MOUNT

ST MARY'S | BARLBOROUGH HALL

E-Safety Policy

ISI Regulatory Code – 7h

Policy written by: Jack Murphy

Policy Date: September 2023

This Policy is for: Mount St Mary's College

Linked Policies: Safeguarding Policy, Anti-bullying Policy, PSHEE Policy, Behaviour Policy, Staff Code of Conduct

Review date: September 2024

Mount St Mary's College

Educating Men and Women for Others since 1842

Telephone: 01246 433388

Email: headmaster@msmcollege.com

Address: College Road, Spinkhill, Derbyshire, S21 3YL

Barlborough Hall School

Educating Men and Women for Others since 1842

Telephone: 01246 810511

Email: headteacher@barlboroughhallschool.com

Address: Barlborough Park, Chesterfield,S43 4ES

1. Aims

Online safety and the use of mobile technology

We recognise the importance of safeguarding children from potentially harmful and inappropriate online material, and we understand that technology is a significant component in many safeguarding and wellbeing issues.

To address this, our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Protect and educate the whole school community in its safe and responsible use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Set clear guidelines for the use of mobile phones for the whole school community
- Establish clear mechanisms to identify, intervene in and escalate any incidents or concerns, 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, anti-Semitism, radicalisation and extremism
- **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, financial or other purposes
- **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 and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

To meet our aims and address the risks above we will:

- Educate pupils about online safety as part of our curriculum. For example:
    - The safe use of social media, the internet and technology
    - Keeping personal information private
    - How to recognise unacceptable behaviour online
    - How to report any incidents of cyber-bullying, ensuring pupils are encouraged to do so, including where they are a witness rather than a victim
- Train staff, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year
- Educate parents/carers about online safety via communications sent directly to them. We will also share clear procedures with them so they know how to raise concerns about online safety

- Make sure staff are aware of any restrictions placed on them with regards to the use of their mobile phone and cameras, for example that:
    - Staff are allowed to bring their personal phones to school for their own use, but will limit such use to non-contact time when pupils are not present
    - Staff must complete the appropriate disclaimer in order to use their phone to take pictures of pupils for school purposes
- Make all pupils, parents/carers, staff, volunteers and governors aware that they are expected to sign an agreement regarding the acceptable use of the internet in school, use of the school's ICT systems and use of their mobile and smart technology
- Explain the sanctions we will use if a pupil is in breach of our policies on the acceptable use of the internet and mobile phones
- Make sure all staff, pupils and parents/carers are aware that staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation
- Put in place robust filtering and monitoring systems to limit children's exposure to the 4 key categories of risk (described above) from the school's IT systems
- Carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks faced by our school community

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Personal Social and Health Education Policy
- Searching, screening and confiscation
- Filtering and Monitoring

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

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

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and ensuring its implementation

All governors will:

- Ensure that 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 1)
- Online safety is a running and interrelated theme within the whole-school approach to safeguarding and related policies

3.2 The Second Master (DSL)

The Second Master:

- Is responsible for on-line safety and understanding the filtering and monitoring processes in place
- Is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Works with the, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- 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 headmaster and/or governing board

This list is not intended to be exhaustive.

3.4 The IT Engineer

The IT Engineer is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- 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

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Second Master 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

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

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

3.7 Visitors and members of the community

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

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 3**, 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 **Key Stage 4** will be taught:

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

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

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

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

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

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Second Master

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

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, 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 victim.

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

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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

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

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

6.3 Examining electronic devices

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

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

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

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

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in school

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

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them inside building during the school day, with the exception of 6th form students who may use their phones for educational purposes in the library or study rooms. A teacher may allow a student to use their phone for educational purposes during a lesson.

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.

9. Staff using work devices outside school

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

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

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

Work devices must be used solely for work activities.

10. How the school will 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 behaviour policy and pupil code of conduct.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 staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

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

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

The DSL 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.

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.

12. Monitoring arrangements

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

This policy will be reviewed every year by the Second Master. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Anti-Bullying Policy
- Child protection and safeguarding policy

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

14. Acceptable Use Agreement and Bring Your Own Device Policy

RULES FOR USE OF ICT

These rules are taken from the school's Acceptable Use Policy which is published on the College website.

Access to the Mount Trust IT systems is controlled by the use of Usernames and passwords and/or pin numbers. All Usernames and passwords are to be uniquely assigned to named users and consequently, users are accountable for all actions on the Mount Trust's IT systems.

Users must not:

- Allow anyone else to use their user ID/password or pin numbers.
- Leave their user accounts logged in at an unattended and unlocked computer
- Use someone else's user ID and password or pin to access Mount Trusts IT systems
- Leave their password or pin unprotected (for example writing it down).
- Perform any unauthorised changes to Mount Trusts IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-Mount Trust unauthorised device to the Mount Trust network or IT systems. (**Please read the BYOD Policy**)
- Store Mount Trust data on any non-authorised Mount Trust equipment.
- Give or transfer Mount Trust data or software to any person or organisation outside Mount Trust without the authority of Mount Trust.

Use of the Mount Trust internet services is intended for educational use. Personal use is permitted where such use does not affect the individual's performance, is not detrimental to Mount Trust in any way, not in breach of any term and condition in the parent contract and does not place the individual or Mount Trust in breach of statutory or other legal obligations. The IT department have implemented a

centralised firewall to block most known unwanted applications from all devices that connect to the Trust's network.

All users are accountable for their actions when using any internet services.

Users must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Mount Trust considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Mount Trust, alter any information about it, or express any opinion about Mount Trust, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward Mount Trust mail to personal (non-Mount Trust) email accounts (for example a personal Hotmail account).
- Make official commitments through the internet or email on behalf of Mount Trust unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (**not an exhaustive list**) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect Mount Trust devices to the internet using non-standard connections.

Software

Users must only use software that is authorised by Mount Trust on the Mount Trust computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Mount Trust computers must be approved and installed by the Mount Trust IT department.

Users must not:

- Store personal files such as music, video, photographs or games on Mount Trust IT equipment.

Viruses

The IT department has implemented centralised, automated virus detection and virus software updates within the Mount Trust. All Trust computers have antivirus software installed to detect and remove any virus automatically.

Users must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Mount Trust anti-virus software and procedures.

Monitoring and Filtering

All data that is created and stored on Mount Trust computers is the property of Mount Trust and there is no official provision for individual data privacy, however wherever possible Mount Trust will avoid opening personal emails. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Mount Trust has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 1998
- BYOD (Bring Your Own Device) Policy
- Social Media Acceptable Use Policy

The College allows users to access the Guest wireless network using their personal device (laptop, smart phone or tablet). This element of the Mount Trust's ICT provision is a privilege extended to individuals and as such there are rules associated with this Bring Your Own Device policy that, if misused or abused, will result in that privilege being taken away

Terms of Use

The College provides wireless connectivity as a guest service and offers no guarantees that any use of the wireless connection is in any way secure or that any privacy can be protected when using this wireless connection.

Use of the College's wireless network is entirely at the risk of the user and the Trust is not responsible for any loss of any information that may arise from the use of the wireless connection.

All users using the College's networks are bound by the College's ICT Acceptable Use Policy.

When a device connects to the wireless network, all users will have filtered internet access.

Use of the device in lesson time is entirely at the discretion of the teacher. If the teacher asks you not to use your device then you must follow those instructions.

The use of a personal device is not to be a distraction in any way to teachers or students. Personal devices must not disrupt class or Private Study areas in any way.

Users shall make no attempts to circumvent the Mount Trust's network security. This includes setting up proxies and downloading programs to bypass security.

The College has the right to take action against anyone involved in incidents of inappropriate behaviour, that are covered in this policy and other policies such as the Anti-Bullying and Cyber-Bullying Policy, whether on or off the Trusts premises.

Any failure to comply with this policy, will be subject to disciplinary action. This may include loss of access to the College's network / internet, detentions, suspensions, contact with parents and in the event of illegal activities, involvement of the police.

The College reserves the right to search the content of any mobile or devices on their premises where there is a reasonable suspicion that it may contain inappropriate material including, but not limited to, those which promote pornography, gambling, violence, bullying or discrimination of any form.