Online Policy

Prepared by: The Central Team
Date: July 2025
Version: V1

CONTENTS

1. Introduction

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 values.

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 updated August 2023, 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 contracts the services of third-party organisations to ensure regulatory compliance and implement best practices for:

- HR and Employment Law
- Health & Safety Guidance
- DBS Check processing
- Mandatory Safeguarding, Health & Safety, and other relevant training
- Data protection and GDPR guidance
- Specialist insurance cover

Where this policy refers to 'employees', the term refers to any individual who is classified as an employee or a worker, working with and on behalf of the school (including volunteers and contractors).

The 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 republication 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.

2. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism (All schools and colleges are subject to the **Prevent Duty** under the Counter-Terrorism and Security Act 2015)
- Contact – being subjected to harmful online interaction with other users, such as 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, radicalisation, abuse and trafficking, financial or other purposes as well as bullying and cyberbullying. Sexual exploitation (CSE).
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as 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, harassment, and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

3. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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 headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE'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 cyberbullying by, if necessary, searching for and deleting inappropriate images or files on pupils' 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.

4. Roles and responsibilities

The Board of Directors
The Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Board will coordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

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

All Local Governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the school. The headteacher will inform the governing body three times a year via the Headteacher's report regarding online concerns, system alerts, or relevant policy updates.

The Designated Safeguarding Lead (DSL)

In line with KCSIE, the DSL holds ultimate operational accountability for the school's filtering and monitoring systems. The DSL ensures that safeguarding workflows are seamlessly integrated with technical alerts, reviews logging data, oversees filtering configuration changes, and ensures all online safety interventions are handled under child protection frameworks.

The Online Safety Co-ordinator (working within the DSL team)

Details of the school's Designated Safeguarding Lead (DSL), Online Safety Co-ordinator, and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The Online Safety Co-ordinator (who is DSL-trained) works within the DSL team and takes lead operational responsibility for online safety in school while reporting directly to the DSL. The Online Safety Co-ordinator must report to the Safeguarding Team every other academic week to maintain regular oversight of potential risks. Responsibilities include:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the operational lead on understanding and managing the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and are reviewed regularly
- Working with the IT Technician and Cavendish Network team to make sure the appropriate systems and processes are in place
- Working with the headteacher, IT Technician, and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring software
- Ensuring that any online safety incidents are logged 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

<u>The IT Technician (working with the eSafety Co-ordinator)</u>
The IT Technician is responsible for:

- Deploying and maintaining appropriate security protection procedures, specifically managing Smoothwall for network-level filtering and keyword detection, and Classroom Cloud to conduct classroom-level keyword detection and monitor student laptops during lessons. These provisions are reviewed and updated at least annually to assess effectiveness.
- Ensuring that the school's ICT infrastructure meets the technical requirements outlined by the Southwest Grid for Learning (SWGFL) and UKSIC, and remains secure against viruses and malware.
- Ensuring that when inappropriate sites are accessed or concerning keywords are flagged by Smoothwall or Classroom Cloud, an automatic alert email is sent instantly to the Online Safety Co-ordinator, DSL, and Headteacher.
- Conducting a full technical security check and monitoring the school's ICT systems on a termly basis.
- Blocking access to potentially dangerous sites and preventing the downloading of malicious files.

<u>All staff and volunteers</u>
All staff, including contractors, agency staff, and volunteers, are responsible for:

- Maintaining a complete understanding of this policy and implementing it consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2), and ensuring that pupils follow their terms on acceptable use.
- Knowing that the DSL retains ultimate accountability for the filtering and monitoring systems, and knowing how to report failures in those systems by notifying the Online Safety Co-ordinator, IT Technician, and Safeguarding team immediately.
- Following correct procedures by making the Online Safety Co-ordinator and IT Technician aware if they need to bypass filtering systems for legitimate educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged 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.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, maintaining an attitude of 'it could happen here'.

Parents/carers
Parents/carers are expected to:

- Notify a member of staff or the headteacher 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)

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

- What are the issues? – UK Safer Internet Centre
- Online safety topics for parents/carers – Childnet
- Parent resource sheet – Childnet

Visitors and members of the community
Visitors and members of the community who use the school's ICT systems or the internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms of acceptable use (appendix 2).

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum during ICT lessons, PSHE lessons, Internet safety days and assemblies.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In Key Stage (KS) 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage (KS) 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others, and know how to recognise and display respectful behaviour online, and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

In KS3, pupils 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

Pupils in KS4 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, pupils 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 to be shared further, and not to share personal material that 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 that 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
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse, and pupils with SEND, using a personalized or contextualized approach.

6. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications at home, via our website, via parent information evenings , and during Parent Forums.

The school will let parents/carers know:

- What systems the school use to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with their class tutor and/or the eSafety Co-ordinator/DSL team.

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

7. Cyber-bullying

Definition
Cyberbullying 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

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

The school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyberbullying with their tutor groups and it will also be discussed during anti-bullying week in assemblies..

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyberbullying to parents/carers so 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 cyberbullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining Electronic Devices
The headteacher and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- There is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Safeguarding Team.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

Staff members do not have the authority to delete files or data independently from a student's device.

If the material is suspected to be evidence relating to an offense, staff must not delete or alter the material under any circumstances. The device must be preserved exactly as found and handed to the police by the DSL as soon as reasonably practicable. The DSL will manage the incident in strict alignment with DfE's *Screening, Searching and Confiscation* advice and UKCIS *Sharing Nudes and Semi-Nudes* guidelines.

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they must:

- Do not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:
- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy
- Searches, and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

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 Gemini.

Heathermount 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.

Heathermount School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying/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 school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

Any use of Artificial Intelligence should be carried out in accordance with our AI usage policy

8. Acceptable use of the Internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the Internet (appendices 1 to 2). Visitors will be expected to read and agree to the school's terms of acceptable use if relevant.

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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate. We monitor websites visited via Smoothwall network filtering and track in-lesson activity via Classroom Cloud.

More information is set out in the acceptable use agreements in Appendices 1 to 2.

9. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day. They are to be placed in the device box before they come into the school, once they leave their transport to school. Devices are then collected from the box at the end of the day. The exception to this is if they are going out on a trip for all or part of the day, pupils may be given permission to keep and use their devices whilst on the trip. It is up to the trip leader to decide if they would like the pupils to have their devices on the trip.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendices 1 and 2).

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

10. Staff using work devices outside of school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of three random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in Appendix 2.

Work devices must be used solely for work activities.
If staff have any concerns over the security of their device, they must seek advice from The IT Technician.

11. How will the school respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. 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 ICT systems or the internet or misuses a personal device, where the action constitutes misconduct, the matter will be dealt with in accordance with the Employer handbook 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

Staff, local governors and volunteers
All new staff members will receive training, as part of their induction, on safe internet use.
Online safeguarding issues, including cyberbullying 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, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and well-being issues, and children are at risk of online abuse

  Children can abuse their peers online through:

- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography with those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing-type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies 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.

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

Volunteers will receive appropriate training and updates, if applicable.

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

Pupils
All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security

- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use agreement

Contact Information

For any questions or concerns regarding this policy, please contact Jax Snipp - jax.snipp@heathermount.co.uk

Approval & Policy Review

This Policy has been reviewed and approved by:

Policy Approver(s)	Cavendish Education Board of Directors/Senior Leadership Team of the school
Storage Location	Online, hard copy in the schools online drive
Effective Date	July 2025
Next Review Date	July 2026

Revision History

Version	Change	Author	Date of Change
1	First published	Cavendish Central Team	July 2025
2	Updated procedures	Heathermount SLT (JSn)	July 2026

Appendix 1: acceptable use agreement (pupils and parents/carers)

Heathermount School Acceptable User Agreement -

pupils and parents

Pupil name: _____

Our school promotes the use of technology in school as all pupils 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 utmost to ensure the safety of children when using it. It is important that pupils 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 Agreement (AUA) for our school. It highlights the do's/don'ts of using all technology in school and shows how we want pupils to behave when using IT. Any misuse will result in pupils 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 Pupils:

Using Technology in School

- I will only use the school Internet and network for my school work 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 & 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 & 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 pupils, 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 pupils 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 - Pupil: _____

Date: _____

Signed - Parent/Guardian: _____

Date: _____

Appendix 2: acceptable use agreement (contractors, agency staff, and volunteers)

Heathermount School Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This Acceptable Use Agreement is intended to ensure:

- that staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- that school ICT systems and users are protected from accidental or deliberate misuse.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement
I understand that I must use school ICT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of its ICT systems including email and other digital communications technologies. This may include but not be limited to the following circumstances:
    - With software to monitor 'trigger' words or phrases for safeguarding and to ensure acceptable, professional use of IT.
    - When staff leave or are on long-term absence for retrieval or redirection of messages.
    - When a member of staff is under investigation or suspected of illegal, fraudulent, inappropriate or safeguarding activity.
    - To collect and review information contained in any electronic system for documented purposes and authorised by the Headteacher, or in their absence a member of the Senior Leadership Team, for example, to complete a Subject Access Request or similar.
- I understand that information and resources stored on the organisations equipment and drives should be considered to be controlled and accessible by the School and authorised staff.
- I understand that this agreement also applies to use of school ICT systems out of school (e.g. laptops, email, VLE etc). This includes my personal or work mobile phone or tablet if it contains my work email.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my usernames and passwords private and will not try to use anyone else's username and password.
- I will not share or continue to use any logins for any school service or platform when I leave my employment.
- I will return all school owned ICT equipment and delete all school data from my personal devices when I leave my employment.

I will immediately report any illegal, inappropriate or harmful material or incident, to the Head Teacher or other person appointed by the Head Teacher/DPO.

I will be professional in my communications and actions when using school ICT systems:

I will not access, copy, delete or otherwise alter any other user's files, without their permission.

I will communicate with others in a professional manner.

- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's Agreement. I will not use my personal equipment to record these images, unless I have permission to do so.

- Where these images are published (e.g. on the school website / VLE) it will not be possible to identify pupils by name, or other personal information.
- I will not use chat and social networking sites in school.
- I will only communicate with pupils and parents / carers using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will lock my screen or log off my computer should I leave it unattended.
- I will not allow a third party to access my work emails on my mobile phone or tablet

The school and the local authority have the responsibility to provide safe and secure access to technologies:

- When I use my personal handheld / external devices in school (PDAs / laptops / mobile phones / USB devices etc), I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. As far as I am able, I will ensure that when connecting these devices to school ICT systems, they are using up to date Operating Systems (e.g. latest versions of Android / iOS) and protected by up to date anti-virus software where applicable.
- I will not save any personal data to my personal computer.
- I will only use the recommended apps on my personal device for accessing data\emails via Office 365 or G-Suite.
- I will encrypt (Password Protect in most cases) my personal device if I use it to access school personal data or Office 365\G-Suite apps.
- I will inform the school's Head Teacher or other person appointed by the Head Teacher/DPO if my personal device e.g. phone or tablet is lost or stolen should it contain any school personal data.
- I will immediately report any Internet content that is not filtered that I suspect could be inappropriate.
- I will delete personal data according to the school's retention policy.
- I will not use personal email addresses for work-related purposes.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (eg child sexual abuse images, criminally racist material, adult pornography etc).
- I will not use any programmes or software that might allow me to bypass the filtering / security systems intended to prevent access to such materials.
- I will not install or attempt to install programmes of any type on school systems, nor will alter computer settings, unless this has been authorised.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where personal data is electronically transferred outside the secure school network, it must be encrypted.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

System Specific Guidelines & Procedures

Use of Electronic Whiteboards and Screen Sharing

- I understand that electronic whiteboards should be used in a manner that upholds the school's standards of professionalism and respect.
- I will ensure that any content displayed or written on electronic whiteboards during lessons or meetings is appropriate for the intended audience.

- I will not save or store sensitive information displayed on the whiteboard without the necessary permissions or safeguards in place.
- When using interactive features, I will ensure that student data and privacy are protected at all times.
- When sharing the screen of my device (laptop, tablet, work phone etc) to the electronic whiteboard, I will ensure that only the necessary applications or windows are visible to avoid unintentionally sharing sensitive or personal information. This also applies to screensharing during online remote lessons or meetings.
- I will be vigilant and ensure that any notifications or pop-ups that may contain personal or sensitive information are disabled before sharing my screen to the electronic whiteboard. This also applies to screen sharing during online remote lessons or meetings.
- I will ensure that any shared content displayed on the electronic whiteboard or shared during online remote lessons or meetings, upholds the school's standards of professionalism and respect.

School's Management Information System (MIS)

- I understand that the school's MIS contains sensitive data and information pertinent to the functioning of the school.
- I will only access the MIS with the appropriate permissions and for legitimate school-related purposes.
- I will not share my MIS login credentials with anyone and will ensure that I log out after each session.
- I will ensure that I do not display or share information from the MIS with individuals that are not authorised to access the data (for example, by displaying the MIS on classroom screens or electronic whiteboards).
- I will immediately report any suspected breaches or unauthorised access to the MIS to the school's IT department.
- I will use multi-factor authentication, where available, to enhance the security of my access to the MIS.

School's Safeguarding System (MyConcern)

- I acknowledge the sensitive nature of data within the school's safeguarding systems and will handle this information with utmost care and discretion.
- I will ensure that I only access these systems for legitimate safeguarding-related activities and will avoid unnecessary browsing or querying of data.
- I will not share my login credentials for safeguarding systems with anyone.
- I will ensure that I do not display or share information from the Safeguarding System with individuals that are not authorised to access the data (for example, by displaying the MIS on classroom screens or electronic whiteboards).
- Multi-factor authentication should be used when accessing these systems to ensure the highest level of security.
- Any suspected breaches, mishandling, or unauthorised access to these systems should be reported immediately to the designated safeguarding lead.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Signed: …….

Print name: …….

Date: …….