Moorland School

ICT AND ACCEPTABLE USE POLICY

This Policy includes the Junior School and Senior School

Links to other policies:
Anti-Bullying Policy; Data Protection & Confidentiality Policy;
Safeguarding & Child Protection Policy

Introduction

Children and young people have grown up in a world where modern technologies are becoming increasingly common. They view the internet and mobile phones as a positive, productive and creative part of their activities and development of their identities; always on and always there. ICT supports social activities and allows young people to feel connected to their peers.

Unfortunately, technologies can also be used negatively. Internet sites can contain illegal, inappropriate or biased information, mobile phone cameras are instantly available and Video Publishing sites such as You Tube means that the images taken can quickly be available to view all over the world. Mobile phones and social network sites have meant that cyberbullying is now a feature of many young people's lives.

Responsibilities of children and young people

The responsibilities of children and young people themselves should not be underestimated – they are to be encouraged to develop their own sets of safe and responsible behaviours as, ultimately, this will provide the best defence for keeping them safe online. Responsibilities must be appropriate to the age, maturity and understanding of the child but, nevertheless, awareness should start at a very young age.
Key responsibilities for children and young people include:

- Reading AUPs – and adhering to them.
- Taking responsibility for keeping themselves – and others – safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.
- Respecting the feelings, rights, values and intellectual property of others.
- Seeking help from a trusted adult if things go wrong, and supporting others who may be experiencing e-safety issues.
- Discussing e-safety issues with parents and carers in an open and honest way.

Responsibilities of the SLT team

The SLT team in school have statutory responsibilities for child protection, of which e-safety is an aspect. The SLT endeavours to have a sound awareness of e-safety issues, and to fully understand the importance of having effective e-safety policies and procedures in place. The leadership team ensures that e-safety implications are duly considered within all other school business.

E-Safety Safeguards

All schools have a responsibility to ensure that all students and staff access the internet safely and responsibly. The following safeguards have been introduced into the school to help ensure all users remain safe on-line.

All users of the school network must sign an acceptable use policy. This can be found in the pupils' homework planner and is included for information. Parents/carers must also sign this policy.

The acceptable use policy (AUP) and E-Safety guidelines have been agreed by the SLT.

There are clear, written procedures within the Student ICT acceptable use policy of the sanctions that exist if the policy is not followed.

E-Safety and Cyberbullying lessons are written into the Year 7 ICT scheme of work. E-safety is also a feature of the GCSE specification followed at KS4. Posters on this issue, both professionally produced and student made, are prominently displayed in school.

There are pastoral sessions on Cyberbullying and E-safety in the Junior school and the Year 13s receive a reminder session on assessing the advantages and pitfalls of the virtual world.

Parents/Carers' E-Safety evenings are held where current trends and risks are highlighted and key safety advice given.

The school's internet is filtered so that inappropriate sites are blocked. These include pornography, race hate, drugs and violence.

Staff or students who find inappropriate websites should report them to the Headteacher.

The use of mobile phones to make calls or send texts is prohibited during lessons. However, the use of other features such as camera, calculator, web browser, may be allowed at the discretion of the teacher.

Teachers can be contacted by Edmodo. Students should not be talking to teachers using social networking sites.

Cyberbullying

Cyberbullying is the use of Information Communications Technology (ICT), particularly mobile phones and the internet, to deliberately upset someone else.

It differs from other forms of bullying in a number of ways:

- **24/7 and the invasion of home / personal space.** It can take place at anytime, anywhere.

- **Size of the audience.** Electronically circulated messages can reach a very large audience, very quickly. The spread of the messages is very hard to limit or control.
- **Anonymity of the bully.** The bully may never be in the same physical space as their victim.
- **The profile of the bully.** Age or size is not important. Bystanders can quickly become accessories to the bullying; for example, by passing on humiliating images.
- **Cyberbullying can be unintentional.** It can be the result of not thinking or a lack of awareness of the consequences.
- **Many cyberbullying incidents can themselves act as evidence.** This is one of the reasons why it is important to know how to respond.

Bullying is never acceptable. The school has a duty to protect all its members and provide a safe, healthy environment. Here are details about how an incidence of cyberbullying should be dealt with.

Cyberbullying Procedures

When dealing with any incident of cyberbullying it is important to follow the procedures set out in the schools anti-bullying policy. However, there are some additional steps to take when responding to cyberbullying.

- Reassure the victim that they have done the right thing and that everything will be done to deal with the problem.
- Make sure the person knows not to retaliate or return any messages.
- Help the person to keep any relevant evidence. Note down any web addresses used, take screen capture shots if possible and try to ensure messages are not deleted.
- Advise the person of some simple steps they can take to prevent it from happening again. E.g. Blocking a contact, changing your own contact details, leaving a chat room, reporting the abuse to the service provider.

Action needs to be taken to contain the incident as quickly as possible.

- Any on-line content should be removed.
- Use disciplinary powers to confiscate any mobile phone being used for cyberbullying.
- Ask the bully to tell you who they have sent messages on to.
- In the case of any illegal content the Police should be contacted.

For a more detailed look at cyberbullying and ways of responding, the DCSF'spublication "Safe to Learn: Embedding anti-bullying work in schools" provides some very useful guidance.

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT & PSHEE and is regularly revisited – this will cover both the use of ICT and new technologies in school and outside school

- **Key e-safety messages are reinforced as part of the planned programme of tutorial / pastoral activities**

- **Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information**

- Students should be helped to understand the need for the student ICT AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Rules for use of ICT systems / internet are available in student planners.

- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents/carers often either underestimate or do notrealise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

• Letters, newsletters, web site
• Parent/carer workshops

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e- safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that 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.

- Where students are allowed to freely search the internet, using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally not be acceptable.

- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- An audit of the e-safety training needs of all staff will be carried out by the Headteacher. It is expected that some staff will identify e-safety as a training need within the Teacher Appraisal process.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.

- Teaching staff are issued with a copy of DfE guidance 'Teaching Online Safety in School' and are expected to embed this in their teaching.

- This E-Safety policy and its updates will be reviewed and consulted upon by staff.

- Staff Inset will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Users are prevented from installing programmes on school workstations.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

School Filtering Policy

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities
The responsibility for the management of the school's filtering policy will be held by the Assistant Headteacher. She will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

All users have a responsibility to report immediately to the Headteacher any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through staff meetings, briefings & Inset.

Parent/carers will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc.

Any changes to the Filtering System should be supported by strong educational reasons for changes that are agreed.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

Monitoring will take place as follows:

Communication Technologies

This is an area of rapidly developing technologies and uses which have the potential to enhance learning. The following list shows how the school currently views the use of these technologies.

- Mobile phones may be brought to school but at the users" own risk. The school takesno responsibility for the safe keeping of these items.
- Use of mobile phones for making calls or texting in lessons is prohibited. All mobile phones are to be handed in to the form tutor at registration, and are returned at the end of the school day.

- Use of mobile phones in social time is allowed.
- Taking photos on mobile phones or other camera devices is prohibited.
- Use of chat rooms / facilities is prohibited.
- Use of instant messaging is prohibited.
- Use of social networking sites is prohibited.

When using communication technologies the school considers the following as good practice:

- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students are taught about email safety issues, such as the risks attached to the use of personal details. They are also taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Use of digital and video images

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. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those 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 or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without permission from a member of staff.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.
- **Student's work can only be published with the permission of the student and parents or carers.**

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of “high profile” losses of personal data by public organisations, staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, once it has been transferred or its use is complete.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, 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, through 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, for example,

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

ICT ACCEPTABLE USE POLICY

When using the school network. I will:

- always log off when I am finished on the computer;
- not attempt to alter any computer settings, including background images;
- always ask permission before attempting to transfer any files to the school network;
- not attempt to download, upload or otherwise bring onto the school network programs and files that may contain hidden programs (zip, exe etc.). This includes all files that may be used for purposes forbidden on the school network such as games and chat rooms;
- not attempt to deliberately seek out files on the school network that may be used for malicious purposes;
- never access other people's files unless a copy has been sent to me by email;
- only use the computers for school work or homework;
- always handle the equipment with care and respect;
- report any faults to my teacher straight away.

When using the internet. I will:

- ensure a teacher is present in the room before using the internet and always ask if I may use it, unless I have been directed to do so as part of my lesson;
- not deliberately seek out inappropriate or offensive material;
- not deliberately seek to bypass the school internet filters in order to gain access to sites that have been deemed inappropriate;
- report any material that I accidentally come across that is inappropriate to my teacher, this applies to any material of a violent, dangerous, racist or inappropriate sexual nature;

- not download applications or other software;
- not access games sites other than those specifically directed by my teacher for educational purposes;
- never publish personal details about myself, my friends or other people that I know;
- not use chatrooms or instant message type applications;
- refrain from using foul language in any email correspondence and will never use the school email system to send messages that are aimed at causing harm or upset to others;
- always report any unpleasant emails I am sent to a teacher;
- not open email attachments without the permission of my teacher.

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.

Reviewed by Deborah Frost, September 2022