THE GRANGE ACADEMY

ASPIRE FOR EXCELLENCE

E-Safety Policy
2021- 2022

Version Number: 02
Ratified by Local Governing Body: September 2019
Next Review Date: September 2022
Academy Link: Mr T Hutton

Contents

Introduction

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
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Apps
- 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.

We understand the responsibility to educate our students on eSafety 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 Agreement** (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital photography equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, smart watches, etc).

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the academy, the Principal and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. For the purposes of this document the following staff are referenced throughout:

Principal	Mr I Critchley
Assistant Associate Principle	Mr T Hutton
ICT Manager	Mr C Buckley
School's Safeguarding	Mrs K Price

All members of the school community have been made aware of who holds these posts. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Halton LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Principal and all governors understand the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors, is to protect the interests and safety of the whole school community.

E-Safety skills development for staff

- New staff receive information on the school's acceptable use policy as part of their induction.
- 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.

Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. Staff are regularly reminded of the need for password security.

- Staff are required to set their own password that requires at least 8 characters. SIMS Usernames and passwords are provided by the SIMS Manager.
- If staff believe their password may have been compromised or someone else has become aware of their password they must report this to ICT Support.
- Staff are made aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS systems, including ensuring that passwords are not shared and are changed regularlly.
- All users must make sure that workstations are not left unattended and are locked.
- In school, all ICT password policies are the responsibility of the ICT Manager and all staff are expected to comply with the policies at all times.

Data and Security

The accessing and appropriate use of school data is something that the school takes very seriously. The school follows the Information Commissioners Office (ICO) guidelines

- Staff are made aware of their responsibility when accessing school data.
- The Level of access is determined by either the Head Teacher and / or the ICT Manager.
- Confidential or sensitive data taken off the school premises must be encrypted.
- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any confidential or sensitive data without the express permissions of the Head Teacher.
- Only software properly purchased and/or approved by ICT Support may be used on TGA hardware. It is the responsibility of the user to ensure that ICT Support is fully consulted if they wish to purchase and install additional software on their laptop. It is also the responsibility of the user to ensure that any licensing issues are addressed promptly.
- It is TGA policy to store data on a network drive which is backed up each day. It is the responsibility of each individual user to ensure that data not stored on the network (i.e. on USB memory, or other storage medium) is backed up regularly. The School does not take responsibility for data not in the backup plan being lost, deleted stolen etc.
- Personal devices (Laptops, Mobile Phones etc.) are not permitted to be used on the system, or connected to the wireless infrastructure without the express permissions of the Head Teacher and / or ICT Manager.

- The School does not guarantee the security of any information users may enter while making permitted personal use of a School computer. The School disclaims all liability that may arise from loss or harm suffered by a user as a result of that information being disclosed to or obtained by any other person and then being further disclosed or being used so as to cause loss to the user. The School disclaims all liability for such losses and any employee using a School computer for permitted private purposes does so on the basis of having agreed this disclaimer of liability.
- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is neither the school's responsibility nor the system managers to install or maintain virus protection on personal systems.
- If there are any issues related to viruses or anti-virus software, the ICT Manager should be informed.

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. All use of the Internet at the Grange is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- All users must observe software copyright at all times. It is illegal to copy or distribute school software, non-licensed software or illegal software.
- All users must observe copyright of materials from electronic resources.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with students.
- 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.

Infrastructure

- School internet access is controlled through cloud based web filtering
- The Grange is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff are aware that school internet activity can be monitored and explored further if required.
- Intrusions into the privacy of employees must be proportionate to the purpose of the monitoring.
- The school uses AB Tutor management control tools for controlling and monitoring workstations.

- If staff discover an unsuitable site, the incident must be reported immediately to the ICT manager.
- It is the responsibility of the school, by delegation to the ICT Manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Staff are not permitted to download programs on school based technologies without seeking prior permission from ICT Support.

Managing email

The use of email within most schools is an essential means of communication for both staff and students. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international.

- The school gives all staff and students their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses.
- School e-mails must clearly indicate the following at the end of each message: Name, Position or Department, The Grange Academy, Telephone Number and Web Address.
- 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.
- Staff sending emails to external organisations, parents or students are advised to cc. their line Manager.
- 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 (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Staff must inform either the their line manager or ICT Manager if they receive an offensive e-mail.
- The School will assist the relevant authorities in taking action against any employee who commits an unlawful act whilst using the School's computer facilities. The School will report criminal activity to the Police.
- Personal or business e-mails, whether created or stored on School equipment, constitute a School record and as such are deemed to be property of the School.
- E-mails from unknown sources or which may appear suspicious must not be opened. Software received via e-mail must not be installed. You must consult ICT Support for advice if you receive software via e-mail or e-mail from an unknown source or which is otherwise suspicious.

- E-mails are formal documents and must not contain remarks that might be potentially embarrassing to the School, its employees or the general public. Further advice is provided in the Communications Guide produced by Halton Communications Department.

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism.

- At present, the school allows access to social networking sites for Staff within school, this allows for better connectivity with a range of e-learning technologies.
- School staff with social networking profiles should ensure that they set the privacy levels on their accounts to the maximum i.e. only people on their 'friends or trusted' lists should be able to view their pictures / private information.
- The school specifies the following guidelines should a message from a student be received:

    - Do not reply to the message. Replying to a message could allow the recipient to view your profile in its entirety. This is also a way to circumvent the privacy settings on accounts.
    - Inform the school's safeguarding lead at the earliest opportunity and advise them of the full details of the incident. The relevant Facebook communication should be made available to the member of staff to aid in any investigation.

- The School advises staff to keep their account privacy as high as possible.
- Any contact from a student, or attempted contact, must be immediately reported to the school safeguarding lead.
- Staff should not respond to any contact / request for contact from any student other than to delete / block.
- As a professional, you must remember that in addition to protecting yourself, you should not participate in anything via social media that would bring your employer into disrepute.
- All Staff are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Staff are encouraged to be wary about publishing specific and detailed private thoughts online.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using or other systems approved by the Principal.

See further guidance in:

'Guidance for safer working practice, Section 12 – Communication with students (including the use of technology)'

Social Networking Guidance document.

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. Many existing mobile technologies are familiar to children outside of school too. 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.
- Under no circumstances does the school allow a member of staff to contact a student using their personal device.
- The school advises staff not to contact parents or carers using their personal device.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Whilst on the premises or while conducting official school business permission must be sought before any image or sound recordings are made on personal devices by any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- While in School personal mobile phones shall be set on discreet mode.
- Mobile phones shall only be used in work in accordance with instructions issued by the schools mobile phone guidelines.
- Staff should not contact students outside normal school hours.

School provided devices (including phones)

- Where the school provides mobile technologies such as phones or laptops for offsite visits and trips, only these devices should be used to conduct school business.
- Fixed telephony equipment must not be moved, unplugged or switched off except with the express permission of ICT Support.
- Settings on telephones must not be altered as this could cause a failure to ring. Proper use of divert or follow me facilities is permitted.
- Personal incoming calls (by landline or mobile) with the exception of emergencies whilst at work should be discouraged and where unavoidable must be kept to a minimum.

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 (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However, with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

Consent of adults who work at the school

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing student's images and work

On a child's entry to the school, all parents/guardians 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, etc.
Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents / carers in order for it to be deemed valid.
Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.

Before posting student work or images external to the school, e.g. on the Internet or distributing to the Press, a check needs to be made to ensure that permission has been given for work to be displayed. This is the responsibility of the member of staff submitting the information.

Storage of Images

- Images/ films of children are stored only on the school's network.
- Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Principal
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network.
- It is staff's responsibility of deleting the images when they are no longer required.

Webcams and CCTV

- The school uses CCTV for security and safety. This is only accessible through the building management holders SPIE.
- Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes.
- Webcams can be found in the ICT department and with SLT for conducting virtual meetings.
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Principal is sought prior to all video conferences within school.
- No part of any video conference is recorded in any medium without the consent of those taking part.

Misuse and Infringements

Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator, or the Principal, all Incidents should be logged.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT Manager or e-Safety officer.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety officer,

Acceptable Use Agreement: Staff, Governors and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr Hutton, Grange School e-Safety officer.

1. I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head Teacher.
2. I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
3. I will ensure that all electronic communications with students and staff are compatible with my professional role.
4. I will not give out my own personal details, such as mobile phone number and personal email address, to students.
5. I will only use the approved, secure email system(s) for any school business.
6. I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal.
7. I will not install any hardware of software without the express permission of ICT Support
8. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
9. Images of students and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff and the Principal.
10. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.
11. I will respect copyright and intellectual property rights.
12. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
13. I will support and promote the school's e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.
14. I have read the e-safety policy

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……..…….…… Date ……

Full Name …….....(printed)

Job title . . . . . .

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 2018
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.legislation.gov.uk/uksi/2000/2699/contents/made

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.legislation.gov.uk/ukpga/2000/23/contents

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
For more information
www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:
Access to computer files or software without permission (for example using another person's password to access files) this offence carries a penalty of imprisonment up to six months and/or a fine.
Unauthorised access, as above, in order to commit a further criminal act (such as fraud). For this offence the penalty is up to five years' imprisonment and/or a fine.
Impair the operation of a computer or program. For this offence the penalty is up to five years' imprisonment and/or a fine.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Guidance for safer working practice for adults who work with children and young people in education settings 2009
All adults who come into contact with students in their work have a duty of care3 to safeguard and promote their welfare. The Children Act 2004, through the Stay Safe outcome of the Every Child Matters Change for Children programme, places a duty on schools/services to safeguard and promote the well-being of students. This includes the need to ensure that all adults who work with or on behalf of students are competent, confident and safe to do so.