



Midleton C.B.S.
Secondary School
An Edmund Rice School

Acceptable Use Policy

Ratified: 25th May 2026

Due for review: 2028

Contents

1. Introduction	2
2. Purpose of the Policy	2
3. Scope of the Policy	2
4. Definition of Devices	3
5. Student Key Expectations	3
6. General Principles	3
7. Safety, Filtering and Monitoring	4
8. Device Misuse	4
9. Education and Support	5
10. Reporting Serious Online Safety Concerns	5
11. Content Filtering	5
12. Internet Use	6
13. Email and Messaging	7
14. Social Media and Messaging Services	7
15. Personal Devices and School-Managed Chromebooks	8
16. Use of Computer Rooms and Shared School Devices	8
17. Digital Learning Platforms	8
18. Images, Video, Audio and Wearable Technology	9
19. Inappropriate Activities	10
20. School Websites and Publications	10
21. Cyberbullying	11
22. Artificial Intelligence	11
23. Consequences and Recording	12
24. Legislation and Support Structures	13
25. AUP Agreement Form	14
26. Ratification	15
Appendix 1 – SEN Provided Devices	16
Appendix 2 – Care of Devices	18

This policy should be read in conjunction with the school's Code of Ethics and Behaviour, Bí Cineálta Anti-Bullying Policy, Social Media Policy, Data Protection Policy, Child Safeguarding Statement, Personal Mobile Device Usage Policy, and other relevant school policies.

1. Introduction

Midleton CBS Secondary School recognises that digital technology is an important part of teaching, learning, communication, and school life. Access to the internet, school-managed devices, online platforms, and digital tools provides valuable opportunities for students to learn, collaborate, create, research, and develop important digital skills.

The purpose of this Acceptable Use Policy is to promote the safe, responsible, respectful, and effective use of digital technology by students and staff. The policy sets out expectations for the use of devices, school accounts, online platforms, the internet, artificial intelligence tools, and other digital technologies connected with school life.

This policy should be read in conjunction with the school's Code of Ethics and Behaviour, Bí Cineálta Anti-Bullying Policy, Social Media Policy, Data Protection Policy, Child Safeguarding Statement, Personal Mobile Device Usage Policy, and other relevant school policies.

2. Purpose of the Policy

This policy aims to:

- support the effective use of digital technology for teaching and learning;
- promote safe and responsible internet use;
- protect the privacy, dignity, and wellbeing of students, staff, and the wider school community;
- reduce risks associated with inappropriate online activity, cyberbullying, distraction, and misuse of devices;
- clarify expectations around school accounts, digital platforms, personal devices, school-managed devices, wearable technologies and artificial intelligence;
- ensure that misuse of digital technology is addressed consistently through the school's Code of Ethics and Behaviour.

3. Scope of the Policy

This policy applies to students, staff, and all users of the internet, school network, school-managed devices, school accounts, and digital platforms in Midleton CBS Secondary School.

It applies:

- on the school premises;
- during school-related activities, including trips, tours, matches, retreats, liturgies and events;
- when using school accounts or school digital platforms;
- when using a device for school-related learning or communication;

- where online behaviour outside school has an impact on the school community.

4. Definition of Devices

For the purposes of this policy, “devices” refers to any digital device used to access the internet, school networks, school accounts, or digital learning platforms. This includes devices that are owned by parents/guardians but configured or managed by the school for educational purposes.

This includes, but is not limited to:

- school-managed Chromebooks;
- laptops;
- tablets;
- smartphones;
- smartwatches;
- school desktop computers;
- similar technology used for teaching, learning, communication, or school-related activity;
- wearable or emerging technologies such as smart glasses, AI-enabled glasses, body-worn cameras, or any similar device capable of recording, transmitting, processing, displaying, or receiving digital content.

5. Student Key Expectations

Students are expected to:

- use devices only when directed by staff;
- use school accounts and platforms responsibly;
- stay on task and avoid games, messaging, or unrelated websites;
- respect the privacy and dignity of others;
- never take, record, livestream or share images, video, or audio without permission;
- never share passwords or login details;
- report anything online that is upsetting, threatening, inappropriate, unsafe, or bullying in nature;
- use artificial intelligence tools only as permitted by the teacher and never submit AI-generated work as their own.

6. General Principles

When using digital technology, all members of the school community are expected to:

- treat others with respect at all times;
- act in a way that reflects the values and ethos of Midleton CBS;
- respect the privacy and dignity of others;

- use school accounts and platforms only for school-related purposes;
- respect copyright and acknowledge sources and creators when using online content;
- follow staff instructions regarding device and internet use.

Access to digital technology in school is provided to support teaching and learning. During lessons, devices may only be used when directed by the teacher and for the purpose set by the teacher. Students must close, lower, or put away devices when instructed to do so.

7. Safety, Filtering and Monitoring

The school uses a range of measures to support safe and appropriate use of digital technology. These include:

- content filtering and/or equivalent systems to reduce the risk of exposure to inappropriate material;
- monitoring systems to support safeguarding, network security, and appropriate use;
- staff supervision of internet and device use as appropriate;
- restrictions on downloading or installing non-approved software;
- limits on the use of personal external digital storage media unless permission has been given.

Internet and device use in school is subject to staff supervision, filtering, and monitoring as appropriate. Monitoring is proportionate and is used to support student safety, appropriate use of school systems, and the effective operation of the school network.

Monitoring and filtering systems are not a substitute for responsible use by students. No filtering or monitoring system can guarantee that inappropriate material will never be accessed. Students are expected to report accidental access to inappropriate, upsetting, or unsafe material immediately.

8. Device Misuse

Misuse of devices, the internet, school accounts, or digital platforms will be addressed in accordance with the school's Code of Ethics and Behaviour. Recording systems may be used to support consistent follow-up and to identify repeated patterns of misuse. The school also reserves the right to report illegal activity to the appropriate authorities.

Device misuse includes, but is not limited to:

- accessing non-educational websites;
- gaming during class or school activities without permission;
- messaging or chatting without permission;
- switching to unrelated tabs, apps, or content;
- watching videos not directed by the teacher;
- using a device to distract others;

- attempting to bypass filtering or monitoring systems;
- using a device in any way that disrupts teaching and learning;
- using digital technology to harass, bully, intimidate, defame, exclude, impersonate, humiliate or embarrass another person.

9. Education and Support

Midleton CBS promotes safer and more responsible use of digital technology through:

- internet safety education as part of SPHE and other curriculum areas;
- induction, pastoral care, ICT, and peer mentoring programmes;
- participation in Safer Internet Day and related awareness initiatives;
- guidance for students on respectful online behaviour, privacy, copyright, digital wellbeing and academic integrity;
- continuing professional development opportunities for staff where appropriate.

10. Reporting Serious Online Safety Concerns

Students should report any online content, communication, or activity that is upsetting, threatening, inappropriate, unsafe, or bullying in nature to a teacher, Year Head, Deputy Principal, Principal, another trusted adult in the school, or a trusted adult outside the school who can liaise with the school on their behalf.

Where serious online safety incidents arise, the relevant Deputy Principal should be informed. Where a concern may relate to child safeguarding, the matter must be dealt with in accordance with the school's Child Safeguarding Statement and relevant child protection procedures.

11. Content Filtering

The school uses content filtering through the Schools Broadband Network and/or other approved filtering systems. These systems are used to reduce, but cannot eliminate, the risk of exposure to inappropriate material.

Midleton CBS has chosen to implement the following level on content filtering on the Schools Broadband Network:

Level 3 This level allows access to millions of websites including games but blocks YouTube, and blocks access to websites belonging to the personal websites category and websites such as Facebook belonging to the Social Networking category.

Students must not attempt to bypass filtering, monitoring, network restrictions, or other safeguards using proxy sites, VPNs, hotspotting, unauthorised browsers, extensions, apps, or any other method. Such behaviour may be treated as misuse under the Code of Ethics and Behaviour.

Where a student or staff member believes that a legitimate educational website has been incorrectly blocked, they may ask a teacher or member of staff to submit the site for review through the school's ICT procedures.

12. Internet Use

During lessons, devices may only be used when directed by the teacher and for the purpose set by the teacher. Students must close, lower, or put away devices when instructed to do so.

Students must use the internet for educational purposes only and must not intentionally visit websites or access material that is obscene, illegal, hateful, violent, discriminatory, defamatory, harmful, or otherwise inappropriate.

Students should report accidental access to inappropriate material to the teacher in class. If inappropriate material is accessed outside the classroom but during school time, students should report this to a tutor, Year Head, Deputy Principal, Principal or another trusted adult.

Students must not copy information into assignments without acknowledging the source. Plagiarism, copyright infringement, and the submission of work that is not the student's own may be addressed under the school's Code of Ethics and Behaviour and relevant assessment procedures.

Students must not engage in online activities such as uploading or downloading large files that cause heavy network traffic or impair the service for other users. Students must not download, install, or view material that is not relevant to their studies unless directed by staff.

Students must not open, download, install, or share files, programmes, links, or attachments that are suspicious, unknown, or unrelated to schoolwork. If a student believes a device, account, file, or link may pose a security risk, they should inform a teacher or member of staff immediately and should not attempt to resolve the issue themselves.

The school may use appropriate tools and teacher judgement to check student work for plagiarism, inappropriate copying, or misuse of artificial intelligence.

Students must never disclose, share, or publicise passwords, login details, personal information, private images, or personal details belonging to themselves or others.

The school uses filtering and monitoring systems to support safe and appropriate use of school networks and school-managed devices. Monitoring is proportionate and is used during the school day and/or while devices are being used for school-related purposes. The school does not actively monitor student device screens outside designated monitoring times. Responsibility for the supervision of device use outside school hours rests with parents/guardians.

13. Email and Messaging

School email accounts and school messaging systems are provided for school-related communication and learning. Students must use approved school accounts for schoolwork and must not use personal email accounts for school-based work unless specifically permitted by a teacher.

Students are expected to:

- use school email and messaging systems responsibly and for school-related purposes only;
- keep usernames, passwords and login details private;
- not use school email accounts to register for personal online services, social networking services, games, apps, or non-school accounts;
- not send, forward, screenshot, circulate, or respond to messages that are offensive, discriminatory, threatening, bullying, defamatory, obscene, or intended to annoy, intimidate, or upset another person;
- avoid opening suspicious emails or attachments and seek advice from a teacher where unsure;
- report any communication that makes them feel uncomfortable, unsafe, threatened, bullied, or upset to a teacher or another trusted adult.

Emails, messages, and communications sent using school systems may be monitored where necessary for safety, security, network management, safeguarding, or behaviour-related reasons. Views expressed by users do not represent the views of the school unless formally authorised.

14. Social Media and Messaging Services

This section should be read in conjunction with the school's Social Media Policy. Students and staff must use social media, messaging services, and online platforms responsibly and in a way that respects the privacy, dignity, and reputation of others.

Students and staff must not use social media, messaging services, or online platforms to harass, impersonate, insult, abuse, defame, exclude, intimidate, humiliate, or target another person. Personal information about students, staff, parents/guardians, or other members of the school community must not be shared on social media or messaging services.

Students must not use school email addresses to create personal social media accounts, gaming accounts, or other personal online accounts. Staff and students must not represent personal views as those of Midleton CBS Secondary School.

Use of instant messaging services, social media, blogs, forums, video-sharing platforms, or similar services during school time or school activities is only permitted where directed by staff for an approved educational purpose. The use of such platforms must comply with this policy, the Code of Ethics and Behaviour, the Bí Cineálta Anti-Bullying Policy, the Social Media Policy and the Data Protection Policy.

15. Personal Devices and School-Managed Chromebooks

Students using their own technology in school must follow this policy in the same way as if they were using school equipment.

Students may only use personal internet-enabled devices on campus where permitted by staff and for an approved educational purpose. Personal mobile device use is governed by the school's Personal Mobile Device Usage Policy and Code of Ethics and Behaviour.

Some students use Chromebooks or laptops that are owned by parents/guardians but configured and managed by the school for educational purposes. These devices are subject to school settings, filtering, and monitoring during the school day and while used for school-related activity. Students are expected to bring their device charged and ready for learning where required, and to use it only as directed by staff.

Students may be required to close, lower, put away, remove, or hand up a device where its use or functionality could interfere with teaching and learning, privacy, supervision, or the safe operation of the school. Responsibility for supervision of device use outside school hours rests with parents/guardians.

16. Use of Computer Rooms and Shared School Devices

Students using computer rooms, shared school computers, Chromebook carts, or other shared school devices must follow the directions of the supervising teacher. Food and drink are not permitted near school devices. Students must not interfere with hardware, software, cables, settings, or the work of other users. Printing may only take place with staff permission and must be for school-related purposes. Students should log out correctly after use.

17. Digital Learning Platforms

Midleton CBS uses school-managed digital learning platforms and accounts to support teaching, learning, communication, collaboration, and assessment. These platforms should be used in accordance with this policy and the school's Data Protection Policy.

Students must use their school account to access school digital learning platforms. Personal email addresses should not be used when creating accounts on school digital platforms unless specifically permitted by the school.

Each user of school digital platforms will be provided with their own login credentials. Passwords for digital platforms and accounts must not be shared.

When working on shared or collaborative documents/devices, students must respect the work of others and must not delete, alter, copy, or interfere with another person's work without permission.

All school-related media and data should be stored on school-approved systems. Teachers may direct students to use approved or appropriate educational platforms to support teaching and learning. Where a platform requires student accounts, logins, or the processing of student data, its use should be consistent with the school's Data Protection Policy and school procedures.

In the event of remote learning, students are expected to follow the same standards of respectful, responsible, and appropriate digital behaviour as apply in school.

18. Images, Video, Audio and Wearable Technology

Students must not photograph, record, livestream, transcribe, or share images, video, or audio of students, staff, classes, school activities, school events, conversations, or school premises without express permission from a staff member.

Taking photographs, video, or audio on school grounds or while participating in school activities is only allowed with express permission from staff. Any approved use must respect the privacy, dignity, and safety of all involved.

Smart glasses, AI-enabled glasses, wearable cameras, AI dictation tools, transcription tools, or similar devices must not be used to photograph, record, livestream, transcribe, summarise, or process images, video, audio, classroom activity, conversations, meetings, or school events without the express permission of the staff member responsible for the class, meeting, activity, or event. Permission must be specific to the use proposed, and any staff member or student whose voice, image, words, or personal information may be captured must be made aware in advance.

Students must not share images, videos, audio, screenshots, recordings, or other digital content online with the intention to harm, embarrass, humiliate, intimidate, harass, bully, defame, or target another member of the school community, regardless of whether this happens in school or outside school.

Sharing explicit images, particularly images involving students or minors, is strictly prohibited and will be treated as a serious breach of the Code of Ethics and Behaviour. Such matters may also require referral to parents/guardians, the Designated Liaison Person, An Garda Síochána, Tusla, or other relevant authorities, as appropriate.

Students should be aware that the non-consensual recording, sharing, publication, or distribution of intimate images or harmful communications may have serious school and legal consequences and may constitute a criminal offence under Irish law, including Coco's Law. In Ireland, the general age of criminal responsibility is 12. Students should think carefully before creating, forwarding, reposting, or sending any image, video, message, or online content involving another person.

The school will seek appropriate consent before publishing student photographs, recordings, or student work on the school website, app, newsletter, social media accounts, or other school publications, in accordance with the school's Data Protection Policy and consent procedures.

19. Inappropriate Activities

The following activities are prohibited unless expressly permitted by staff for an approved educational purpose. This list is not exhaustive.

- promotion or conduct of illegal acts, including under child protection, harassment, harmful communications, computer misuse, fraud, obscenity or criminal damage legislation;
- accessing, creating, sharing or promoting racist, sexist, homophobic, transphobic, discriminatory, hateful, extremist, violent, pornographic, or otherwise harmful material;
- promotion of any kind of discrimination, racial hatred, religious hatred, harassment, bullying, intimidation, violence, self-harm or harm to others;
- using school systems for private business, commercial activity, gambling, shopping, gaming, or non-school purposes;
- using systems, applications, websites, extensions, VPNs, proxy sites, hotspotting or other mechanisms to bypass filtering, monitoring, or other safeguards employed by the school;
- uploading, downloading, or transmitting commercial software or copyrighted material without necessary permissions;
- revealing or publicising confidential, personal, financial, private, proprietary, or login information;
- creating, distributing, downloading, or propagating computer viruses, malware, harmful files, or malicious code;
- carrying out high-volume network activity that causes congestion or hinders others in their use of the internet;
- accessing, creating, storing, sharing, or distributing child sexual abuse material or explicit images of minors.

20. School Websites and Publications

The school website, school app, newsletter, social media accounts, and other school publications will be managed in a way that protects the safety, privacy, and reputation of students, staff, and the wider school community.

The publication of student work, photographs, audio, or video will be coordinated by staff and managed in accordance with the school's Data Protection Policy, Social Media Policy, and consent procedures.

Personal student information, including home addresses, personal contact details, and other identifying information, will not be published on school websites or school social media accounts.

Where images are published online, the school will take reasonable steps to ensure that files are appropriately named and that personal data is not unnecessarily included in file names, captions, tags, metadata, or alternative text.

Where webpages or online platforms allow comments or user-generated content, the school will moderate or review content as appropriate to reduce the risk of inappropriate, offensive, or harmful material being displayed.

Students retain ownership of their own original work, subject to the school's right to display or publish it for educational, celebratory, or school-related purposes in line with consent procedures.

21. Cyberbullying

Cyberbullying is bullying behaviour carried out through digital technology, including text, social media, email, messaging apps, gaming platforms, chat rooms, websites, images, video, or other online technologies. This section should be read in conjunction with the school's Bí Cineálta Anti-Bullying Policy.

Bullying is defined in the Bí Cineálta procedures as targeted behaviour, online or offline, that causes harm. The harm can be physical, social and/or emotional. Bullying behaviour is repeated over time and involves an imbalance of power. However, posting a single harmful message, image, video, or statement online that is highly likely to be reposted or shared may be considered bullying behaviour.

Students must not use digital technology to harm, harass, intimidate, humiliate, exclude, impersonate, threaten, embarrass, defame, or target another student, member of staff, or member of the school community.

Where cyberbullying has an impact in school, the school will support the students involved. Where bullying behaviour continues in school, it will be dealt with in accordance with the school's Bí Cineálta Anti-Bullying Policy. Where behaviour is inappropriate but does not meet the definition of bullying, it may be addressed under the Code of Ethics and Behaviour.

22. Artificial Intelligence

Midleton CBS recognises that artificial intelligence (AI) tools can support teaching, learning, research, study, accessibility, creativity, and revision when used responsibly and where permitted by the teacher.

AI tools may be used to support learning where permitted by the teacher. Acceptable uses may include helping students understand a topic, generate study prompts, summarise notes, create revision materials, check understanding, brainstorm ideas, or improve clarity in their own work.

Students must not submit AI-generated work, in whole or in part, as their own work unless this has been expressly permitted by the teacher and properly acknowledged. Misuse of AI may be treated as academic dishonesty under the school's Code of Ethics and Behaviour and relevant assessment procedures.

Where AI is used with teacher permission, students may be required to explain how the tool was used, the extent of its contribution, and how they checked the accuracy and reliability of the output. Students remain responsible for the accuracy, originality, and integrity of work submitted.

Students must not use AI to create, share, or send material that is illegal, obscene, offensive, discriminatory, defamatory, misleading, harmful, bullying, intimidating, or intended to annoy, embarrass, or upset another person.

Students must not enter personal, sensitive, confidential, private, or identifying information about themselves or others into AI tools without express permission from a staff member. This includes names, images, voices, medical information, school records, private conversations, or any information that could identify another person.

AI dictation, transcription, recording, or note-taking tools must not be used to record, transcribe, summarise, or process lessons, conversations, meetings, or school activities without express permission from a staff member. Permission must be specific to the use proposed, and any staff member or student whose voice, image, words, or personal information may be captured must be made aware in advance. This applies even where the tool does not save an audio recording, as the spoken content may still be processed as personal data.

Staff introducing AI tools for student use should consider whether the tool is appropriate for the age and needs of students, whether it requires student accounts or personal data, and whether its use is consistent with the school's Data Protection Policy and school procedures.

The school will promote digital literacy, critical thinking, and responsible AI use through relevant curriculum areas, guidance, and staff professional learning where appropriate.

23. Consequences and Recording

Misuse of devices, the internet, school accounts, digital platforms, AI tools, social media, or other digital technologies will be addressed in accordance with the school's Code of Ethics and Behaviour and, where appropriate, the Bí Cineálta Anti-Bullying Policy, Child Safeguarding Statement, Data Protection Policy, Social Media Policy, Personal Mobile Device Usage Policy, and other relevant policies.

Incidents may be recorded using school systems to support consistency, identify repeated patterns of misuse, and inform appropriate follow-up by teachers, Year Heads, Deputy Principals or the Principal. Repeated misuse may lead to sanctions or interventions under the Code of Ethics and Behaviour.

Access to school accounts, school-managed devices, digital platforms, or network services may be restricted, suspended, or withdrawn where misuse occurs, in line with the school's Code of Ethics and Behaviour.

Depending on the nature of the incident, the school may contact parents/guardians, restrict access to school systems, temporarily confiscate devices, require restorative or educational follow-up, refer the matter to the Designated Liaison Person, and/or report illegal activity to An Garda Síochána or other relevant authorities.

24. Legislation and Support Structures

The school will provide or signpost information, as appropriate, on relevant legislation and support structures relating to internet safety and digital technology. Relevant legislation includes, but is not limited to:

- Data Protection Acts 1988 to 2018 and the General Data Protection Regulation (GDPR);
- Copyright and Related Rights Act 2000;
- Children First Act 2015;
- Criminal Law (Sexual Offences) Act 2017;
- Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law);
- Criminal Damage Act 1991;
- other legislation relevant to child safeguarding, privacy, harmful communications, online safety, copyright, cybercrime or digital technology.

The school will also inform students and parents/guardians, as appropriate, of key support structures and organisations that deal with illegal material, harmful online behaviour, cyberbullying, online safety, digital wellbeing, and responsible use of technology.

25. AUP Agreement Form

Student Agreement

I have read and agree to follow the school's Acceptable Use Policy. I understand that I must use the internet, school accounts, devices, digital platforms, artificial intelligence tools, and other digital technologies in a safe, respectful, responsible, and school-appropriate way. I understand that misuse may be addressed under the school's Code of Ethics and Behaviour.

Student Name: _____

Class/Year: _____

Student Signature: _____ Date: _____

Parent/Guardian Agreement

I have read the Acceptable Use Policy and understand that internet access, digital platforms, school accounts, and school-managed devices are provided for educational purposes. I understand that the school uses filtering and monitoring systems to support safe and appropriate use, but that no system can guarantee that students will never access unsuitable material.

I understand that school-managed devices and school accounts may be subject to filtering and monitoring during designated school use, and that responsibility for supervision of device use outside school hours rests with parents/guardians.

I understand that misuse of digital technology may be addressed under the school's Code of Ethics and Behaviour and other relevant school policies. I also understand that the publication of student work, images, audio or video will be managed in accordance with the school's Data Protection Policy, Social Media Policy and consent procedures.

Parent/Guardian Name: _____

Parent/Guardian Signature: _____ Date: _____

26. Ratification

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

Signed:  _____

Dónal Cronin

Chairperson - Board of Management

Signed:  _____

Niall Ahern

Principal

Document History:

Appendix 1 – SEN Provided Devices

The SEN Department will liaise with the Department of Education & Skills and the NCSE to secure and facilitate personal equipment (such as laptop computers) for eligible students with individual needs and learning differences to enhance curricular access.

OWNERSHIP AND USAGE:

- SEN laptops / iPads / Tablets are the property of Midleton CBS Secondary School and must be returned to the school when the student finishes his education, together with charger, carrying case and any other accessories provided by the school.
- Parents/guardians must sign the SEN Electronic Device Acceptable Use Policy before the device is taken from the school.
- The devices are strictly to be used for school-related purposes.
- Students are not permitted to lend or trade their device to anyone else.
- Devices should be in a student's possession, or secured in a designated secure area (e.g. the school office or at home) at all times. The safety of the device is the responsibility of the student.
- Students are expected to treat these devices and accessories with care and respect. Students are advised not to leave their laptops plugged in all the time, but rather to charge battery to 100%, unplug and use, and recharge when battery levels are low. This will help guard the battery life span.
- Students should not deface the device or its carrying case in any way.
- Students are not permitted to add or change the hardware, memory, or hard drive; students are not permitted to download personal programs / apps, inappropriate material, illegal content etc. onto the device; students should not interfere with device management or security system software, including, but not limited to, antivirus; students may not host any web pages, ftp hosting etc. on their laptop.
- If devices are used with Internet access at home, it is the responsibility of parents/guardians to monitor safe and appropriate internet usage.

INSURANCE:

- Once the device leaves the school, it is no longer covered by school insurance. As such, Midleton CBS Secondary School strongly advises parents/guardians to include the device on their own house insurance. Any loss or damage to the laptop will have to be met by parents/guardians.

PASSWORDS:

- Students are not permitted to change the password on their device.

PRINTING OF HOMEWORK:

- If students are using devices to do homework / research at home, it is the responsibility of the student to print their own work on their home printer, or email work to teacher prior to coming to school.

IN-SCHOOL USAGE:

- The devices must be brought to school daily, with the battery fully charged. In some cases, students may be specifically advised to only use devices at home for homework purposes by the SEN Department.
- Where appropriate, students will be encouraged to use devices for in-house assessments – the printing of these assessments will be arranged in school by a member of the SEN Department.
- Students may use devices in class to take down notes when appropriate, and in consultation with their subject teacher. Students need to ensure health and safety procedures are met when plugging in cables.

MEMORY KEY:

- Students may only use memory key with school computers with permission of teacher.

E-BOOKS:

- Students will still need to purchase a hard copy of their school books. Some publishers require receipts for books bought before they will issue E-books. Although the school will aim to help with the provision of E-Books, the primary responsibility for arranging E-books for the student on their devices lies with the parents / guardians.
- Students are strongly advised to spend time daily practicing their typing skills at home, to develop their proficiency with typing, particularly students who wish to use a Word Processor for their State Exams.

Middleton CBS Secondary School reserves the right to monitor or access the hard drives of its SEN devices.

I have read and understood this SEN Acceptable Use Policy and agree to abide by it:

Student Printed Name _____

Student Signature _____

Date _____

I have read and discussed this Acceptable Use Policy with my child:

Parent / Guardian Printed Name _____

Parent / Guardian Signature _____

Date _____

Appendix 2 – Care of Devices

Please read the following instructions carefully.

- Laptops can be fragile, and if they are dropped, even if in their carrying case, they may break.
- Laptops should only be used while they are on a flat, stable surface such as a table.
- When transporting the laptop to and from school, students should be particularly
- cautious.
- Laptops should not be left in a car, even if the car is locked.
- The laptop should either be turned off or in "sleep" mode when placed in the carrying case.
- Laptops should not be placed on or under soft items, such as pillows, chairs, or sofa cushions, or blankets. This will cause the laptop to overheat, and will result in damage to the laptop.
- Do not leave the laptop exposed to direct sunlight or near any heat or moisture sources for extended periods of time. Students should protect their laptop from extreme heat or cold.
- Students should never eat or drink (including water) while using their laptop, or use their laptop near others that are eating or drinking.
- No object should ever be placed or stacked on top of your laptop.
- Students should use care when plugging in their power cord, USB drive and when using their CD ROM drive.
- Laptops should be plugged at home to assure a full charge the following day in school. Laptops should not be plugged in constantly as this will weaken the life of the battery. Charge fully, then unplug and use as normal. Recharge when battery levels are low; do not wait for battery to fully discharge.
- Laptops should be shut down completely when not in use. All students should ensure that correct procedures are followed when shutting down and that the laptop is fully switched off.
- When not in use, the laptops should be stored in their carrying case, along with charger and any other accessories provided.
- Students are advised to back up their own work, either on a memory key or cloud storage.
- The password for each laptop will be set by the school and students are not to change this password.
- Students are not allowed to add or change the hardware, memory, or hard drive.
- As always, students should limit the personal information on the laptop for safety reasons.
- If the computer is lost or stolen, students and/or parents or guardians should immediately report the loss or theft to the School.
- Check for necessary Windows updates on a regular basis and ensure anti-virus software is up-to-date and set to scan regularly.