Acceptable Use and Online Safety Policy

Version	Date	Description	Chair of Committee	Ratified (Y/N)	Next Review Due
1	8/1/09	Draft presented to Curriculum Committee	Simon Bainbridge	Y	Jan 2010
2	27/11/14	Draft presented to Curriculum Committee	Paul Illott	Y	
3	30/9/ 15	Draft presented to Curriculum Committee	Paul Ilott	Y	
4	15/9/16	Draft presented to Curriculum Committee	Paul Ilott	Y	Sept'17
5	03/10/17	Draft presented to Curriculum Committee	Paul Ilott	Y	Sept'18
6	24/09/18	Draft presented to Curriculum Committee	Paul Ilott	Y	Sept'19
7	03/12/19	Draft presented to Curriculum Committee	Paul Ilott	Y	03/12/2020
8	03/12/2020	Draft presented to Curriculum Committee	Paul Ilott		

Introduction

This policy addresses issues related to the acceptable use of the ICT facilities provided for children, staff, parents, occasional community users and governors to use. Specifically it deals with the use of the school curriculum network, the Intranet that runs on this network, the publicly available school website and the facility for access to the Internet provided through the network. It has been produced in accordance with National Association of Advisers for Computers in Education (NAACE) guidelines.

Acceptable use of these facilities implies use which:

- Safeguards individuals from offensive messages, personal or impersonal, in any medium capable of being held on a computer system, e.g. malicious emails messages, pornographic images, etc.
- Safeguards the anonymity of individuals (particularly pupils) and their computer-based work, when that is appropriate.
- Safeguards the integrity of computer based information held within the school or on behalf of the school.
- Safeguards the good standing and legal integrity of the school in terms of computer based information that is held publicly.

The school network

The make-up of the school network
The school network consists of a collection of PC's connected together via Local Area Network (LAN) cabling to a Windows XP file server this has changed to windows 10. A gateway to the E2bn portal further enhances this network. In Summer 2019 we had the wifi upgraded throughout the school. The system runs various levels of software designed to provide security. There are a number of other computers e.g. laptops, ipads and kindles in school which are not permanently connected to the network, but which are considered to be within the scope of this policy as regards acceptable use.

Legitimate users
Legitimate users of the school network are:

- Current pupils/adult learners
- All teaching staff and teaching assistants
- Office personnel
- Site management
- Therapists
- IT Technicians
- Governors
- Parents, when specifically authorised and supervised by a member of staff.
- Visitors, when specifically authorised and supervised by a member of staff e.g. Local Authority officers, software engineers from support companies, community users.
  It is not envisaged that the system will be available for use by, for example, former pupils or cleaning staff.

Legitimate use
The network is designed specifically for educational use. This includes:

- Access to educational and administrative software packages
- Access to reference sources and the sharing of information within the school and outside.
- The storage of information, teaching materials and work products related to educational topics
- The storage of information, teaching materials and work products related to educational topics.
- Communications between people inside and outside the school for educational ends.

It is intended that the network be used right across the curriculum, not just for the ICT curriculum area, and also for administrative support to staff.

It is also envisaged that the network may be used for personal use in an endeavour to develop the general ICT experience and the continued professional development of both pupils and staff*, but with the following provisos:*

- Personal use of the network must not involve the storage of information that would necessitate the registration of that data under the Data Protection Act. An example of this would be lists of personal data containing more than very basic attributes, e.g. a sports club subscriptions list.
- Personal use of the network must not in any way interfere with normal school operations. For example teaching staff and pupils should not be making personal use of the network during lesson time. Also personal use must not significantly impair the performance of the network or cause excessive amounts of resources to be used, especially photographs, printer ink, paper and disc storage space.
- The network must not be used for commercial use in any way.

Network access control

General comments

The network is to be kept secure using a variety of software products, reviewed regularly, which control access. Individuals gain access through a network wide user-name and password system (referred to as "log-ons"). This system will identify the category of user and the system resources to be made available to that user. *It is not acceptable and is an offence by law to attempt to gain access to another log-on without the permission of that user. Pupils must never be allowed access to staff or system administrator log-ons.*

Connection to the network from outside the school will be allowed to teaching staff. Firewall software is used to ensure that access to the network cannot be gained from outside the school when the network is connected to the Internet; this protection is also is provided via the E2bn.

Pupils/adult learners

Pupils/adult learner will be provided with an individual log-on which they will keep throughout their time at Granta. This log-on will be deactivated when they move on from the provision.

Pupils will have access to an area of personal disc space (known as the P: drive) where they can store, edit and delete their work. This area is accessible only by that pupil and by staff users. They also have read-only access to a public (pupil templates) area of disk space (known as the T: drive) from which materials can be copied via year group folders, which gives full public update access to anyone in the year group. This is intended as an area in which collaborative work can take place or where work can be assembled for the teacher to view. *Pupils that use this folder need to be aware that they must be careful not to damage or delete the work of others*.

Staff

Each member of teaching staff is assigned an individual log-on. This must be kept secret, especially from pupils/adult learners and outside visitors. Logins are for individual staff only and are not to be shared under any circumstances.

Staff also have full access to an area of personal disc space (known as the H: drive). This is completely private from pupils/adult learners but is accessible by system administrators. Staff have full access to the T: drive and it is here that they can place materials for children to view and copy. Disc space named G:/Staff is only accessible by staff. Disc space named J:/curriculum is accessible by staff and administrators. All computers are to be logged out or locked by the individual user when staff leave the room.

System Administrators

The system administrators are a small group of staff, selected by the head teacher, who have overall responsibility for the maintenance and integrity of the network. These will usually include the ICT Administrator and the ICT Technician. They have a set of log-ons that afford full access to the system and all its data, including the ability to change access control. *The passwords for these log-ons must never be divulged to anyone other than the system*

administrators, the senior management team and engineers from companies retained to carry out maintenance of the system, without the express permission of the head teacher.

Virus protection
Computer viruses are items of software that attach themselves to other legitimate items of software or data, without the consent of the computer user, and are programmed to proliferate themselves onto other computers, often to cause disruption or damage. It is essential that all users play a part in protecting the network from the presence of viruses.

It is the policy of the school to run up to date virus protection software on all computers that are attached to the network. This software will automatically report the presence of most known viruses. *Any user who receives an on-screen warning from this software (these are very clear and explicit) should stop all use of the computer immediately and report the occurrence to the ICT Administrator or the ICT Technician.*

Viruses can attach themselves easily to digital media, this is one of the main ways in which they are proliferate.

See later sections of this policy regarding Internet use for more details about virus protection considerations.

Internet Access

General
The Internet is destined to play an increasingly significant role in the education of the children and adult learners at Granta and the professional practice of the staff. For this reason access to the internet is made available from any network computer in school or ipads/laptops/Kindles through wifi.-Staff monitor pupils whilst using these and restrictions are placed on the ipads/laptops/Kindles as it is recognised that the Internet contains material which is unsuitable within a school context or which is offensive. Furthermore the enhanced communications facilities afforded by the Internet raise issues of privacy and personal safety. For this reason it is necessary to put in place a range of restrictions on the use of the Internet and all users of the network must be made aware of these.

The network offers the following Internet facilities:
- The World Wide Web - i.e. pages of text, images and sound linked together and accessible from computers all over the World.
- Email.

The following Internet facilities however are explicitly **not** to be used in school and are masked out by software:
- IRC - Usually known as "Chat rooms". These allow Internet users to chat to one another in real time and offer a high degree of anonymity to participants. Whilst there is a place for such a facility in an educational context, the risks inherent in conversations between children and anonymous individuals is much too great for this facility to be offered in its current form. The availability of more secure and supervised chat facilities will be kept under review.
- Usenet - publicly available on-line "notice boards" or "news groups" in which threaded discussions about subject specific themes takes place via email style messages. There are a number of these news groups that are specifically designed for the use of UK teachers and are quite useful. However Usenet is largely uncontrolled and is the source of much of the inappropriate and obscene material on the Internet. For this reason it is not allowed in school although this will again be kept under review.

If you accidentally find a child abuse image do not open it, do not send it on, it is an offence.
- Immediately lock out the computer and contact the ICT administrator. Ensure no other staff and students have access to the machine.

The World Wide Web
The World Wide Web (WWW) should prove to be an invaluable resource for teachers and children and its use is to be greatly encouraged in all curriculum areas. However two important usage issues arise:

Finding useful and authoritative materials
The amount of information to be found on the WWW is vast and there are no controls on what is there and how authentic it is. This means that whilst sometimes a rich source of information can be found remarkably quickly, on other occasions hours can be spent in fruitless searching. The ability to sift and search is an essential ICT skill for children and needs to be taught specifically. On the other hand, for many Internet linked activities, protracted periods of searching will not lend themselves to the main learning objectives of the lesson. *For this reason staff should generally have searched for suitable websites in advance of a lesson and have checked their suitability and accuracy in just the same way as they would do with a book.*

Protection from inappropriate material
The protection of our pupils from inappropriate materials on the WWW is achieved through the use of software and staff supervision. The following measures must be in place:

- Our connection to the WWW must be through an Internet Service Provider that provides a basic level of filtering of inappropriate material.
- The default filtering is via County, which is to the British Educational Communications & Technology Agency (BECTa) standard.
- Staff need to be active in observing where children are browsing on the WWW in case they are moving towards inappropriate areas.
- Any discovery of an unsuitable website should be reported to the ICT Administrator so that the site can be filtered out.
- When asking pupil/adult learners to use search engines to find suitable websites, child oriented search engines such as "Google" or "Ask Jeeves for Kids" should be used as far as possible.
- Children/adult learners are shown how to use ‘advanced’ searches, therefore limiting the chance of finding inappropriate material.

Downloading of materials
The WWW affords many opportunities to download items of data or software free of charge and this material can often be very useful. However caution must be exercised as such downloads can be the source of viruses and other malicious content. The following practices should be followed:

- Children/adult learners should be expected to ask permission before accessing material that requires downloading. There will be appropriate sanctions for pupils who are caught downloading inappropriate materials from the Internet or specific mobile devices.
- Staff can download, or allow to be downloaded, the following materials freely:
  -Text (*but not unknown Microsoft Word files*), pictures, databases, etc. that do not contain any executable elements.
  - "Plug-ins" - These are computer programs which extend the ability of a web browser to display different types of graphics and sound. They usually download and install themselves automatically if the user approves. The network will already support the most common plug-ins but new ones must be requested if needed on PC’s or Laptops. Importing of files including from unknown or un-trusted origins should not be allowed.
- The following materials must be virus-checked by a system administrator before they are used in any way. *<u>Any</u> form of use of these materials before the have been checked could lead to the destruction of large amounts of the school’s data! :*
  - Any executable program.
  - Microsoft Office files as these can contain executable elements hidden in the document.

Where staff suspect that they have a problem with their computer or portable device, no data should be transferred and if possible the device should not be logged on to the system before talking to the systems administrator.

Supplying personal details
Often websites can ask for personal details to be supplied. For example an educational website might ask for a user's email address so that a regular newsletter can be sent to the user. Staff may supply personal details at their discretion. On the other hand *pupils/adult learners must be taught that they must never supply any details about themselves or the school unless they have consulted a member of staff first*.

E-commerce
E-commerce is a growing area of the WWW and facilitates the buying and selling of goods on-line. No sales or purchases of any kind must be made via the school network except by the school Business Manager, after completion of a school order signed by the budget holder.

Social media

When using social media for personal use, members of staff must not talk about their professional role in any capacity.

Staff members must not use social media to communicate with any pupils or any past pupils. In the unlikely event that a member of staff wishes to communicate with a parent of a pupil via social media then this must first be approved by the head of the school of executive head in writing.

Members of staff will be instructed to ensure that the maximum privacy setting are set u and maintained on any social media account. They must also only give permission for known friends to access the information on these accounts.

If any member of the staff experiences or comes across any derogatory or slanderous comments relating to the school, the academy trust, colleagues or pupils they should take screen shots and pass onto the e-safety coordinator.

Pupils will receive information and guidance on how to safely use social media.

Note to parents

- It is written within this policy that no member of staff may be in communication with parents from the school via social media on any platform unless senior management are aware that the staff member knew a parent before gaining employment at the school. Please make this as easy as possible by contacting staff members using the appropriate channels.

Email

Staff email
Every member of staff is allocated an email address for their professional use. This address uses the registered domain name for the school.

Staff email is web-based rather than held on a mail server in the school so that staff can access their email from home as well as at school.

Pupil/adult learner email
An email account will be provided for some pupils/adult learners in school and there is a class email account.

Despite these security measures staff must still be sure that they do not accidentally disclose children's email addresses to anyone other than legitimate correspondents. For example, do not put up a list of email addresses in a classroom.

It is very important that pupils/adult learners are taught about the dangers of email and reminded of these dangers at the start of each academic year. The issues that should be covered are:

- That the people they are communicating with should be known to them and also to school staff/support workers and/or parents.
- That they should never reply to a message from somebody they do not know and that when they receive such a message they should tell a teacher or their parents immediately.
- That they should report anything they consider to be abusive, upsetting or inappropriate in an email message to a teacher or parent immediately and not respond to the message.
- That they should never give out personal details such as their address or telephone number in an email.
- That their email is not private and that staff and parents must have access to it.
- That they themselves must never include abusive, upsetting or inappropriate material in any message that they send.

Email attachments

- It is possible to attach any number of computer files to an email message. This is very useful and could be used, for example, for a child/adult learner to submit a piece of homework done on a home computer to his or her teacher. However these attachments do provide another way viruses and other malicious computer code to enter the school's network.
- *For this reason Email users must never open or execute attachments from unknown correspondents.* These should instead be deleted straight away. If staff are at all unsure about other email attachments then they should ask a systems administrator to examine the files and run a virus check if necessary.

School website

In the future editorial control of this website will remain with the Senior Management Team with day to day management of the site being performed by e schools and Emma Jennings (school communication officer) This site will target a wide audience including the pupils/adult learners, parents, staff and governors of the school, other schools and casual visitors from around the world. It aims to have the following content:

- Information for visitors
- Information for parents and prospective parents, including an on-line version of the prospectus and our OFSTED reports.
- Displays of good work from our children
- Curriculum materials and guidance to help our children with homework
- General items of school news including celebrations of success in competitions and fund raising events.
- School policies

It is the school's policy not to identify the full names of children/adult learners on this website, as a means of protecting privacy. First names only must be used to annotate pictures, good work, sports results, etc. parents will be asked to give or withhold permission for photographs of their children/adult learners to be included in this way through our general information form.

Visitors to the website may be able to contact the school through email using a feedback form.

School Intranet

The school's curriculum Intranet is available to all staff and pupils and can be openly accessed throughout the network. It aims to have the following content:

- Displays of good work.
- Reference materials for children/adult learners in a well-indexed form.
- Teaching activities and resources related to particular year groups.

The Intranet will contain a secure "staff folder" section, accessible via a staff log-on, with the following extra content:

- All policy documents and related materials
- Schemes of Work and Units of Work
- Reference materials

The Emma Jennings (communications officer) will manage the Intranet, but there should be an ethos of openness and joint ownership. Hence all pupils/adult learners and staff are encouraged to produce content and software and make these contents easily available. Because the Intranet is private to the school pupils full names can be used openly.

Monitoring and reporting misuse

It is the responsibility of all users of the school's network to report breaches of this Acceptable Use Policy. In addition the system administrators will routinely examine the log files kept by various pieces of network monitoring software to identify potential problems. Examination of staff files and email however will only take place with the permission of the Head Teacher. Breaches of the Policy should be reported to the ICT Co-ordinator or Emma Jennings in the first instance, who will report to the Senior Management Team if a breach is confirmed. The Senior Management Team will make decisions on appropriate sanctions. Care should be taken with the storage of equipment to reduce the risk of theft or burglary, any equipment left unattended and in plain view should be reported so that it may be stored away safely, especially outside of school opening hours.

Security

All ICT equipment will be security marked and noted in the school inventory

- Any equipment taken off site should be signed out by the school administrator
- The administrator and ICT service will be responsible for regularly updating anti-virus software
- No portable data storage devices unless they are encrypted from outside school should be allowed in machines without permission from the ICT coordinator or system administrator. Encrypted flash drives can be supplied to teachers and TA's as necessary.
- Use of ICT will be strictly in line with the school's 'Acceptable Use Policy'
- Parents will be made aware of the 'Acceptable Use policy' and will be asked to give signed permission for their children/young adult to use computers, the Internet and e-mail in school
- All pupils/adult learners and parents will be aware of the School Rules for Responsible Use of ICT and the Internet and will understand the consequence of any misuse. If appropriate pupils and their parents can be asked to read and sign an ICT contract. Via the school agreement on administration and by availability of policies to read online,
- The agreed rules for Safe and Responsible Use of ICT and the Internet will be included in the school prospectus and staff handbook

Use of cameras, mobile phones and other portable devices

Increasingly technology is making it easier for images to be misused and it is therefore important we take practical steps to ensure that images of children/young adults taken by staff, parents, carers and by members of the media are done so in a way that is in accordance with the protective ethos of the school.

Images must be maintained securely for authorised school use only, and disposed of or stored as appropriate in line with GDPR. We reserve the right to examine any mobile device and investigate any reports of an infringement of use of school or personal equipment.

- Photos/ video can be taken on mobile devices, including phones at celebration events such as Christmas plays and sports days by parents or carers and pupils/ adult learns if appropriate. If the school suspects that the images are to be used inappropriately then it must report this on to the appropriate authority. Parents are required to sign a declaration form at each event and agree not to distribute, upload or share images, this includes uploads to social media sites.

- Teachers/support workers may store photographs on laptops. However, they may only be attached to school documentation and used for school purposes only. They may not be attached to personal emails or used to advertise your position in school.

- Any images taken by the media, or for use as publicity etc. must have a signed declaration form the head teacher, stating the intended use for the images before taking them. Having signed a declaration visitors are allowed to record celebrations etc. but parents of pupils included must be informed and permission sought before publication.

    - The use of personal mobile phones and personal devices within school teaching areas (including playgrounds) is strictly prohibited. Under no circumstances are images to be captured or shared. Mobile phones are only to be used in emergency situations when it is a designated point of contact off the school teaching site. Unless a staff member informs a senior manager that they need to keep their phone with them for personal reasons.

Appendix 1 - The main points that staff need to remember

- Don't divulge your staff log-on password under any circumstances and change it if you think it has been compromised.

- Don't leave a computer unattended and logged on to a staff log-on.

- Make sure that personal use of the network does not interfere with normal school operations.

- Explicitly teach children the points laid out in Appendix 2 i) at the start of each academic year and ii) when relevant computer based activities are about to begin.

- Actively monitor the websites that children are visiting during open web-browsing sessions and do not leave a group unsupervised.

- Try wherever possible to visit websites before you use them in your teaching so that you can check their acceptability.

- When children are to use a search engine, try to make it one that has been developed for children.

- Report any inappropriate websites that you find to the ICT Co-ordinator/Administrator so that they can be filtered out.

- Never divulge the "www" log-on password, and ask for it to be changed if you think it has been compromised.

- Actively monitor pupils' email messages.

- Always respond to an on-screen virus warning. Isolate the machine and inform the ICT Co-ordinator/Administrator immediately.

- If you download any executable programs or Microsoft Word documents, have them virus checked before you open them or execute them. The same applies when this type of file has been emailed to you by someone that you know.

- Never open or execute a file sent to you by someone that you don't know. Delete it immediately.

- Do not buy or sell anything via the school network without the permission of the Head Teacher.

- Be careful not to divulge pupil email addresses accidentally.
- The use of personal mobile phones and personal devices within school teaching areas (including playgrounds) is strictly prohibited. Under no circumstances are images to be captured or shared. Mobile phones are only to be used in emergency situations when it is a designated point of contact off the school teaching site. Unless a staff member informs a senior manager that they need to keep their phone with them for personal reasons.
- When using social media for personal use, ensure that privacy setting are at a maximum. Do not discuss anything to do with school or your role; do not become “friends or followers” (ie communicate with) of any current pupils or past pupils. The same applies to parents/carers of current students. If you see anything derogatory related to the school, report it to the Head of the school.

Appendix 2 - What pupils need to be taught about acceptable use

Obviously these teaching points will need to be modified relevant to the age of the children and to the extent of their use of the network.

- Always log off when you have finished using a computer.
- Never disclose your password.
- Do not log-on as anyone else.
- If you get a message on the screen about a virus, stop working and tell a teacher straight away.
- Don't put portable data storage devices from home into the school’s computers. If you want to use one, discuss it with a teacher.
- If you see anything on the Internet that you think is upsetting or rude, use Hector the Protector and show it to an adult who will inform the teacher straightaway.
- Do not give your email address to anybody, particularly a stranger, without asking your teacher first.
- Never type your name, address or other personal details in on a web page without asking permission first.
- If you receive an email from somebody that you don't know, tell a teacher as soon as possible.
- Never tell anyone private details about yourself in an email, especially your address and telephone number.
- Remember that the school rules about being kind and considerate in what we say to others applies to email as well.
- Be aware that their email is not private and that teachers may look at what they have written.
- Be aware that the network can detect misuse of the computers and record details of the person responsible.

- Never download files or programs from the Internet without getting permission from a teacher.
- Tell a teacher about any files attached to an email that you were not expecting to receive.
- Be careful not to change or delete other people's work in the T:\Shared Files folder.

ACCEPTABLE USE OF INTERNET

- All potential users of the Internet should understand basic conventions and navigation techniques before going on-line and accessing Web pages.
- We will inform children that logs are kept of sites visited and why. Children should report any cyber-bullying to a member of staff who will be able to follow the trail
- Children/ adult learners must agree to act responsibly and use the Internet in school for course-related work only
- Children/ adult learners must agree to respect copyright and not to plagiarize others' work
- Children/ adult learners must agree to download pages only to the disk specified by the teacher. We will explain why such restrictions are necessary
- Members of staff will check personal disks and mobile devices for viruses and unsuitable material
- Children/ adult learners must agree not to attempt to access unsuitable material
- We will remind children that the possession of certain types of unsuitable material can Lead to prosecution by the police

Sanctions for violations of the Acceptable Use Policy

Minor infringements will be dealt with by enforcing a temporary ban on Internet use and / or by additional disciplinary action in accordance with existing school procedures and policies. For serious or repeated minor violations, the child's parents will be involved.

The Internet at home

Parents are expected to discuss and agree some sensible points with their children. We suggest they:

- keep in touch with what children/adult learners are doing with their computers,
- Ask them to show which sites they have visited and talk about what they learned there
- Encourage children/adult learners to use computers only as one of a range of out of school activities.
- Ensure that social media has the highest possible privacy settings and that pupils/ adult learner are only in contact with 'real' friends.

Parents are strongly advised to:

- Keep use of internet accessible devices such as phones, tablets and laptops restricted to a place where a responsible adult can supervise

- Be aware that devices are not limited to those mentioned above. Gaming machines also allow online communication

- Take an interest in what children are doing with the computer and install '*Hector the Protector'* monitoring device on www.microsoft.com

- Ask children/adult learners to show how the family computer works and explain how they use computers at Granta

- Advise children/adult learners to take care whenever they are on-line reminding them never to give out any personal information about themselves, particularly full, names, addresses, phone numbers, or financial information.

- Remind children/adult learners never to give anyone else their password

- Remind children/adult learners that people on-line may not be who they seem, and no matter how well they feel they know someone, ***that person is still a stranger***

- Ensure that children/adult learners never arrange to meet someone in person that they have made contact with on-line

- Tell children/adult learners to inform a ~~member of staff/family member~~ Trusted adult who will delete attachments from strangers without opening them; they may contain viruses that can damage the computer

- Tell children/adult learners not to respond if they see any messages which they find upsetting, and reinforce that emails. They should tell a ~~member of staff/family member~~ Trusted adult about any such message

- Emails offering banking and/or prizes are from people they don't know and therefore shouldn't be responded to. They should tell a ~~member of staff/family member~~ Trusted adult about any such messages.

- Make sure that using social media and playing video games are only two activities among many that you can enjoy.

- Be aware that children/young adult learners with access to credit cards could use then for on-line purchases, if not supervised.

- Learn at least the basics about computers if not computer literate

Authorised Use consent form for pupils

The school has adopted certain safeguards in order to minimise any risk to pupils. Please read through these points and sign below.

- Always log off when you have finished using a computer.
- Never disclose your password.
- Do not log-on as anyone else.
- If you get a message on the screen about a virus, stop working and tell a teacher straight away.
- Don't put portable data storage devices such as memory sticks from home into the school's computers. If you want to use one, discuss it with a teacher.
- If you see anything on the Internet that you think is upsetting or rude, use Hector the Protector and show it to a Trusted adult who will inform the teacher straightaway.
- Do not give your email address to anybody, particularly a stranger, without asking your teacher first.
- Never type your name, address or other personal details in on a web page without asking permission first.
- If you receive an email from somebody that you don't know, tell a trusted adult away.
- Never tell anyone private details about yourself in an email, especially your address and telephone number.
- Remember that the school rules about being kind and considerate in what we say to others applies to email as well.
- Be aware that your email is not private and that teachers may look at what you have written.
- Be aware that the network can detect misuse of the computers and record details of the person responsible.
- Never download files or programs from the Internet without getting permission from a teacher.
- Tell a ~~teacher~~ Trusted adult about any files attached to an email that you were not expecting to receive.
- Be careful not to change or delete other people's work in the T:\Shared Files folder.

Parent/carer ……Date……

Pupil ……

We will advise individual parents on the following:

- Take an interest in what children and adult learners are doing with the computer and install 'Hector the protector' monitoring device on www.microsoft.com
- Ask children and adult learners to show how the family computer works and explain how they use it at Granta
- Advise children and adult learners to take care whenever they are on-line reminding them never to give out any personal information about themselves, particularly full, names, address, phone numbers, or finical information.
- Remind children and adult learners never to give anyone else their password.
- Remind children and adult learners that the people on-line may not be who they seem. And no matter how well they feel they know someone, that the person is still a stranger
- Ensure that children and adult learners never arrange to meet someone in person that they have made contact with on-line.
- Tell students and adult learners to inform a member of staff/family member who will delete attachments from strangers without opening them; they may contain viruses that can damage the computer.
- Tell students and adult learners no to respond if they see any messages which they find upsetting, and reinforce that emails. They should tell a member of staff/family member about any such messages.
- Email offering banking and/or prizes are form people they don't know and therefore shouldn't be responded to. They should tell a member of staff /family member about any such messages.

Dear Parent,

Use of Internet by Pupils/young adults

As part of the Government National Grid for Learning Scheme and to support learning opportunities within the school, your child/children/young adult will at appropriate times be given access to the Internet as an information source, a communications tool and a publishing medium.

The Internet is fast becoming a major source of educationally useful material and the primary distribution medium for a wide range of organisations. The potential to support the classroom teacher and the learner is significant and will continue to grow.

There are well publicised concerns regarding access to material on the Internet that would be unsuitable for school pupils. Whilst it is impossible to ensure that a pupil will not access such material, the school in liaison with Cambridgeshire Education Authority, is taking all reasonable steps to minimise a pupils access to unsuitable material. These include:

- Use of a filtered Internet Service to prevent access to Internet sites with undesirable material
- The requirement that wherever possible, all Internet access during school hours will be supervised by a member of staff or another responsible adult
- Education of pupils as to the potential legal consequences of accessing certain types of materials.

The school has a website that includes information about many aspects of school life. Within published guidelines the school may publish pictures or work relating to your child/young adult. Please indicate on the form below your willingness (or not) for any reference to your child/young adult to be included on the school Internet site.

Parental Consent Form

Pupil Name:……

As parent or legal guardian of the above pupil/adult learner:

- I give my permission for my son/daughter to use computer systems to access the Internet and E mail.
- I have read the attached letter and understand that the school will endeavour to take all reasonable steps to restrict access to unsuitable material on the Internet.
- I have read the Rules for Responsible Use of ICT and the Internet and have discussed them with my child/adult learner
- I do/do not give permission for my child's/adult learner picture or work to be published on the school website (no names are used for any pupil work on the website).

Signature of Parent or Guardian

…… Date……

If you wish to discuss anything in connection with the above issues, please contact the school

- I will always tell an adult when I am using the internet
- I will keep my password private - it is personal to me
- I will keep my personal information private online and at school
- I will only send kind messages when using social media
- I will only send and accept friend requests from people I know
- I will only talk to people I know in computer games or on social media
- I will tell a trusted adult if I see something that upsets me or that I am unsure about

Authorised Use consent form for staff

The school has adopted certain safeguards in order to minimise any risk to staff. The main points are detailed below. Once you have read these please sign below for our files.

- Don't divulge your staff log-on password under any circumstances and change it if you think it has been compromised.
- Don't leave a computer unattended and logged on to a staff log-on.
- Make sure that personal use of the network does not interfere with normal school operations.
- Explicitly teach children the points laid out in Appendix 2 i) at the start of each academic year and ii) when relevant computer based activities are about to begin.
- Actively monitor the websites that children are visiting during open web-browsing sessions and do not leave a group unsupervised.
- Try wherever possible to visit websites before you use them in your teaching so that you can check their acceptability.
- When children are to use a search engine, try to make it one that has been developed for children.
- Report any inappropriate websites that you find to the ICT Co-ordinator/Administrator so that they can be filtered out.
- Never divulge the "www" log-on password, and always ask for it to be changed if you think it has been compromised.
- Actively monitor pupils' email messages.
- Always respond to an on-screen virus warning. Isolate the machine and inform the ICT Co-ordinator/Administrator immediately.
- If you download any executable programs or Microsoft Word documents, have them virus checked before you open them or execute them. The same applies when this type of file has been emailed to you by someone that you know.
- Never open or execute a file sent to you by someone that you don't know. Delete it immediately.
- Do not buy or sell anything via the school network without the permission of the Head Teacher.
- Do not use personal mobile phone and personal mobile devices within school teaching areas (including playgrounds/outside spaces, this is strictly prohibited. Under no circumstances are images to be captured or shared. Mobile phones are only of be used in emergency situations when it’s a designated point off the school teaching site.

Name…….. Date……