eSafety Policy

Date Written :	*February 2017*
Date approved by Governors :	*24/04/2017*
Last reviewed:	*08/02/2018*
To be reviewed in:	*08/02/2019*
The person responsible for monitoring this policy statement and monitoring and evaluating its implementation is:	*Mr Simon Coward – ICT Co-ordinator*

Rationale

National guidance suggests that it is essential for schools to take a leading role in eSafety. Becta in its "Safeguarding Children in a Digital World" suggested:

> "That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for eSafety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting eSafety messages in home use of ICT, too."

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> "One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering eSafety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their eSafety policy, ensure that they meet their statutory obligations to ensure that children and

young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

Aims and Purposes

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors) who have access to and are users of school ICT systems, both in and out of school.

The following section outlines the roles and responsibilities for eSafety of individuals and groups within the school.

Prevent agenda

All staff should be aware of the Prevent agenda:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf.

- All staff should have undertaken the online training module as specified by Government.
- They should be aware of these issues when supervising use of any internet capable devices.

Use of the Internet

As the Internet is an essential part of learning today, it is implied that by attending Greenbank school permission is given by parents to access the Internet as a part of the learning experience.

Governors:

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

The Headteacher is responsible for ensuring the safety (including eSafety) of members of the school community.

The Headteacher/Senior Leaders are responsible for ensuring that staff receive suitable CPD to enable them to carry out their eSafety roles and to train other colleagues, as relevant.

The Headteacher and another member Senior Management Team (Mr M McCann & Mrs B Scott) should be aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff. (see WBC flow chart on dealing with eSafety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR/disciplinary procedures)

Teaching/Residential and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of eSafety matters and of the current school eSafety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation/action/sanction
- digital communications with students/pupils (email/Learning Platform) should be on a professional level and only carried out using official school systems
- eSafety issues are embedded in all aspects of the curriculum and other school activities
- students/pupils understand and follow the school eSafety and acceptable use policy
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of eSafety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated person for child protection – Mrs B Scott

Should be trained in eSafety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Students/pupils:

- are responsible for using the school ICT systems in accordance with the Acceptable Use Policy (Appendix 1), which their parents will be expected to sign before being given access to school systems
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good eSafety practice when using digital

technologies out of school and realise that the school's eSafety Policy covers their actions out of school, if related to their membership of the school

Please note: due to the nature of the students at Greenbank, understanding of the above issues may be limited or not present.

Implementation

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and student /pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.
The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school eSafety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students/pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil/student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this eSafety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students'/pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Policy Statements

Education – students/pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students/pupils to take a responsible approach. The education of students/pupils in eSafety is therefore an essential part of the school's eSafety provision. Children and young people need the help and support of the school to recognise and avoid eSafety risks and build their resilience. eSafety education will be provided in the following ways:

- A planned eSafety programme should be provided as part of ICT/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key eSafety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils should be helped to understand the need for the student/pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems/internet will be posted in all ICT suites

Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents/carers

Many parents and carers have only a limited understanding of eSafety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, learning platform and digital parenting guides given at reviews.

Education & Training – Staff

It is essential that all staff receive eSafety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal eSafety training will be made available to staff.
- This eSafety policy and its updates will be presented to and discussed by staff in staff/team meetings.
- The eSafety Coordinator (Mr S Coward) will provide advice/guidance/training as required to individuals as required

Training – Governors

- The Safeguarding governor will take part in eSafety training/awareness sessions.

Technical – infrastructure/equipment, filtering and monitoring

- The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
- School ICT systems must be regularly updated to ensure up-to-date anti-virus definitions and Microsoft Windows Security Updates are installed.
- Servers, wireless systems must be securely located and physical access restricted.
- All users will be provided with a username.
- The Administrator password for the school ICT system, must be available to the Headteacher.
- School data should be securely managed when taken off the school site using encrypted memory devices.
- Staff Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by shared Local Authotity IT services .
- Any filtering issues should be reported immediately to IT support.
- An appropriate system is in place for users to report any actual/potential eSafety incident.

Curriculum

- eSafety should be a focus in all areas of the curriculum and staff should reinforce eSafety messages in the use of ICT across the curriculum.
- eSafety should be taught regularly through a scheme of work with identified progression of knowledge, skills and understanding.
- eSafety skills should be embedded through both discrete ICT and cross-curricular application.
- In lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students/pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites visited.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that they can temporarily be removed from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- Students/pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students/pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website.
- Student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive

- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
- The data must be encrypted and password protected

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

- When using communication technologies the school considers the following as good practice:
- Where available the official school email service may be regarded as safe and secure.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students/pupils or parents/carers (email, chat, Learning Platform etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Students/pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used by members of staff.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:
If any apparent or actual misuse appears to involve illegal activity ie:

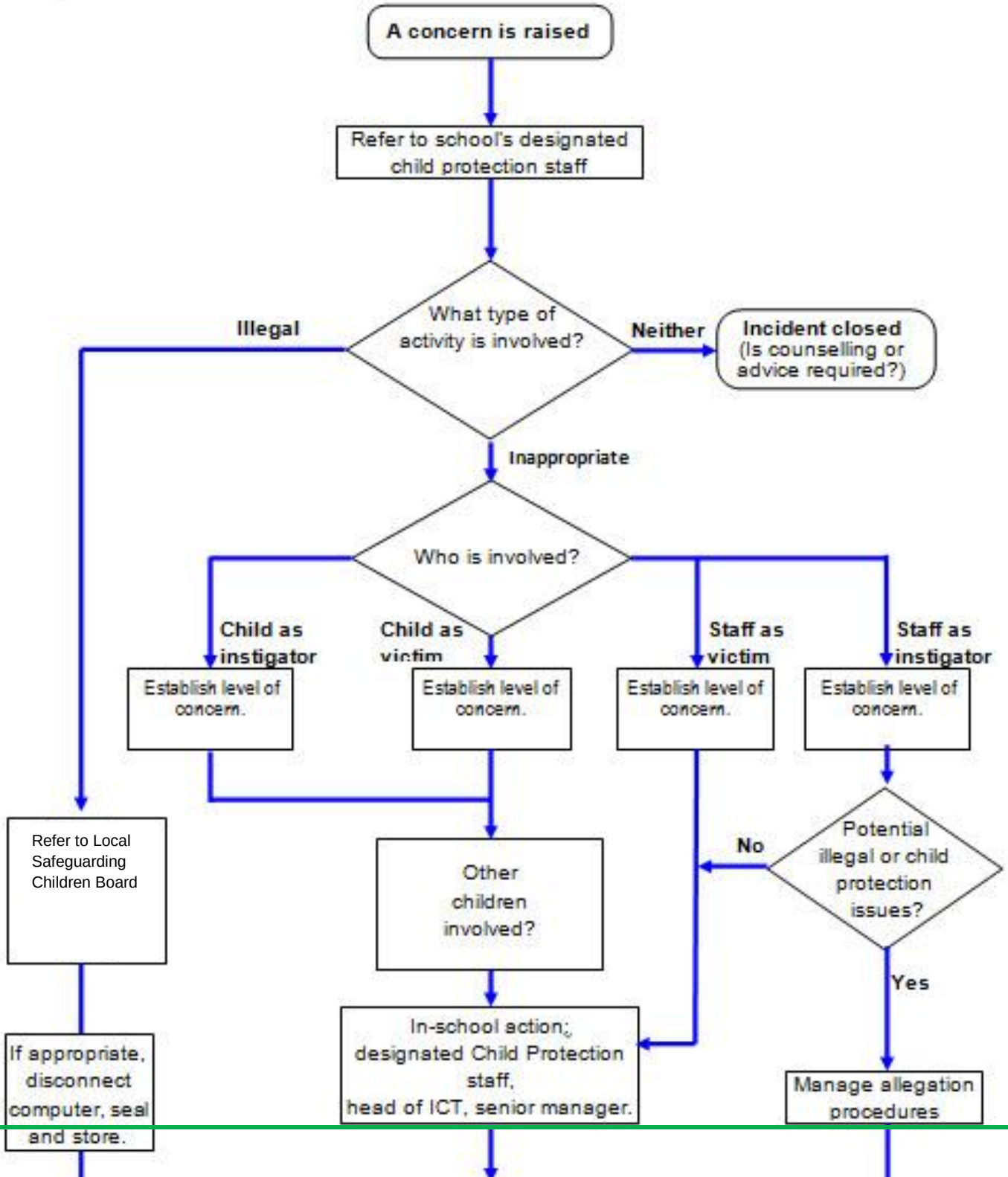
- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The WBC flow chart (on the following page) - should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal 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. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Response to an incident of concern



Appendixes

- **Staff acceptable use policy**

- **Internet rules/parent permission letter.**

- **Using images permission letter.**

Greenbank School

Staff 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 eSafety 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, learning platform etc) out of school.
- I understand that the school ICT systems are primarily intended for educational/professional purposes.
- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- 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 Staff user's files, without their express permission (unless I have Administrative access).
- 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 not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website/learning platform) 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 policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not use personal email addresses on the school ICT systems.

- 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 try to 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.
- 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, as outlined in the School/LA Personal Data Policy.
- Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy 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.
- I am aware of the Prevent agenda and its implications for the supervision of internet capable devices.

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 / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name

Signed

Date

Think then Click!

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can choose on Cool Maths Games or programs on the desktop.

We always ask if we get lost on the Internet.

We can send and open emails together.

We do not search without permission.

We can write polite and friendly emails to people that we know.

Using Images of Children

Occasionally, we may take photographs of the children at our school. We may use these images in our school prospectus or in other printed publications we may produce, as well as on our website. We may also make video or webcam recordings for school to school conferences, monitoring or other educational use.

From time to time, our school may be visited by the media who will take photographs or film footage of a visiting dignitary or other high profile event. Pupils will often appear in these images, which may appear in local or national newspapers, or on television news programmes.

Before we take a photograph, we need written consent in order to comply with the Data Protection Act 1998.

Please answer the following questions, then sign and date the form.

If the form is not signed, we cannot, and will not use the photograph.

Name of Child :_____

Name of Parent / Guardian : _____

Please circle Yes / No

May we use your child's photograph in the school prospectus and other printed publications that we produce for Promotional purposes ? YES / NO

May we use your child's image on our website ? YES / NO

Conditions Of Use