E-Safety Policy

June 2023

Document title	E-Safety Policy
Status of policy	*Non-statutory guidance*
Author (name & role title)	*Craig Drummond*
Version number	V4
Date approved	June 2023
Approved by	Senior Leadership Team
Date of review	June 2024

Document history

Version	Date	Author	Note of revisions
V1	June 2020	RH/ND	
V2	November 2021	CD	Updated to reflect changes in KCSIE Sept 2021
V3	February 2022	CD	Updated to reflect changes in Behaviour Policy
V4	June 2023	CD	Updated to reflect changes to monitoring system

Heathermount School is owned and operated by Cavendish Education.

This policy is one of a series of school policies that, taken together, are designed to form a comprehensive statement of the school's aspiration to provide an outstanding education for each of its students and of the mechanisms and procedures in place to achieve this. Accordingly, this policy should be read alongside these policies. In particular, it should be read in conjunction with the policies covering equality and diversity, Health and Safety, safeguarding and child protection.

All of these policies have been written, not simply to meet statutory and other requirements, but to enable and evidence the work that the whole school is undertaking to ensure the implementation of its core value of building confidence and preparing students for life.

While this current policy document may be referred to elsewhere in Heathermount School documentation, including particulars of employment, it is non-contractual.

In the school's policies, unless the specific context requires otherwise, the word "parent" is used in terms of Section 576 of the Education Act 1996, which states that a 'parent', in relation to a child or young person, includes any person who is not a biological parent but who has parental responsibility, or who has care of the child. Department for Education guidance Understanding and dealing with issues relating to parental responsibility considers a 'parent' to include:

- all biological parents, whether they are married or not.
- any person who, although not a biological parent, has parental responsibility for a child or young person - this could be an adoptive parent, a step-parent, guardian or other relative
- any person who, although not a biological parent and does not have parental responsibility, has care of a child or young person.
- A person typically has care of a child or young person if they are the person with whom the child lives, either full or part time and who looks after the child, irrespective of what their biological or legal relationship is with the child.

The school employs the services of the following consulting companies to ensure regulatory compliance and the implementation of best practice:

- Peninsula BrightHR
- Peninsula BusinessSafe (Health and Safety)
- Atlantic Data (DBS)
- Educare (online CPD)

Heathermount School is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers, pupils and visitors to share this commitment.

All outcomes generated by this document must take account of and seek to contribute to safeguarding and promoting the welfare of children and young people at Heathermount School.

The policy documents of Heathermount School are revised and published periodically in good faith. They are inevitably subject to revision. On occasions a significant revision, although promulgated in school separately, may have to take effect between the re-publication of a set of policy documents. Care should therefore be taken to ensure, by consultation with the Senior Leadership Team, that the details of any policy document are still effectively current at a particular moment.

Contents

1. Rationale

New technologies have become integral to the lives of children and young people in today's society both in schools and in their lives outside school. The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone.

Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Children and young people should have an entitlement to safe Internet access at all times.

The requirement to ensure that children and young people are able to use the Internet and related communication technologies appropriately and safely are addressed as part of the wider duty of care to which all who work in schools are bound.

This policy should help to ensure safe and appropriate use.

The development and implementation of the E-Safety strategy should involve all the stakeholders in a student's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact with on the Internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video content
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:
    - consensual and non-consensual sharing of nude and semi-nude images and/or videos. As set out in UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people, 2020 (which provides detailed advice for schools and colleges) taking and sharing nude photographs of U18s is a criminal offence;
    - sharing of unwanted explicit content;
    - sexualised online bullying;
    - unwanted sexual comments and messages, including, on social media; and
    - sexual exploitation; coercion and threats (including online).

- Many of these risks reflect situations in the off-line world and it is essential that this policy is used in conjunction with other school policies (e.g., Safeguarding, Behaviour policies).
- As with all other risks, it is impossible to eliminate those risks completely. It is essential, through good educational provision, to build students' resilience to the risks.

- The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other E-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- Heathermount School has made investments over a number of years, both financially and physically, to ensure these technologies are available to all students. The benefits are perceived to "outweigh the risks." However, our school must, through this policy, ensure that we meet the statutory obligations to ensure that students are safe and are protected from potential harm, both within and outside school.
- All staff should be aware that technology is a significant component in many safeguarding and
- wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will
- take place concurrently via online channels and in daily life. Children can also abuse their peers online,
- and can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of
- indecent images, especially around chat groups, and the sharing of abusive images and pornography, or other sexualised harassment or violence to those who do not want to receive such content.
- KCSIE 2022 now recognises that abuse categories can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults or by another child or children.
- Child on child abuse is most likely to include, but may not be limited to:
- bullying (including cyberbullying, prejudice-based and discriminatory bullying)
- abuse in intimate personal relationships between peers
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm (this may include an online element which facilitates, threatens and/or encourages physical
- abuse)
- sexual violence, such as rape, assault by penetration and sexual assault; (this may include an online element which facilitates, threatens and/or encourages sexual violence); For further information about sexual violence see Annex B.
- sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
- consensual and non-consensual sharing of nudes and semi-nude images and or videos (also known as sexting or youth produced sexual imagery)
- upskirting, which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element).
- This policy is designed to be read in conjunction with the policies and documentation mentioned in section 29.

2. Scope of this policy

- This policy provides guidelines and working practices for the effective and safe use of the Internet, email and other communication technologies in the school for staff, governors, students, parents, carers and volunteers.

- This policy explains how we will provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce risks of the use of Internet and other communication technologies for education, personal and recreational use.

3. The role and responsibility of governors

- Stephen Aiano, Compliance Director at Cavendish Education is our nominated E safety Governor.
- The role of the E-Safety Governor will include three yearly meetings with the E-Safety Coordinator and team that incorporate:
  - monitoring of e-safety incidents
  - monitoring of e-safety action plan/documents/ policies
  - reporting to relevant Governors' committee / meeting
- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

4. The role and responsibility of the headteacher and senior leaders

- The Headteacher is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day-to-day responsibility for E-Safety will be delegated to the E-Safety Coordinator.
- The Headteacher/Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher/Senior Leaders must ensure that staff must be provided with online safety information and training at induction.

5. The role and responsibility of the E-Safety co-ordinator

- The E-Safety Coordinator takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies/documents.
- The E-Safety Coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- The E-Safety Coordinator provides at least an annual update training and advice for staff.
- The E-Safety Coordinator liaises with school's IT Engineer to identify, triage and resolve issues.
- The E-Safety Coordinator receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.
- E-safety coordinator informs the e-safety Governor and governing body three times a year via the Headteachers report about any issues, concerns or changes. 5.7. The E-Safety Coordinator reports to the Heathermount Safeguarding Team every other academic week.
- The E-Safety Coordinator collaborates and reviews the PSHE curriculum to ensure that E-Safety learning is an effective part of the curriculum across whole school.

6. The role and responsibility of technical staff

- The IT Engineer is responsible for ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- The IT Engineer is responsible for ensuring that the school meets the E-Safety technical requirements outlined by Southwest Grid for Learning (SWGfL).

- The IT Engineer is responsible for ensuring that the web filtering applied by the school's filtering policy is applied and updated on a regular basis.
- The IT Engineer is responsible for ensuring that he/she keeps up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant.
- The IT Engineer is responsible for ensuring that the use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Coordinator/ Senior Service Desk Technician for investigation/action/sanction.
- The IT Engineer is responsible for ensuring that monitoring software/systems are implemented and updated.

7. The role and responsibility of teaching and support staff

- Staff have an up-to-date awareness of E-Safety matters and of the current school E-Safety policy and practices.
- Staff report any suspected misuse or problem to the E-Safety Coordinator/ IT Engineer for investigation/action/sanction using the reporting system linked with the MY Concerns software.
- Digital communications with students are on a professional level and only carried out using official school systems only.
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- Staff ensure that students understand and follow the school E-Safety and acceptable use policy.
- Staff ensure students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Staff monitor IT activity in lessons and any extracurricular and extended school activities and manage its usage locally.
- Staff are aware of E-Safety issues related to the use of cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices.
- Where Internet use is pre-planned students are guided to sites staff check the suitability beforehand.
- Staff refer any E-Safety concerns using the My Concern platform.

8. The role and responsibility of students

Students are responsible for using the school IT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (NB for some students, e.g., KS1, it would be expected that parents/carers would sign on behalf of the students.)
Students should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Students need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- Students will be expected to know and understand school policies on the use of digital and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Students should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- Students will follow the school rules on personal devices.

9. The role and responsibility of parents/carers

- Parents / Carers play a crucial role in ensuring that their children understand the need to use the Internet /mobile devices in an appropriate way.
- The school will therefore take every opportunity to educate parents understand E-Safety issues through parents' evenings, newsletters, letters, website and information about national/local E-Safety campaigns/literature.
- Parents and carers will be responsible for endorsing (by signature) the Student Acceptable Use Policy.
- Parents and carers will be responsible for accessing the school website /VLE/on-line student/ student records in accordance with the relevant school Acceptable Use Policy.
- Parents and carers will be responsible for reporting any identified Cyber-bullying/Abuse to the school

10. E-safety and safeguarding

Safeguarding young people and equipping them with the skills and knowledge starts in Early Years and continues through to the end of KS5. The DFE (2023) recommend that the Online safety is embedded across the curriculum. E-Safety is a whole school approach, including working with parents, cross curricular content as well as being specifically taught across the Business Admin Studies (City & Guilds), ICT and Computer Science, PSHE curriculums.

Content, Contact, Conduct and Commerce are the four key areas covered (KCSIE 2022):

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, sexualised harassment/violence, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing

11.The filtering policy

- Heathermount School currently uses N-Sight RMM Dashboard. 'N-Sight' is a specialist developer and provider of Internet security and web filtering solutions and specialises in education.
- The IT Engineer and the Cavendish IT team is responsible for the school's management of this software providing information on request for the school leadership team.
- If and when the filtering parameters will need to be changed (for educational purposes) the IT Engineer seeks approval from the E-Safety Coordinator or other Senior Leader before implementing this request.
- The E-Safety Coordinator and IT Engineer will, on occasions, differentiate the parameters to suit the age group and the student special educational needs.
- The IT Engineer and Cavendish IT should work closely with the E-Safety Co-ordinator to ensure that technological solutions are implemented which support good internet safety in normal classroom practices.

- See Appendix 8 for the current filtering policy (using N-Sight software). This policy is renewed once a year by Cavendish IT and the Safeguarding Team.

12.Managing internet access information system security

- The school IT system security will be formally reviewed periodically as necessary by the school's Safeguarding Team and IT engineer.
- Virus protection is installed and updated continuously throughout the working week.
- 'Safe-Search' is activated on all student accounts and browsers.

13. Data protection

- Heathermount School is required to keep and process personal information about its staff members and pupils in accordance with its legal obligations under the GDPR.
- The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and Children's Services.
- A policy is in place under Cavendish Education as a whole to ensure all staff and governors are aware of their responsibilities and outlines how the trust complies with the core principles of Data Protection and GDPR.
- The school employs the services of SchoolPro to help support Data Protection, GDPR compliance and staff training.
- Organisational methods for keeping data secure are imperative, and Heathermount School believes that it is good practice to ensure policies are practical, backed up by clear written procedures.
- Please refer to the Cavendish Data protection policy for further information. This policy complies with the requirements set out in the GDPR, which came into effect in May 2018.

14. Unsuitable/inappropriate activities

Heathermount School believes that the activities listed below would be inappropriate in a school context and users should not engage in these activities in school or outside school when using school equipment or systems.

Users shall not make, post, download, upload, data transfer, communicate or pass on material, remarks proposals or comments from the Internet that contain or relate to:

- child sexual abuse images
- promotion of or participation in illegal acts, e.g., under the Safeguarding and Child Protection Policy
- obscenity
- Computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- 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 and/or Cavendish Education into disrepute
- using school systems to run a private business
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards 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 gambling
- online shopping except when it is essential for the purchase of school resources
- using social networking sites
- sexual comments, such as: telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance and calling someone sexualised names;
- sexual "jokes" or taunting;
- physical behaviour, such as: deliberately brushing against someone, interfering with someone's clothes (schools and colleges should be considering when any of this crosses a line into sexual violence - it is important to talk to and consider the experience of the victim) and displaying pictures, photos or drawings of a sexual nature; and
- online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence.
- unwanted sexual comments and messages, including, on social media; and
- sexual exploitation; coercion and threats.

15.Responding to incidents of misuse

- All members of the school community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:
- If any apparent or actual misuse appears to involve illegal activity (eg child sexual abuse images or adult material which potentially breaches the Obscene Publications Act), the flowchart (see Appendix 1) should be consulted and actions followed.
- If a member of staff suspects that misuse might have taken place, but that the misuse is not illegal (as above) it must be reported using SchoolPod behaviour log and My Concerns.
- Once logged, an email alert will be sent to all members of the safeguarding team and triaged accordingly.
- The IT Engineer, E-Safety Coordinator, Designated Safeguarding Lead (DSL), Headteacher or the Deputy Designated Safeguarding Lead (DDSL) will be responsible for the event to be appropriately investigated.
- If a student suspects that misuse might have taken place, they should report this to the class teacher, E-Safety Coordinator, Designated Safeguarding Lead (DSL) or one of the Deputy Designated Safeguarding Leads (DDSL).
- If a concern around misuse by staff is raised, this should be taken directly to the Headteacher. If a concern is raised regarding the headteacher, this will be reported to Stephen Aiano, Compliance Director of Cavendish Education.
- It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.
- It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

16.Use of digital and video images – photographic, video

- The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the Internet.
- Staff and students need to be aware of the risks associated with sharing images and with posting digital images on the Internet.
- Images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term.
- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g., on social networking sites.
- Staff are allowed to take digital/video images to support educational aims. However, these images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals, the school or Cavendish Education into disrepute.
- Whilst in school, students must not take, use, share, publish or distribute images of others without staff permission.
- Photographs published on the website or elsewhere, that include students, are carefully selected and comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.
- Students' work can only be published with the permission of the student and parents or carers.

17.Teaching and learning – classroom practice

- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.
- Internet use will enhance and extend learning.
- The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of students if required to do so.
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.
- Students will be taught how to evaluate Internet content.
- The school will ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

18. PSHE curriculum and e-safety

- Staff should reinforce E-Safety messages in the use of IT across the whole curriculum especially in lessons where Internet use is pre-planned. Students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

- Staff should reinforce E-Safety messages in the use of IT across the whole curriculum especially where students are allowed to freely search the Internet, e.g., using search engines, staff should be vigilant in monitoring the content of the websites visited by the students.
- From time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, and discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the Senior Service Technician, E-Safety Coordinator or ICT technician can temporarily remove those sites from the filtered list for the period of time (see section for more details).
- PSHE is the curriculum element of safeguarding. In line with current guidance E-Safety knowledge and skill development is taught from Early years through to KS5. Core skills are developed throughout the PSHE curriculum as well as the development of age-appropriate knowledge and understanding across:
    - Content: being exposed to illegal, inappropriate or harmful material
    - Contact: being subjected to harmful online interaction with other users
    - Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
    - Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
- All students explore key concepts such as Managing Risk, Identity (including online), Power (including others connected to online), Rights and Responsibilities and Peer on Peer Abuse which include positive behaviour and how to report concerns. The DFE (2019) recommend that online safety be embedded across the curriculum. The PSHE SOW is available via the website to evidence how our PSHE curriculum supports Primary and Secondary students safeguarding and the internet. This document highlights how the learning is embedded.

19.E-mail

- Students may only use their own approved school e-mail account when working on school business.
- Students must immediately inform a teacher if they receive an e-mail that upsets them/makes them feel uncomfortable.
- In e-mail communication, students must not reveal their personal details or those of others or arrange to meet anyone without specific permission.

20.Published content and the school website

- Staff or student personal contact information will not be published.
- The contact details given online should be the school office or the professional email and extension within the school.
- The Headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

21.Social networking and personal publishing

- At present Heathermount School has its own specific and controlled Vimeo channel to upload documentation for families. These videos can be password protected where required.
- Social networking sites, forums and newsgroups will be blocked unless a specific use is approved.
- The school will consider how to educate students in their safe use. Students will be advised never to give out personal details of any kind which may identify them, their friends or their location and not place personal photos on any social network space without considering how the photo could be used now or in the future.

- Students should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.

22.Managing video conferencing

At present Heathermount School uses Microsoft Teams to communicate via video conferencing.

23.Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The school notes that technologies such as mobile phones with wireless Internet access (3G, 4G, 5G) can bypass school filtering systems and present a new route to undesirable material and communications.
- Heathermount has a no personal device and mobile phone student policy. However, we appreciate that under certain circumstances our students use the music facility on school approved devices with no data access to help regulate.
- Personal devices are only permitted for students to use on external trips when agreed by all parties.
- The sending of abusive or inappropriate text messages and misuse of camera phones are forbidden.

24.Policy decisions

- When authorising Internet access, the school will maintain a current record of all staff and students who are granted access to school IT systems.
- When authorising Internet access, all student, staff and families must agree to comply with the Acceptable User Agreement.

25.Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material.
- It is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.

26.Communicating e-safety

- E-safety rules will be posted on the website and in relevant learning areas.
- Students will be informed that network and Internet use will be monitored at all times.
- Links, available E safety packs and online training is updated and reviewed and posted on the school website. Families are signposted to it throughout the school year.
- The School Council will take an active role in educating students within the school community.
- All staff will be given access to the School E-Safety Policy and its importance. A copy will be put in the relevant folder within the school's computer system.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor IT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

- Under no circumstances are staff to have students as 'friends' on social networking sites, current or ex-students.
- Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters and on the school website.
- The school will maintain a list of E-Safety resources for parents/carers.
- Parents and carers must countersign the Acceptable user agreement for all students at Heathermount.

27.Equal opportunities

The school supports the right of all staff and students to equal access and chances regardless of age, ethnicity, gender, social circumstances, ability/ disability or sexuality.

28.Health and safety

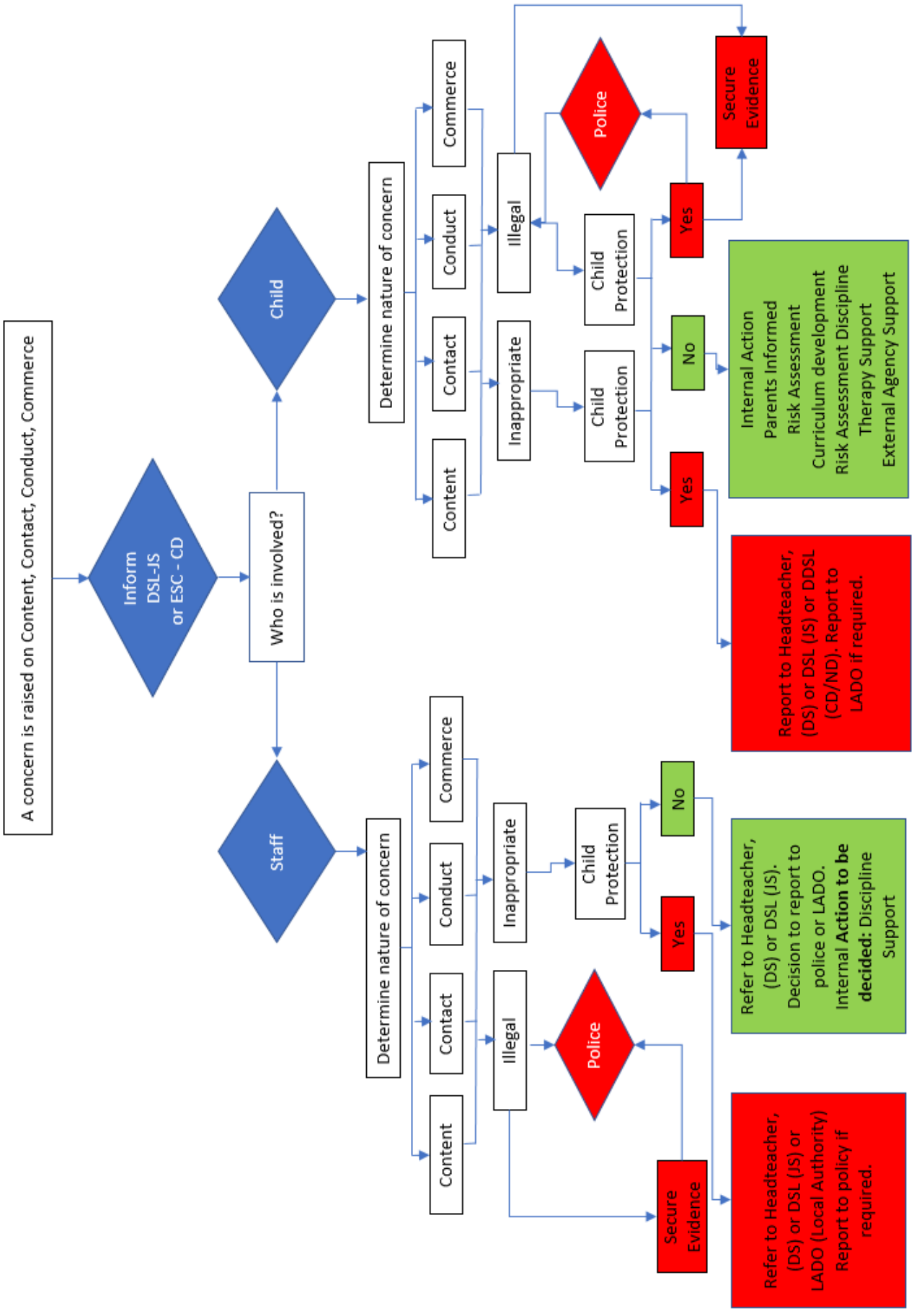
Health and Safety issues are described fully in the School Health and Safety Policy. It is the responsibility of each adult to report health and safety issues without delay.

29.Related policy and supporting legislation and guidance

This policy is written with due regard and in line with related policies including:

- Safeguarding & Child Protection Policy April 2023
- RSE Policy (Relationship, Sex education) April 2023
- Anti- bullying Policy Jan 2023
- Behaviour Policy June2023
- Staff Code of conduct May 2018 (under review)
- Curriculum policy June2021
- Staff Handbook/Staff Induction handbook
- Mental Health & Wellbeing Policy September 2022
- School Health and Safety Policy January 2023
- Heathermount Student, Staff & Family acceptable IT Use agreement
- Guidance on teaching online safety in School: https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

Appendix 1: Responding to incidents of misuse – flow chart



Appendix 2
Heathermount School acceptable use policy - primary students and parents

Student Name: _____

Our school promotes the use of technology in school as all students will need the skills and knowledge in whatever field of work they enter when they become an adult. We ensure that our school IT network is robust and resilient, and we do our upmost to ensure the safety of children when using it. It is important that students abide by the school rules when using technology in school and inform a member of staff immediately, if they become aware of any misuse.

This is the Acceptable User Policy (AUP) for our school. It highlights the do's/don'ts of using all technology in school and shows how we want students to behave when using IT. Any misuse will result in students being temporarily banned from using the school network.

Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form, you will not be able to use the IT systems in school.

For Students using Technology in School:

- I will only use the school Internet and network for my schoolwork or when a teacher has given permission.
- I will not try and bypass the schools VLE or Internet settings.
- I will only use my school email address when using email in school. I will always log off my email account when finished
- I will not look at, change or delete other people's work or files.
- I will be careful with keyboards, mice, headphones and all other equipment, and when turning a computer on or off.
- I will be sensible when using mobile technologies and follow the rules about moving about the school when using them.
- I will follow the rules about bringing my own personal device into school e.g. smartphone and/or smartwatch.

Security, Passwords and Copyright

- I will not share my Internet or network passwords. I will also create a password which uses capital and lower-case letters, numbers and symbols.
- I will be careful when opening emails from people I don't know, and I will ask an adult if I'm unsure whether to open it.
- I won't upload or download any pictures, writing or movies which might upset people or make other people think the school is a bad place.
- I will use non-copyrighted images and music from the Internet when creating documents, presentations or other media.
- I won't try to install software onto the school network because it might have a virus on and cause a lot of damage. Instead I will ask a teacher for advice.

Online Behaviour and Safety

- I won't give out my personal details, such as my name, address, school or phone number on the Internet or when registering for a software app.
- I won't meet people I've met on the Internet unless I have told my parents and they come with me.
- I will make sure all my contact with other people at school is responsible. I will not cyber bully students, teachers or other members of staff.
- I won't look for or look at unpleasant or inappropriate web sites or software apps. I will check with a teacher if I think it might be unsuitable.
- I know that everything I do on the computers at school is recorded and that the school can talk to my parents if a teacher is worried about my online safety.
- I will try to follow these rules all the time because I know they are designed to keep me safe.

For Parents:

- I agree to support and uphold the principles of this policy in relation to my child and their use of technology and the Internet, at home and at school.
- I agree to uphold the principles of this policy in relation to my own use of the Internet, when that use is related to the school, employees of the school and other students at the school.
- Images of students will only be taken, stored and used for school purposes in line with school policy. Images will only be used on the Internet, in the press, or in media, with permission.

Signed: Student: _____

Date: _____

Signed: Parent/Guardian: _____

Date: _____

Appendix 3
Heathermount School acceptable use policy - secondary students and parents

Student name: _____

Our school promotes the use of technology in school as all students will need the skills and knowledge in whatever field of work they enter when they become an adult. We ensure that our school IT network is robust and resilient and we do our upmost to ensure the safety of children when using it. It is important that students abide by the school rules when using technology in school and inform a member of staff immediately, if they become aware of any misuse.

This is the Acceptable User Policy (AUP) for our school. It highlights the do's/don'ts of using all technology in school and shows how we want students to behave when using IT. Any misuse will result in students being temporarily banned from using the school network. In addition, the AUP covers the following legislation:

- Keeping Children Safe in Education (2022)
- Malicious Communications Act
- GDPR 2018
- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Sexual Offences Act 2003

Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form you will not be able to use the IT systems in school.

For Students:
Using Technology in Schools

- I will only use school Internet, IT facilities and mobile technologies for educational purposes which follow the teachers' instructions. This includes email, video, messaging, videoconferencing, using software apps, social media, Internet, file-saving and printing.
- I will only use my mobile phone, mobile device or smartwatch in school when permission has been granted by a teacher. If permission is granted, I will use my mobile device in line with how I would use other technology in school.
- I will not look at or delete or amend other people's work or files.
- I will treat all IT equipment at school with respect and ensure the computer or mobile device is left in the state that I found it.

Security, Passwords & Copyright

- I will not install software on school IT facilities due to the risk of damage being caused by malware or viruses. I will ask an ICT teacher or technician to install software if required.
- I will only install software apps on mobile devices when directed to by a teacher. I will only use school-related information when registering for an app.
- I will not share my network, Internet or any other school-related passwords.
- I will change my passwords when asked to and ensure that they have complexity e.g. Capital, lower case letters, numbers and symbols.
- I will only use my school-supplied email address for school-related activities.
- I will respect copyright when making use of images, videos or other media in my schoolwork. I will use and attribute 'Creative Commons' material as taught in ICT/e-safety lessons.
- I will follow the school procedures when using removable media e.g. flash drives to ensure that I don't infect any machines.
- I will not look for ways to bypass the school filtering, monitoring or proxy service.
- I will not bypass the school filtering, monitoring or proxy service.

Online Behaviour & Safety

- I will make sure all my contact with other people at school is responsible. I will not cyber bully students, teachers or other members of staff.
- I will be responsible and polite when I talk online to students, teachers and other people related to the school, both in school-time and outside school-time.
- I won't look for or look at unpleasant, unsuitable or extremist websites in school. I will check with a teacher if I think a website might be unsuitable.
- I won't give out my personal details, such as my name, address, school or phone number on the Internet.
- I won't meet people I've met on the Internet unless I have told my parents and they come with me.
- I won't upload or download any pictures, writing or films which might upset people online.
- I won't write unpleasant, rude or untrue comments online about students, teachers or other staff employed by the school.
- I won't share inappropriate images or videos of other students on the school network or personal devices.
- I am aware that everything I do on the computers at school is monitored and logged, and that the school can talk to my parents if a teacher is concerned about my online safety or my behaviour when using school computers.
- I will not look for, view, upload or download offensive, illegal, copyright-infringing or pornographic material. If I find such material on school, IT equipment I will inform a teacher immediately.
- I understand that these rules are designed to keep me safe and that if they are not followed, sanctions may be applied, and my parent/guardian may be contacted.

For parents:

- I agree to support and uphold the principles of this policy in relation to my child and their use of the Internet, at home and at school.
- I agree to uphold the principles of this policy in relation to my own use of the Internet, when that use is related to the school, employees of the school and other students at the school.
- Images of students will only be taken, stored and used for school purposes in line with school policy. Images will only be used on the Internet or in the media with permission.

Student:_____ Date:

Parent/Guardian_____ Date:

Appendix 4
Heathermount School acceptable use agreement: staff, governors and visitors

ICT (including data) and the related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school E-Safety coordinator or Child Protection Officer (Designated Safeguarding Lead).

- I will only use the school's email/Internet/Intranet Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- will not give out my own personal details, such as mobile phone number and personal e-mail address, to students.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the ICT Technician and/or the E-Safety Coordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature……Date ……

Full Name …….. (printed)

Job title ……