The Grange Trust
E-Safety Policy & ICT Acceptable Usage Agreement (AUA)

Rationale

As an Academy Trust working with our local, national and international communities, ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

- At Bramley Grange Primary School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.
- Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, digital cameras etc); and technologies owned by pupils and staff, but brought onto school premises (such as mobile phones, camera phones, and portable media players, etc).

Roles and Responsibilities

- ➢ As e-safety is an important aspect of strategic leadership within the school the trust have ultimate responsibility to ensure that the policy and practices are embedded and monitored. This responsibility is delegated to the Head. Teacher.
- ➢ The designated safeguarding person and ICT leader have the responsibility of ensuring this policy is upheld by all members of the school community and that they have been made aware of the implication this has. It is the role of these members of staff to keep abreast of current issues and guidance through organisations such as, Becta, CEOP (Child Exploitation and Online Protection), Childnet, NSPCC, Childline and Rotherham Local Authority Safeguarding Children Board.
- ➢ This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, safeguarding policy, behaviour policy and bullying plicy.

E-safety skills development for staff

- Our staff receive regular information and training on e-safety issues in the form of full staff meetings and briefings.
- New staff receive information on the school's acceptable use policy as part of their induction through the staff handbook.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Communicating the school e-safety messages

- E-safety rules will be discussed with the pupils at the start of each academic year.
- Pupils will be informed that network and Internet use will be monitored.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety. We actively monitor and assess our pupils' understanding of e-safety.

- The school provides opportunities within a range of curriculum areas and discrete ICT lessons to teach about e-safety (in accordance with the medium term planning.)
- Educating pupils on the dangers of technologies that maybe encountered outside school may also be done informally when opportunities arise.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button. Yearly e-safety promotion sessions take place within school for children, parents and the wider school community.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff passwords remain confidential to all staff for all systems and must never be shared or 'loaned out' The pupils from the Nursery upwards have separate logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. Level of access is determined by the Head Teacher

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- All staff must read and agree to the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Access to the Internet will always be supervised by an adult and is filtered by the service provider rgfl.
- Staff will always preview any recommended sites before use, checking for inappropriate images and material including inappropriate language
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- School internet access is controlled through rgfl's web filtering service.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be closed and the incident reported immediately to the class teacher who must inform the designated safeguarding person.

- It is the responsibility of the technical support; to ensure that Anti-virus protection (Sophos) is installed and kept up-to-date on all school machines including staff laptops
- If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.
- Pupils and staff are not permitted to download programs on school based technologies without initially consulting with the ICT technicians. If there are any issues related to viruses or anti-virus software, the ICT technicians should be informed through the 'Computer Problems' book held in the main office

Managing Social networking Sites

Refer to Social networking policy

- At present, the school endeavours to deny access to unmonitored social networking sites such as Facebook to pupils or staff within school.
- There should be no communication between staff and pupils or staff and parents through social networking sites such as Facebook.
- Staff are advised to keep their Facebook pages private using privacy settings
- Staff are advised not to upload personal images onto Facebook
- Parents are advised of issues surrounding social networking that may arise
- Parents and pupils are advised of the legal age for accessing Facebook
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. These must be switched off during teaching time.
- Staff and pupils are not permitted to bring digital cameras into school, each class has its own school digital camera for the purpose of taking photographs.
- Staff are strongly advised not to contact a pupil or parent/ carer using their personal device.
- Pupils are allowed to bring mobile phones to school if there is a safeguarding need. Parents must complete a parental permission form prior to bringing phones into school and they must be handed to teachers for safe keeping at the start of the school day. If such a device is in school without parental permission forms and without knowledge of the class teacher, it will be confiscated and a responsible adult will be required to claim it from the headteacher. In such circumstances the headteacher will give a reminder about 'e' safety.
- The school is not responsible for the loss, damage or theft of any mobile phone.
- Pupils are encouraged not to bring personal mobile devices into school including digital cameras
- The sending of inappropriate text/internet messages between any member of the school community (including staff) is not allowed. (This includes inappropriate 'jokes')
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device and the device is not being used for the purpose of illegal activity.

Managing email

The use of email is an essential means of communication for both staff and pupils. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The school gives all staff their own email and a class email (bgpclass+ teacher initials) accounts to use for all school business.
- Children can email homework projects to the class name account (i.e. bgpclassxx@rgfl.org) This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff are never to give personal email addresses to pupils or parents
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses. The main school e-mail or SIMS e-mail should be used to contact parents.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use the class account on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arranging to meet anyone without specific permission, virus checking attachments.
- Staff should monitor the class e-mail account, checking the content of the e-mails prior to sharing with pupils
- Staff must inform the Headteacher if they receive an offensive e-mail.
- Pupils should be introduced to email as part of learning in year three and continued in year four, five and six.

Safe Use of Images - Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips.
- Pupils are **not** permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on school trips. This is made explicit on permission letters.

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, safeguarding reasons.
- Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by one parent/carer
- Pupils' full names will not be published alongside their image and vice versa.
- E-mail and postal addresses of pupils will not be published.
- Before posting pupils' work/photo's on the Internet, staff will check to ensure that permission has been given for work/photo's to be displayed.

Storage of Images

- Images/films of children are to be stored in the 'photos' folder within the staff area of the server. They should be removed when they are no longer needed.
- Images shown on other areas of the school's network must be temporary in nature and removed as soon as possible.
- Images taken on portable media (FLIP, Cameras, IPADS, staff laptops, curriculum laptops, curriculum desktops must be deleted as soon as they have been uploaded so that the media is 'empty'
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks)
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.
- Teaching Staff have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

Misuse and Infringements

Complaints

- Complaints relating to e-safety should be made to the Head Teacher.
- All incidents will be logged and followed up.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and must be reported to the DSP (headteacher)
- Pupils and parents will be informed of the complaints procedure.

Inappropriate material (see ICT Acceptable Use Agreement)

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the headteacher.
- The appropriateness of websites may be checked by the head teacher. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the headteacher, depending on the seriousness of the offence may lead to an investigation by the Head Teacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct.

Equal Opportunities: Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-safety where appropriate in the form of;
    - Information sessions
    - Posters
    - Newsletter/email items
- Parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Parents/carers are expected to reinforce the guidance from school when using technologies at home. The school will not be responsible for communications between pupils' outside school through social networking sites or for pupils accessing inappropriate sites outside school.