This policy is currently under review by the Governing Body and will be updated shortly. March 2017

Graveney School E-safety and Acceptable use of ICT

Adopted by the Governing Body

Last updated: June 2015
Review date: June 2016

To be read in conjunction with the Anti-bullying, Safeguarding/ Child Protection/ Looked After Learners and Citizenship policies.

Graveney School E-safety and Acceptable use of ICT

This policy applies to all members of the Graveney school community (including staff, pupils, governors, volunteers, parents/carers, visitors and community users) who have access to, and are users of, school ICT systems, both in school and out of school where actions relate directly to school set activity or use of school online systems.

THE BACKGROUND

To prepare pupils for the needs of both today and their future working lives the curriculum requires them to learn how to locate, retrieve and exchange information using a variety of technologies. Computer skills are vital to access life-long learning and employment, and indeed ICT is now seen as an essential life skill for all. The internet is an integral element of 21st century life for education, business and social interaction
However technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings our staff and pupils into contact with a wide variety of influences some of which may be unsuitable. These new technologies are enhancing communication and the sharing of information, and inevitably challenge the accepted definitions of the boundaries of a school. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

> **Internet websites, instant messaging, social networking sites e-mail, blogs, podcasting, video broadcasting sites, chat rooms, gaming and gambling sites, music download sites, mobile phones with camera and video functionality, digital cameras, PDAs, and smart phones with e-mail and web applications.**

All of these have the potential to help raise standards of teaching and learning, but may equally present challenges to both pupils and staff in terms of keeping themselves safe. These challenges include;

- exposure to age inappropriate material
- cyber-bullying via websites, mobile phones or other technologies.
- Identify theft or invasion of privacy
- downloading copyrighted materials
- exposure to inappropriate advertising, online gambling and financial scams
- child protection issues such as grooming, extremism, ‘sexting’ etc
- other illegal activities

At Graveney we need to maximise the educational benefit that can be obtained by exploiting the use of ICT, while at the same time minimising any associated risks. By making clear to pupils, staff and parents what the schools expectations are regarding the use of ICT we aim protect our pupils and staff from harm, as far as is reasonably practicable. The precise nature of the risks faced by users will change over time as technologies, fads, and fashions change, but there are general principles of behaviour that apply to all situations, e.g. pupils need to know how to react if they come across inappropriate material, and that they should not give out their personal information such as their telephone numbers and addresses to strangers or publish this information on social networking sites.

A balance needs to be struck between educating staff and pupils to take a responsible approach, and the use of regulation and technical solutions. We must recognise that there are no totally effective solutions to moderate and control the internet, so this policy incorporates both approaches.

ROLES AND RESPONSIBILITIES

Staff

All teaching and non teaching staff (including volunteers, supply and temporary staff) are responsible for promoting and supporting safe behaviour in the school and following school e-safety procedures. All Graveney staff should be familiar with the E-safety and Acceptable Use of ICT Policy (AUP) as well as their relevance to the Anti-bullying, Extremism and Anti-Radicalisation, Child Protection, and Behaviour Policies, which are available in the Staff Guide, in the Staff Room on Fronter.

- All staff should participate in any e-safety training and awareness raising sessions
- All staff should have read, understood and accepted the Staff Acceptable Use Agreement. (It is explicitly stated in employment contracts and is a condition of service).
- Act in accordance with the AUP and e-safety policy
- They should report any suspected misuse or problem to the E-Safety Co-ordinator

- Staff should help educate pupils in keeping safe. Whilst regulation and technical solutions (such as filtering systems) are very important, they must be balanced by educating learners to take a responsible approach. The education of pupils in e-safety is an essential part of using technology in lessons. Guidance and support should be appropriate to the age of the learners. Older pupils will probably have both more access to and experience of, technologies, but may therefore be more likely to encounter problems e.g. through mobile phone usage. Staff should act as good role models in their own use of ICT.
- Where internet use is pre-planned in lessons, extracurricular and extended school activities, pupils should be guided to sites checked as suitable for their use, and procedures followed for reporting any unsuitable material that is found in internet searches. Staff should pre-check any searches.
- Where learners are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit and encourage them to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Staff should be aware of the potential for cyber- bullying in their lessons where malicious messages e.g. through the use of 'stickies' on Fronter can cause hurt and distress.
- Pupils should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils are educated of the need to acknowledge the source of any information used and to respect copyright when using material accessed on the internet.

Pupils

Pupils are encouraged to access various technologies in lessons, private study periods, the completion of homework and independent research, and are therefore expected to follow the Graveney Acceptable Use Policy,. They should participate fully in e-safety activities, and report any suspected misuse to a member of staff. They need to understand that the E-Safety Policy covers actions out of school that are related to their membership of the school

To assist them in this:

- pupils are helped to understand the Acceptable Use Policy and to acknowledge agreement they sign a copy in their organizers. In KS3 this takes place in IT lessons; for KS4 and 5, this is done in form time.
- the Acceptable use policy has to be accepted every time a pupil logs onto the Graveney IT system; the policy is clearly displayed on their main entry page.
- there is a planned e-safety programme delivered in Key Stage 3 IT lessons.
- e-safety messages are reinforced regularly through assemblies and e-safety week e.g. competitions, and presentations.
- poster displays are placed in the most appropriate parts of the school e.g. the plasma screen in the dining hall, IT rooms LS hall etc. Including pupil work from recent e-safety competitions.
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- learners are to be encouraged to question what they read and seek confirmation of the content they are reading from another source.
- pupils, particularly those who are younger or more vulnerable need to be encouraged and supported to report bullying or inappropriate material to staff so that appropriate action can be taken, e.g. through online reporting in Fronter. Links to helpful websites outside school are made clear and accessible in Fronter and on the school website.

Parents / Carers

Parents and carers may have only a limited understanding of e-safety issues and may be unaware of risks and how to minimize them. But they have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. We expect parents to support our policies by;

- endorsing (by signature) the Pupil Acceptable Use Policy
- ensuring that their child / children follow acceptable use rules at home
- discussing e-safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet.
- supporting the Graveney policy on the use of personal mobile phones in school

The school supports parents to do this by;

- issuing clear acceptable use policy guidance e.g. in the pupil organizer and on the Graveney web site.
- providing advice and guidance on the school website with further links to specialist websites such as CEOPs. 'Think U Know' etc.

- providing awareness raising meetings for parents e.g. the GPTA meetings, the Year 10 Introduction to GCSE evening and the induction day for new parents. Information and guidance on cyber bullying, chat rooms and the use of Fronter has been a key feature of these sessions.
- keeping parents abreast of the latest IT developments affecting their children e.g. online reporting, use of parent mail, and the expanded use of our VLE, Fronter.

E Safety Incidents outside school

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school. The school will deal with such incidents where they are contrary to good order and discipline within the school. An investigation will take place, parents will be informed and other sanctions will be considered such as use of the behaviour support unit or even exclusion if it is deemed appropriate by the school. A referral to other agencies will also be considered if required.

Governors

Governors should appoint an e-safety governor with responsibility for working with members of the school in this field. Currently it is **Ian Parkes** who is a member of the curriculum sub-committee. The curriculum sub-committee should approve and review the effectiveness of the E-Safety Policy and acceptable use policies annually. The e-safety governor should work closely with members of the school e-safety committee to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then report to the full governors. The outcome of the review and monitoring procedures will be formally recorded in the relevant minutes.

The E Safety Committee

The group consists of:

Peter Sutton – Senior Teacher with responsibilities for curriculum
Lynlea Ward – Senior ICT manager
Duncan Wood – Joint Manager ISD
Marie Robertson – Assistant head and DSM Child Protection Officer.
Cynthia Rickman – Bursar and the IT technician line manager

The committee (together with the senior management and designated technical staff) will ensure that:

- all pupils and staff (particularly new appointments) are made aware of the procedures outlined in our policies.
- school ICT systems are managed in ways that ensure that the school meets the e-safety technical requirements outlined in the LGFL Security and Acceptable Usage Policy and relevant local authority e-safety guidance.
- e-safety policies and practices are reviewed, monitored and amended as required through regular meetings, analysis of data and consultation with others, including parents/carers and pupil feedback e.g. questionnaires.
- advice and guidance to pupils, staff and parents/carers is reviewed, updated and disseminated in line with technological changes and capability.
- the school maintains and supports the managed filtering service with daily monitoring of appropriate use. Users are made aware of this in the Acceptable Use Policy.
- the E-Safety Policy is reviewed annually by the Governors Curriculum sub-committee. Regular reports are presented with details of planned developments, incidents of misuse and any problems experienced.
- appropriate security measures are in place to protect the ICT systems through use of antivirus software, firewalls, passwords, policies on the use of USBs etc
- respond quickly and appropriately to incidents of misuse. Whilst the vast majority of members of the school community will be responsible users of ICT, there may be times when infringements of the policy take place, through careless, irresponsible or, deliberate misuse.
- make recommendations to senior leaders and governors of the need to make changes.

Senior Leaders

The school senior leadership takes e-safety very seriously and will ensure that policies and procedures are in line with best practice and the Every Child Matters agenda. In particular they will ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resources are allocated to the task. Senior leaders will follow correct procedure in the event of a serious e-safety allegation being made against a member of staff, and ensure that there is a robust system in place for monitoring e-safety. This includes making sure that the school infrastructure / network is

safe and secure, and that policies and procedures approved within this policy are implemented. Regular review of the issues will take place at senior staff meetings.

RESPONDING TO INCIDENTS OF MISUSE

It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Where it is suspected that any misuse might have taken place the relevant member of staff (which will depend on the nature of the misuse - the Head teacher for example will be informed of any staff misuse) will investigate, taking the necessary steps to ensure that any evidence is secured and preserved. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse, but where there are good grounds to believe that illegal activity has taken place the Head teacher will be informed immediately, policies on child protection will be followed, and referrals to the necessary outside agencies will take place where required.

The investigation into pupil misuse will result in an appropriate sanction. The nature of that sanction will depend upon whether an action was accidental or deliberate, a first time or repeated offence, thoughtless or malicious, e.g. intended to cause harm to others. Sanctions may involve the pupil being interviewed and reprimanded, parents informed, removal of IT access for a temporary period, use of the behaviour support unit, or in very serious cases, exclusion. Where there is a potential legal issue the Head teacher will decide on the need for the involvement of outside agencies including the police, in line with child protection and other policies.

Useful web addresses:

www.thinkuknow.co.uk – lots of advice for parents and young people on staying safe online.
www.ceop.gov.uk – Child exploitation and Online Protection centre focussed on tackling child abuse.
www.chatdanger.com – gives details on the potential dangers of interactive services e.g. chat, online games, email etc.
www.kidsmart.org.uk – a practical internet safety programme for young people and parents/carers.
www.childnet-int.org – from charity Childnet International
http://schools.becta.org.uk – further advice and guidance.

RECENT ACTION IN SUPPORT OF THE E SAFETY POLICY

- The pupil esafety competition was held again in 2013-14. Winning entries continue to be used in subsequent assemblies and on the website/Fronter page, as well as exemplars in a presentation to the local authority staff.
- Special assemblies in the autumn term 2014 on the issues around personal safety, ‘sexting’ and exposure to inappropriate material were given to year 9.
- In Autumn term 2014 a special letter was sent to Year 9 parents (following issues in that year) on the problems of mobile phone use and the dangers of inappropriate images. The legal position explained.
- Various staff assemblies on the use of technologies and safety in 2014-15 e.g. the consequences of cyber-bullying as well as the negative impact of overuse of computer games to Year 7 in the autumn and spring term terms of 2014-15.
- Thorough and regular checks on the use of school IT equipment with a particular focus on extremist websites, potential radicalisation and the dangers of violent and inappropriate images.
- GAGV workshops in the summer term 2014 and again later in 2015 for Years 7-11. The focus is on ‘gang grooming’ and how images and texts are used to entrap young people into gang culture particularly girls.
- Workshops for pupils on esafety by other outside agencies planned for summer term 2015.
- May 5th 2015 - workshop for parents on esafety presented by a Graveney parent who works in the IT industry. The focus was on general esafety tips, as well as useful information on the apps and sites that young people are using today. The emphasis was ‘what parents need to know’ about these sites.
- Disciplinary action (including exclusion) has been taken against some pupils who have abused this policy, for example cyber- bullying, in the 2014-15 academic year – see exclusion and BSU reports to SMT and governors.
- Extremism and anti-radicalisation training for staff by Prevent on September 1 and then again on 23 April 2015 to ensure all staff are trained in this important area (which has an important esafety dimension). After governors have agreed the policy changes it is anticipated there will be further follow up work on extremism/radicalisation issues, including esafety.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, Citrix, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I will ensure that I log off my computer when I am not using it to avoid unauthorised access by others to school systems and data
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I understand that I may compromise my professional standing if I misuse or place personal material on social networking sites
- I understand that to use personal equipment for the recording and storage of images of pupils/parents and the use of personal email addresses or phone numbers to contact pupils/parents may leave me vulnerable to allegations of inappropriate conduct

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will use school equipment to record these images Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's Code of Practice.
- I will communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. Should this occur accidentally then I will immediately report the incident.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others in accordance with the school's Data Protection Policy . Personal data about another person will never be transferred outside the secure school network without express permission from the school Data Controller, currently Cynthia Rickman.
- I understand that the school's Data Protection Policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except where I am required by law or where I have the express permission of the school to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police. ***

Graveney School Code of Practice on Staff Use of ICTs

At Graveney we are committed to maximising the potential of ICTs and the Internet as learning and research tools and to ensuring that these facilities are used both efficiently and effectively across the curriculum for the benefit of all pupils and staff. Our Acceptable use Policy describes the framework for the use of ICTs in school and this Code of Practice provides further guidance for staff.

ACCEPTABLE USE – FURTHER GUIDANCE

Given that the Internet has become an integral part of our professional lives, we need to agree the framework within which we can use it. It is provided to facilitate your work as an employee of the school specifically for educational, training, administrative and research purposes.

Acceptable use may also include personal email and recreational use of internet services as long as these are in keeping with the framework defined in this code of practice. However, recreational use is a privilege and not a right and must not, in any way, bring the name of the school into disrepute.

The following guidelines will help you to keep within our definition of acceptable use of ICTs:

- do not expect to hold information on school systems that you would not wish to be seen by an authorised member of staff. Your use of the facilities may be monitored and IT staff are authorised to release the contents of your files to your manager if there is a reasonable work-based reason for so doing.

It will always be unacceptable to:

- retain or propagate material that is offensive, obscene or indecent
- break into or damage computer systems or data held thereon
- access or take actions intended to facilitate access to computers/files for which the individual is not authorised
- engage in non-academic activities which generate heavy network traffic or which interfere with your duties or the work of others
- disregard the school's security requirements (data and equipment).

EMAIL

A school wide internal email system is available for use by staff. It provides a quick and easy means for staff to communicate with each other. However, if used carelessly, it can cause additional work, irritation and frustration for others. We therefore expect staff to use email in accordance with the following guidelines:

You are responsible for maintaining (keeping tidy) your Outlook account and separate guidance will be provided on its use including transmission, storage, deletion of messages and attachments.

Remember, your emails are not private – they can be forwarded to anyone including parties you may not have expected. Remarks or jokes sent by email can amount to harassment and could well form the foundation of a discrimination claim.
There might be occasions when you need to use the school facilities for personal reasons and you have a right to respect for your private life and correspondence. However, you cannot expect complete privacy

and you should be aware that your use of the email system will be monitored. In the first instance, monitoring will be undertaken by the IT team who will treat all information thus accessed as confidential. Only if certain criteria are met (level of use/search on key words) will information about your use be passed on to your manager.

The following guidelines will help you to ensure that your use of email is acceptable

- do not circulate frivolous material via email to in-school circulation lists
- remember that it is a criminal offence to send an email with an obscene image attached to it.
- do not pass on electronic chain mail
- never open emails unless you are certain of their source. If the sender is unknown to you, you should ask for emailed confirmation of the contents of any attachment before you open it
- never email material that contains comments or remarks about, or images of, an identifiable individual or in any way infringes the school's equal opportunities policy. To do so will result in disciplinary action but also puts you in danger of contravening a variety of legislation including that relating to sex/race discrimination, harassment and data protection
- you may be held responsible for the retention of attachment material that has been received via electronic mail whether or not you have viewed it. You should therefore delete email items and attachments where you have concerns about their source/appropriateness without opening them. Where this is not clear from header material and you open and read an inappropriate item, you should then delete it.

To help us all to manage email we will put in place the following protocols:

- we will set up a number of email groups to try and reduce the amount of irrelevant mail we receive. In the first instance this will be limited to email groups for the teachers of KS3 classes. In future, we may be able to expand the range of groups

- in order to assist your filing and retrieval of email information from SLT, which may be sent from a range of different addresses, we will code important whole school correspondence from SLT to which you may need to refer later with the subject header 'Colleagues Letter - ..subject….'

CHAT ROOMS AND SOCIAL NETWORKING SITES

You should only use chat rooms whilst using school facilities where there is a clear educational reason for doing so. Usually, this will be through using Fronter chat room facilities.

You should not use social networking sites as a means to contact pupils or parents whilst using school equipment or at home. Separate guidance is available to staff on how to use social networking sites safely and to reduce exposure to risks including harassment by others, inappropriate behaviour from others and/or accusations of the same against yourself.

GENERAL

This policy is not exhaustive and inevitably new social and technological developments will lead to further uses which are not fully covered. In the first instance, staff should address questions concerning what is acceptable to their manager. If there continues to be any doubt, the issue should be raised with a member of the senior leadership team.

Graveney School Student / Pupil Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Graveney School will try to ensure that *students / pupils* will have good access to ICT to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.

ACCEPTABLE USE POLICY AGREEMENT

I understand that I must use Graveney's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- I will not arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that Graveney's ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that Graveney School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use chat and social networking sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that Graveney School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

STUDENT / PUPIL ACCEPTABLE USE AGREEMENT FORM

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, PDAs, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil	
Group / Class	

Signed		Date	