



**Montagu Academy**

Striving for excellence, broadening horizons

Montagu Academy	
E-Safeguarding Policy	

Date	Review Date	Lead
October 2016	October 2017	Judith Astwood/James Barker

Head teacher Signed	Date	Chair of Governors Signed	Date

## Rationale

In a rapidly changing technological world, internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. At Montagu Academy, we aim for pupils and staff to have access to the most up to date information, which beneficial for both teaching and learning. The vast majority of pupils at Montagu Academy have access to the internet at home and are encouraged to use educational sites out of school. When in school, our curriculum and teaching promotes a safe, responsible and positive use of digital technology.

## Purposes

To enable children to:

- Access world-wide educational resources including games, museums and up to date information.
- Access blogs and other platforms and use them effectively.
- Find enjoyment when learning through the incorporation of ICT.
- Learn how critically evaluate information and realise that not all print is true.
- Understand that email can be used as a modern way of communication.
- Understand and learn about the importance of e-safety.

## Guidelines

- When accessing the internet, the school uses an excellent filtering service put in place via the Doncaster filtering service.
- Parents are asked at the beginning of every academic year to sign a consent form to allow their child to use the internet in school.
- Pupils are taught, through clear guidelines, how to use the Internet safely and to recognise the difference between acceptable and unacceptable internet use. This is reflected through an Acceptable Use Agreement for using the Internet (*See Appendices*)
- Pupils will not be permitted to use the Internet without an adult regularly monitoring what they are accessing.
- Pupils are taught the skills to keep safe when accessing the internet through weekly computing sessions and weeks designated to focusing on the importance of e-safety.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing Co-Coordinator (James Barker)
- Pupils must reveal personal details of themselves or others in e-communication, such as address or telephone number, or arrange to meet anyone.
- The point of contact on the website is the school address, school admin e-mail and telephone number. Staff or pupils' home information will not be published.
- Pupil's full names will not be used on any online platform, including blogs and reward systems, particularly when in associated with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website or in any documentation that will appear outside of the school. This is collected every academic year.

## Roles and Responsibilities

Within the school, there are a range of people who are responsible for keeping staff and pupils safe online. The key professionals in relation to online safety are:

Name	Role
Katie Moran	Head Teacher
Judith Astwood	Designated Safeguarding Lead, Deputy Head Teacher, E-Safety Lead
Louise Johnson	Deputy Head Teacher
Hedd Williams	Deputy Head Teacher
James Barker	Computing Co-Coordinator/E-Safety Lead

EAST ICT Technical Support (David Wakefield and John Thomas)	ICT Technical Support
---	-----------------------

The duties for each of these positions and other members of staff are outlined below:

#### *Governors*

- Governors will be expected to approve the E-Safety policy following every review and ensure that the effectiveness of the policy is considered. This will be carried out by the Governors receiving information about e-safety incidents and monitoring reports. This may involve:
  - Meetings with the E-Safety leader.
  - Monitoring of e-safety incident logs
  - Monitoring of filtering/change control logs
  - Updates from the safeguarding team regarding e-safety.

#### *Head Teacher and Senior Leaders*

- The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community.
- The Head Teacher/Senior Leaders are responsible for ensuring that the E-Safety leader and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Leader.
- The Head Teacher and E-Safety Leader should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

#### *E-Safety Leader*

- Leads on e-safety
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documentation.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority when appropriate.
- Liaises with school ICT technical support staff.
- Receives reports of e-safety incidents and uses the school safeguarding system to keep a log of all e-safety incidents to inform future e-safety developments. At Montagu Academy, this is achieved through the use of CPOMS.
- Meets annually with the Designated Safeguarding Officer to discuss current issues, review incident logs and filtering logs. This may be reported to governors.
- Attends relevant meetings with the Governing Body.
- Reports regularly to the Senior Leadership Team.

#### *Technical Staff*

- Ensuring the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Ensuring users may only access the school's networks through a tightly enforced password protection policy.
- Ensuring that they are up to date with the e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- Ensuring that the use of the network, remote access, email and online learning platforms is regularly monitored in order to oversee any attempted misuse and is logged as an e-safety issue.
- Ensure that the monitoring software/systems are implemented and updated as agreed in school policies if they are deployed.

#### *Teaching and other Classroom Professionals*

- Up to date with all e-safety matters and the current e-safety policy and practices.
- Read and understand the Acceptable Use Policy.
- Read, understand, sign the Acceptable Use Agreement.

- Report any suspected misuse or problem to the E-Safety Leader/Designated Safeguarding Officer/Head Teacher for investigation.
- All forms of digital communications with pupils/parents should be on a professional level and only carried out using official school systems. (Class Dojo and Mathletics)
- Recognise that mobile phones and other hand held devices that are used for personal use, should not be in an unlocked place following the arrival of children in school. They should be placed in the staff room in a locker or placed in the school safe.
- Refrain from using personal devices to take photos in the classroom or on school visits. Class iPads, school iPads and any digital cameras purchased by the school should be used.
- Any form of inappropriate messages received from a parent/carer or pupil is reported immediately to the E-Safety Leader/Designated Safeguarding Officer and recorded on CPOMS for investigation.
- Ensuring e-safety issues are embedded in all aspects of the curriculum and other school activities.
- Complete an e-safety week every term to focus on current e-safety issues in relation to stage expectations.
- Allow pupils to understand and follow the school e-safety policy and adhere to the acceptable use policy.
- Allow pupils to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Monitor ICT activity in lessons, extra-curricular activities and extended school activities.
- Be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that their use is monitored and implement current school policies with regard to these devices.
- In lessons, where Internet use is pre-planned, pupils 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.

#### *Designated Safeguarding Officer*

- Ensure they are aware of the child protection issues that can arise from:
  - Sharing of personal data
  - Access to illegal/inappropriate materials
  - Inappropriate on-line contact with adults/strangers
  - Potential or actual incidents of grooming
  - Cyber bullying
- Monitor and action any serious E-Safety incidents that arise.
- Keep an up to date log of any E-Safety incidents through the use of the safeguarding software CPOMS.

#### *Pupils*

- Use the school ICT systems in accordance with the Pupil Acceptable Use Agreement (See *Appendices*).
- Sign the Acceptable Use Agreement prior to use prior to accessing school systems.
- Understand how to avoid plagiarism and uphold copyright regulations.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Be expected to refrain from using mobile phones, digital cameras and hand held devices whilst on school premises. When hand held devices are brought into school, they will be expected to be handed into the appropriate office and locked in the school safe until the end of the school day.
- Understand what cyber bullying is, the consequences that it can lead to and the need to report any incidents.
- Adopt a good e-safety approach to using digital technologies out of school and realise the benefits of adhering the school E-Safety code out of school.

#### *Parents and Carers*

- Endorsing the pupil acceptable use agreement.
- Promoting e-safety to their child when their child is accessing the internet.

- Adhering to the Acceptable Use agreement when accessing school websites, blogs and learning platforms.
- Communicating with staff in an appropriate manner only when necessary through school systems only, such as Class Dojo.
- Understanding that any inappropriate communication towards the school will be reported immediately and an investigation will take place that may need to further actions being deemed necessary to be undertaken.

*Amended:*                      *October 2016*  
*Next Review Date:*        *October 2017*