GREATFIELDS SCHOOL

Partnership Learning

Date approved: Awaiting ratification by governors – July 2016

Review Frequency: Every three years.

Date next review due: July 2019

E-Safety Policy

Introduction

The purpose of the document is to present the E-Safety Policy for staff and students. It is also to ensure that all staff are aware of the appropriate steps to take when presented with an e safety issue. This policy is part of the School Improvement Plan and relates to other policies including the safe use of ICT, bullying and child protection to ensure the safety of all users.

What is E-Safety?

- e-safety is important to safeguard young people and adults in the digital world;
- e-safety is about learning to understand and use new technologies and ICT in a positive and safe way;
- e-safety is not about restricting learning; it is about educating young people and adults of the risks as well as the benefits so they can feel confident and safe using technology;
- e-safety is about adults being educated to be able to support and help young people.

Policy

The Greatfields e-safety policy is one which provides clear direction to staff and others about expected behaviour when dealing with e-safety issues. This policy makes explicit the school's commitment to the development of good practice and sound procedures. It ensures that child protection concerns, referrals and monitoring may be handled sensitively, professionally and in ways which support the needs of the child.

The Greatfields school is committed to:

- developing students behaviour towards, and respect for, other young people and adults, including freedom from bullying and harassment that may include cyber bulling;
- supporting students' ability to assess and manage risk appropriately and to keep themselves safe online and through the use of technology;
- the provision of a broad and balanced curriculum that enables all students to achieve their full potential and make progress in their learning supported by the safe use of relevant technology.
- engaging with parents and carers in the safe use of technology outside of school.
- ensuring students know how to protect themselves online outside of school.

The school has appointed an e-safety coordinator and will ensure that the Safeguarding Lead also undertakes training in inter-agency working and attends refresher training at two yearly intervals to keep knowledge and skills up to date. Temporary staff and volunteers who work with children in the school will be made aware of the school's arrangements for child protection and their responsibilities.

This e-Safety Policy has been written by the school, building on government guidance. All staff are reminded that e-safety should be consistent with the school ethos, other safeguarding policies and the Law.

Teaching and Learning

Internet use is part of the school curriculum and an important tool for learning; students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. The school Internet access is designed to enhance and extend education and students will be taught what Internet use is acceptable and what is not.

Greatfields will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law; students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students will use age-appropriate tools to research Internet content.

Managing Information Services

- the security of the school information systems and users will be reviewed regularly;
- virus protection will be updated regularly;
- the contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- images or videos that include students will be selected carefully and will not provide material that could be reused.
- students' full names will not be used anywhere on the website, particularly in association with photographs.
- written permission from parents or carers is obtained when a student joins the school before any images/videos of pupils are electronically published or videoconferencing takes place.
- students will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.
- the school will control access to social media and social networking sites.
- if staff or students discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.

- the school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure;
- the school's broadband access will include filtering appropriate to the age and maturity of pupils;
- videoconferencing will be supervised appropriately for the students' age and ability;
- students will ask permission from a teacher before making or answering a videoconference call;
- all videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer;
- parents and carers consent will be obtained prior to students taking part in videoconferences;
- emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed;
- students will be instructed about safe and appropriate use of personal devices both on and off site;
- personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

- all staff will read and sign the school Acceptable Use Policy before using any school ICT resources;
- students will apply for Internet access individually by agreeing to comply with the school Student Acceptable Use Policy;
- the school will maintain a current record of all staff and students who are granted access to the school's electronic communications;
- the school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate;
- the school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use;
- all incidents of cyberbullying reported to the school will be recorded;
- cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour;
- there are clear procedures in place to support anyone in the school community affected by cyberbullying;
- there will be clear procedures in place to investigate incidents or allegations of Cyberbullying;
- all users will be mindful of copyright issues and will only upload appropriate content onto school network drives;
- only members of the current pupil and staff community will have access to the school network;
- pupils/staff will be advised about acceptable conduct and use when using the school network;

- SLT and staff will regularly monitor the usage of the school network by pupils and staff in all areas, in particular message and communication tools and publishing facilities;
- when staff, pupils etc leave the school their account or rights to specific school areas will be disabled;
- personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998;
- school staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation;
- the sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy;
- the use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school acceptable use policy.

Communications Policy

- all users will be informed that network and Internet use will be monitored.;
- an e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils;
- staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential;
- the e–Safety Policy will be formally provided to and discussed with all members of staff;
- to protect all staff and pupils, the school will implement Acceptable Use Policies;
- up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff;
- parents' attention will be drawn to the school e–Safety Policy in newsletters and on the school website.

The E-Safety Officer's responsibilities include:

- taking day to day responsibility for e-safety issues and having a leading role in establishing and reviewing the school e-safety policies/documents in conjunction with the Designated Child protection Coordinator;
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- providing training and advice for staff;
- liaising with school IT technical staff
- Receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments
- Reporting regularly to Senior Leadership Team

- Undertaking regular e-safety training

Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- students are aware of all necessary measures to protect data and personal information
- students are critically aware of the materials they read and shown how to validate information before accepting their accuracy;
- they report any suspected misuse, problems or availability of inappropriate online material to the E-Safety coordinator for investigation, action or sanction and inform the relevant staff (Form Tutor and Heads of Year)at the earliest convenience;
- digital communications with students (email or social media/networking should be on a professional level (in line with the School Acceptable Use Policy)
- e-safety issues are embedded in all aspects of the curriculum and other school activities;
- e-Safety is promoted with the students in their care and they will be supported to develop a responsible attitude to safety online, system use and to the content they access or create;
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extra-curricular and extended school activities;
- they are aware of e-safety issues relating to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices;
- 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;

Students are responsible for:

- using the school ICT systems in accordance with the Student Acceptable Use Policy.
- maintaining a good understanding of how to research effectively and the need to avoid plagiarism and uphold copyright regulations;
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understanding school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on bullying through the use of technology;
- understanding the importance of adopting good e-safety practice when using digital technologies and social media/networking sites out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school;
- ensuring they do not reveal personal details of themselves or others in online communication, or arrange to meet anyone without specific permission.

GREATFIELDS SCHOOL

Partnership Learning