

Our Wi-Fi services are provided -as is - we disclaim all warranties of any kind, either express or implied, including, without limitation, implied warranties of merchantability and fitness for a particular purpose.

In addition to what is outlined above I understand that

- These rules are designed to keep our school community safe
- If I fail to follow the rules outlined above, my access to the internet and/or the computer network will be affected and school policies will apply

Please read the **Wireless Terms of Use & User License Agreement/Disclaimer**

I ______________________________ have read this agreement
(Full name)

And agree to follow the terms of use and to support the safe and responsible use of ICT and wifi at Drayton Manor High School

NAME ______________________________
BLOCK CAPITALS PLEASE

SIGNATURE ______________________________
BLOCK CAPITALS PLEASE

STAFF LINK NAME ______________________________

DATE ______________________________

APPENDIX 6

NEC ASPERA TERRENT

DRAYTON MANOR HIGH SCHOOL

Student Laptop Loan Agreement

The laptop, and any accessories provided with it, remains the property of Drayton Manor High School and is strictly for the sole use of assisting in the delivery of the curriculum. For example

- Class/homework purposes
- Independent learning and academic development
- Reasonable personal use that relates to learning and academic development

I understand

- This agreement applies to the use of the laptop regardless of my location
- Emails, MS Teams, Office files and all data are stored on the laptop for learning purposes only
- This information will be filtered and monitored, and may be accessed to meet the school's business needs at any time
- All internet activity is closely filtered, monitored and restricted for the safeguarding of myself and others

I will not

- Deface or stick anything to the laptop
- Eat or drink whilst using the laptop or keep food or drink near the laptop
- Leave the laptop unattended in class without being secured
- Do anything that may compromise the safety of myself, other students or staff
- Give out personal information or disclose my username or password to anyone else. If you forget your password or think someone may know it speak to your form tutor immediately
- Try to use any other person's username and password for any purpose
- Attempt to access files or programmes for which I have not been granted access
- Engage in any online activity that might bring the school's reputation into disrepute
- Access, copy, remove or alter any other user's files without their explicit permission
- Play online games or engage in online chat/messaging not directly linked to learning
- Attempt to download and install programmes, software or viruses on the school's device
- Try to circumvent security settings or content filters

- Deliberately breach anyone's copyright
- Attempt to fix suspected faults (hardware or software) nor shall I let anyone other than school IT staff

I will

- Treat the laptop with due care and keep the laptop in good condition,
- Bring to the attention of my form tutor any ICT activity or material that may be inappropriate or harmful
- Report any damage or faults involving equipment or software, however this may have happened, as soon as reasonably possible to the IT Department
- Only use Drayton Manor provided systems to communicate with staff and students
- Return the laptop to a designated member of staff upon request

Emails

Email access is provided for use both within and outside Drayton Manor High School Sixth Form (for Sixth Form students only) but must be used appropriately and for school work only.

Always ensure you are polite, use appropriate language and never reveal any personal information about yourself. Student email is not considered to be private and is actively monitored; inappropriate use of the system will be passed on to the relevant staff member.

Protect yourself by being ultra-cautious with emails you receive

- If you were not expecting it, then be suspicious
- Do not open attachments unless you were specifically expecting them
- Do not click on links outside of Drayton Manor High School network unless you are certain they are safe
- If in doubt, do not open the email.
- Report all concerns – no matter how trivial – to your form tutor

It would be completely unacceptable to send threatening, inappropriate or harassing emails/messages to anyone within or outside of the school community. Circulating such emails/messages that others have written or taken is also forbidden.

Images and Videos

- I will not use the school's laptop device to take or store images which are not linked to my learning and the school's curriculum
- I will not use the school's laptop device to take photos or videos of anyone else without their permission
- I will not use the school's laptop device to store photos or videos of anyone else without their permission

Any of the above activity, in addition to anything else which is deemed an unacceptable use of the school's laptop devices, will be reported to the relevant member of staff and dealt with appropriately.

Loss, accidental damage, theft and general hardware issues

- Loss of the laptop or any accidental damage should be reported immediately to the IT Department and Head of Year
- Any general problems should be reported to the IT staff and all hardware and accessories must be supplied to help resolve any issues.
- Students and/or parents/carers may be invoiced to cover the costs of replacing any laptops which are not returned, or if not all parts are returned

Your agreement

I confirm that I have read and agree to adhere to current school policies regarding the following, which can be found on the school website

- Online safety rules and student acceptable use agreement
- Privacy Notice
- Health and safety

I understand that if I fail to comply with this Student Laptop Loan Agreement, I may

- have my ICT access suspended
- have the laptop taken away
- be sanctioned in line with the school's behavior policy

Student Laptop Loan Agreement

Laptop Details

Laptop Make:……………………………………….. Serial Number:……………………………..
Model:……………………………………………… Asset

Personal Details

TO BE COMPLETED BY THE SCHOOL

Loan Authorised by ……………………………………

School (signature): ....……… Date ....

TO BE COMPLETED BY THE STUDENT AND PARENT

Student Name ……………………………………….. Tutor Group ………

I (parent/caret and the student) have read and agree to be bound by the terms and conditions set out above.

Name of parent..

Signature (parent) …………………………………… Date ....

Received by (student signature): .... Date ....

APPENDIX 7

DRAYTON MANOR HIGH SCHOOL
DIGITAL STUDENT CHARTER
OUR VALUES IN KEEPING US SAFE AND WELL

As a student body, we are clear that we do not accept behaviours which deliberately hurt or upset a member of our community either physically, verbally, or mentally. This includes behaviours which occur in person and online. Our student digital charter reinforces our belief as a student body that the way we conduct ourselves in the virtual world is as important as we do in the real world and that this inappropriate behaviour in this domain can have long lasting effects on members of our community and serious consequences for us as individuals.

These behaviours can include:

1. Sharing or spreading hateful content online, including spreading gossip or malicious rumors, posting threatening or intimidating messages or other digital content of a similar nature.
2. Do not advocate or by ‘commenting’ on or ‘liking’ negative hurtful discriminating messages of others.
3. Do not create social media accounts that impersonate or pretend to be others.
4. Using the school email system for anything other than educational purposes.
5. Inappropriately using all electronic devices in school or out of school, which includes playing games, using social media platforms, or searching for harmful or inappropriate content.
6. Sharing inappropriate media which may cause harm to another member of our community.
7. Participating in malicious activities online, which includes hateful comments on social media and within the comment area of any online platform.
8. Distributing malware within the school network or at home.
9. Do not share or give out any personal information or share images or information about others without their consent.

In addition to the above, it is important that we remain safe whilst online and using technology. To help protect our wellbeing, we recommend adhering to the points below:

1. Ensure all your accounts are set to private and do not allow anyone to follow them who you do not know personally.
2. Only use social media platforms that are age appropriate – for example, *whatsapp* user age is 16+.
3. Unless you are using the internet to assist with your independent studies, limit the amount of time you engage with social media each day to no more than 2 hours.
4. Ensure you do not use your phone or computer within 30 minutes of going to sleep.
5. If you have any concerns involving digital media, please report them to the Designated Safeguarding Lead or a member of staff.
6. Do not share images or information about others without consent.
7. Do not post online content that contains your school uniform.